Kolchin's Proof that Differential Galois Groups are Algebraic

R.C. Churchill

Hunter College and the Graduate Center of CUNY, and the
University of Calgary

Prepared for the

Kolchin Seminar on Differential Algebra

Graduate Center, City University of New York

5 September 2014

These notes are an attempt to formulate Kolchin's proof of the algebraic nature of differential Galois groups in a contemporary mathematical style. The prerequisites from algebraic geometry are minimal: one needs to know little more than the Hilbert Basis Theorem and the definition of an algebraic set. The organization is heavily influenced by Kaplansky's treatment of the same result in [Kap, Chapter V, §20-1, pp. 33-37]. One minor difference occurs here: both Kolchin and Kaplansky worked with n^{th}-order linear ordinary differential equations, whereas we work with first order systems.

Contents

1. Introduction

Let K be an ordinary differential field[1]. We will be interested in a first order linear system

$$x' = Ax, \tag{1.1}$$

in which $A = [a_{ij}] \in \mathfrak{gl}(n, K)$. We assume $L \supset K$ is an associated Picard-Vessiot extension[2], and we let

$$\alpha \in \mathrm{GL}(n, L) \tag{1.2}$$

be a fundamental matrix solution of (1.1). The Picard-Vessiot hypothesis ensures that L admits "no new constants," i.e. that

$$L_C = K_C \tag{1.3}$$

($L_C \supset K_C$ is automatic from the containment $L \supset K$), as well as

$$L = K(\alpha). \tag{1.4}$$

The *differential Galois group* G of (1.1) is the group (under composition) of differential automorphisms $g : L \to L$ over K, i.e. automorphisms of L which commute with the derivation and fix K pointwise. By definition this group acts on L by evaluation, i.e. by

$$g \cdot \ell := g(\ell), \qquad (g, \ell) \in G \times L, \tag{1.5}$$

and an induced action on $\mathrm{GL}(n, L)$ is then given by

$$g \cdot m := [g \cdot m_{ij}] \qquad \text{for all} \qquad m = [m_{ij}] \in \mathrm{GL}(n, L). \tag{1.6}$$

If $\sigma : K(\alpha) \to K(\alpha)$ is a differential automorphism of $L = K(\alpha)$ over K then $\beta := \sigma(\alpha) \in \mathrm{GL}(n, L)$ must also be a fundamental matrix solution of (1.1). It follows from (1.3) and the calculation

$$\begin{aligned} (\alpha^{-1}\beta)' &= \alpha^{-1}\beta' - \alpha^{-1}\alpha'\alpha^{-1}\beta \\ &= \alpha^{-1}A\beta - \alpha^{-1}A\alpha\alpha^{-1}\beta \\ &= \alpha^{-1}A\beta - \alpha^{-1}A\beta \\ &= 0 \end{aligned}$$

[1] That is, assume K is a differential field with only one derivation. In these notes a "differential field" always means a field of this type, and when K is such we denote the subfield of constants by K_C.

[2] The required properties of such an extension are summarized in the next few sentences. For the definition see e.g. [C, §9].

that

$$\beta = \alpha C_g, \qquad \text{where} \qquad C_g = [c_{ij}] \in \mathrm{GL}(n, K_C) \tag{1.7}$$

or, equivalently, that[3]

$$\alpha^{-1}(g \cdot \alpha) =: C_g \in \mathrm{GL}(n, K_C). \tag{1.8}$$

In fact the mapping

$$\rho : g \in G \mapsto C_g \in \mathrm{GL}(n, K_C) \tag{1.9}$$

is a faithful representation which one can use to identify G with a subgroup of $\mathrm{GL}(n, K_C)$. The purpose of these notes is to formulate Kolchin's proof of the following result in contemporary terms.

Theorem 1.10 (Kolchin, 1948) [Kol_1]**:** *Assuming the notation introduced above, the image* $\rho(G)$ *is an algebraic subgroup of* $\mathrm{GL}(n, K_C)$.

We will deduce this theorem as a corollary to a stronger result: to achieve a Galois correspondence between closed subgroups and differential subfields one must prove a bit more (as did Kolchin).

All proofs of Theorem 1.10 familiar to this author require some knowledge algebraic geometry, but the particular background expected of readers varies considerably from presentation to presentation. Kolchin used an approach to that subject which is no longer in fashion; many contemporary proofs use such notions as Tannakian categories, Hopf algebras, torsors, and group cohomology. In these notes I hope to convince readers that Kolchin's original proof can be presented in a modern spirit without involving an overwhelming amount of algebraic geometry, either in the classical or modern scheme-theoretic sense.

The arguments I use are adapted from the proof found in Kolchin's original paper [Kol_1, Chapter IV] and from Kaplansky's version of that proof [Kap, Chapter V, §20-1]. The notation employed is my own, and often bears little resemblance to that found in these two references.

[3]The notation $\alpha^{-1}(g \cdot \alpha)$ indicates the product of the $n \times n$ matrices α^{-1} and $g \cdot \alpha$, as opposed to "the evaluation of α^{-1} at the point $g \cdot \alpha$" (which would make no sense, since neither of α and α^{-1} is a function).

2. Preliminary Remarks on Kolchin's Proof

In can be useful to initially regard Kolchin's arguments as being centered around a collection of commutative diagrams

$$\begin{array}{ccc} K[x] & \xrightarrow{\tau} & K(\alpha)[t] \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\gamma_{C_g}} \\ K(\alpha) & \xrightarrow{g} & K(\alpha) \end{array} \tag{2.1}$$

of K-algebras and homomorphisms, one for each $g \in G$. The specifics are as follows.

- $K[x]$ is the polynomial algebra in n^2 indeterminates x_{ij}, realized as a differential ring extension of K by defining[4]

  $$x' := Ax. \tag{2.2}$$

  (Our first-order formulation enables us to avoid introducing differential polynomials.)

- $\lambda : K[x] \to K(\alpha)$ is the K-algebra homomorphism uniquely determined by the assignments $x_{ij} \mapsto \alpha_{ij}$. We indicate this homomorphism by writing

  $$\lambda : x \mapsto \alpha, \tag{2.3}$$

  and we use analogous notation to describe any algebra homomorphism having a polynomial domain.

  We claim that λ is a differential ring homomorphism, and we will present two proofs: the first quite detailed, and the second quite concise. In each proof we use δ to denote both the derivation on K and the extended derivation on $K[x]$ (defined by (2.2)).

[4] Admittedly, the appearance of x in the notation $K[x]$ clashes with the use of x in (1.1), but this should not cause problems.

The First Proof

The typical monomial in $K[x]$ has the form

$$p(x) = k \prod_{ij} x_{ij}^{m_{ij}},$$

from which we see that

$$\begin{aligned}
\delta(p(x)) &= (k \textstyle\prod_{ij} x_{ij}^{m_{ij}})' \\
&= k' \textstyle\prod_{ij} x_{ij}^{m_{ij}} + k \sum_{ij} \big(\prod_{uv \neq ij} x_{uv}^{m_{uv}} \big) m_{ij} x_{ij}^{m_{ij}-1} x_{ij}' \\
&= k' \textstyle\prod_{ij} x_{ij}^{m_{ij}} + k \sum_{ij} \big(\prod_{uv \neq ij} x_{uv}^{m_{uv}} \big) m_{ij} x_{ij}^{m_{ij}-1} \sum_{\ell} a_{i\ell} x_{\ell j}.
\end{aligned}$$

Since λ is a ring homomorphism it follows from (2.3) that

$$(\lambda \circ \delta)(p(x)) = k' \textstyle\prod_{ij} \alpha_{ij}^{m_{ij}} + k \sum_{ij} \big(\prod_{uv \neq ij} \alpha_{uv}^{m_{uv}} \big) m_{ij} \alpha_{ij}^{m_{ij}-1} \sum_{\ell} a_{i\ell} \alpha_{\ell j}.$$

On the other hand, since $\lambda(p(x)) = k \prod_{ij} \alpha_{ij}^{m_{ij}}$ we see by replacing x_{ij} with α_{ij} in the calculation of $\delta(p(x))$ that

$$(\delta \circ \lambda)(p(x)) = k' \textstyle\prod_{ij} \alpha_{ij}^{m_{ij}} + k \sum_{ij} \big(\prod_{uv \neq ij} \alpha_{uv}^{m_{uv}} \big) m_{ij} \alpha_{ij}^{m_{ij}-1} \sum_{\ell} a_{i\ell} \alpha_{\ell j}.$$

The compositions $\lambda \circ \delta$ and $\delta \circ \lambda$ therefore agree on monomials of $K[x]$, and, since both compositions are additive, the claim follows.

The Second Proof

At the level of generators we have

$$(\lambda \circ \delta)(x) = \lambda(x') = \lambda(Ax) = A\lambda(x) = A\alpha = \alpha' = \delta(\lambda(x)) = (\delta \circ \lambda)(x).$$

Since $(\lambda \circ \delta)|_K = (\delta \circ \lambda)|_K$, the result follows.

Note that $\lambda(K[x]) = K[\alpha]$. As a consequence λ factors as

$$\lambda = \mathrm{inc} \circ \lambda_\alpha, \tag{2.4}$$

where $\lambda_\alpha : K[x] \to K[\alpha]$ is the epimorphism which can also be described as in (2.3), i.e. by

$$\lambda_\alpha : x \mapsto \alpha, \tag{2.5}$$

and $\mathrm{inc} : K[\alpha] \hookrightarrow K(\alpha)$ is the inclusion homomorphism. Both these factors are differential homomorphisms: for λ_α this is easily seen from the computation for λ; for inc the assertion is obvious.

- $K(\alpha)[t]$ is the polynomial $K(\alpha)$-algebra in the n^2 indeterminates $t_{11}, t_{12}, \ldots, t_{nn}$, which we realize as a differential ring extension of $K(\alpha) = L$ by defining

$$t'_{ij} := 0.$$

- $\tau : K[x] \to K(\alpha)[t]$ is the K-algebra homomorphism uniquely determined by the assignments

$$x_{ij} \mapsto \textstyle\sum_{\ell=1}^{n} \alpha_{i\ell} t_{\ell j}, \qquad 1 \leq i, j \leq n.$$

We indicate this mapping by writing

$$\tau : x \mapsto \alpha t. \tag{2.6}$$

We claim that τ is a differential ring homomorphism. We only offer a detailed version of the proof, leaving a more concise formulation to the reader. In the proof we again denote all derivations by δ.

As before, it suffices to prove that the compositions $\lambda \circ \tau$ and $\tau \circ \delta$ and $\delta \circ \tau$ agree on monomials $p(x) = k \prod_{ij} x_{ij}^{m_{ij}} \in K[x]$.

As before we have

$$\delta(p(x)) = k' \textstyle\prod_{ij} x_{ij}^{m_{ij}} + k \sum_{ij} \big(\prod_{uv \neq ij} x_{uv}^{m_{uv}} \big) m_{ij} x_{ij}^{m_{ij}-1} \sum_{\ell} a_{i\ell} x_{\ell j},$$

whereupon from (2.6) we see that

(i)
$$\begin{cases} (\tau \circ \delta)(p(x)) = k' \prod_{ij} (\sum \alpha_{ir} t_{rj})^{m_{ij}} \\ \quad + k \sum_{ij} \big(\prod_{uv \neq ij} (\sum_r \alpha_{ur} t_{rv})^{m_{uv}} \big) m_{ij} (\sum_r \alpha_{ir} t_{rj})^{m_{ij}-1} \sum_{\ell} a_{i\ell} (\sum_s \alpha_{\ell s} t_{sj}). \end{cases}$$

As for $(\delta \circ \tau)(p(x))$: from

$$\tau(p(x)) = k \textstyle\prod_{ij} (\sum_r \alpha_{ir} t_{rj})^{m_{ij}}$$

we see that

$$\begin{aligned} (\delta \circ \tau)(p(x)) &= k' \textstyle\prod_{ij} (\sum_r \alpha_{ir} t_{rj})^{m_{ij}} \\ &\quad + k \big(\textstyle\prod_{ij} (\sum_r \alpha_{ir} t_{rj})^{m_{ij}} \big)' \\ &= k' \textstyle\prod_{ij} (\sum_r \alpha_{ir} t_{rj})^{m_{ij}} \\ &\quad + k \textstyle\sum_{ij} \big(\prod_{uv \neq ij} (\sum_r \alpha_{ur} t_{rv})^{m_{uv}} \big) \big((\sum_r \alpha_{ir} t_{rj})^{m_{ij}} \big)' \\ &= k' \textstyle\prod_{ij} (\sum_r \alpha_{ir} t_{rj})^{m_{ij}} \\ &\quad + k \textstyle\sum_{ij} \big(\prod_{uv \neq ij} (\sum_r \alpha_{ur} t_{rv})^{m_{uv}} \big) m_{ij} (\sum_r \alpha_{ir} t_{rj})^{m_{ij}-1} \big(\sum_s \alpha'_{is} t_{sj} \big), \end{aligned}$$

whence from

$$\alpha'_{is} = \textstyle\sum_\ell a_{i\ell}\alpha_{\ell s}$$

and

$$\textstyle\sum_s(\sum_\ell a_{i\ell}\alpha_{\ell s})t_{sj} = \sum_\ell a_{i\ell}(\sum_s \alpha_{\ell s}t_{sj})$$

that

(ii)
$$\begin{cases} (\delta\circ\tau)(p(x)) = k'\prod_{ij}(\sum \alpha_{ir}t_{rj})^{m_{ij}} \\ \quad + k\sum_{ij}\big(\prod_{uv\neq ij}(\sum_r \alpha_{ur}t_{rv})^{m_{uv}}\big)m_{ij}(\sum_r \alpha_{ir}t_{rj})^{m_{ij}-1}\sum_\ell a_{i\ell}(\sum_s \alpha_{\ell s}t_{sj}). \end{cases}$$

Comparing (i) with (ii) we conclude that $\tau\circ\delta = \delta\circ\tau$.

- For each $g \in G$ we let $\gamma_{C_g} : K(\alpha)[t] \to K(\alpha)$ be the $K(\alpha)$-homomorphism uniquely determined by the assignments

$$t_{ij} \mapsto c_{ij}, \qquad 1 \le i,j \le n.$$

We indicate γ_{C_g} by writing

$$\gamma_{C_g} : t \mapsto C_g. \tag{2.7}$$

Using the fact that these homomorphisms are uniquely determined by the assignments (2.3), (2.6) and (2.7), it is a simple matter to check that the diagrams (2.1) (one for each $g \in G$) are commutative.

The definition of γ_{C_g} admits an obvious generalization for any $C \in \mathrm{GL}(n, K_C)$. Specifically, for any such C we let $\gamma_C : K(\alpha)[t] \to K(\alpha)$ be the $K(\alpha)$-homomorphism uniquely determined by the assignments

$$t_{ij} \mapsto c_{ij}, \qquad 1 \le i,j \le n,$$

and we indicate γ_C by writing

$$\gamma_C : t \mapsto C. \tag{2.8}$$

It should come as no surprise that each γ_C (hence each particular γ_{C_g}) is a differential algebra homomorphism.

As usual, it suffices to verify that $\gamma_C \circ \delta$ and $\delta \circ \gamma_C$ agree on monomials $p(t) = k \prod_{ij} t_{ij}^{m_{ij}} \in K(\alpha)[t]$. (Here we have $k \in K(\alpha)$.)

Since in this case the t_{ij} are constants we have

$$\delta(p(t)) = k' \prod_{ij} t_{ij}^{m_{ij}},$$

hence

$$(\gamma_C \circ \delta)(p(t)) = k' \prod_{ij} c_{ij}^{m_{ij}}.$$

On the other hand,

$$\gamma_C(p(t)) = k \prod_{ij} c_{ij}^{m_{ij}},$$

and since the c_{ij} are constants this gives

$$(\delta \circ \gamma_C)(p(t)) = k' \prod_{ij} c_{ij}^{m_{ij}} = (\gamma_C \circ \delta)(p(t)).$$

The assertion follows.

Proposition 2.9 : *For all $g \in G$ one has*

(i) $$\ker \lambda = \ker(\gamma_{C_g} \circ \tau).$$

Proof : Since g is an automorphism one has $\ker \lambda = \ker(g \circ \lambda)$, and since the diagram commutes one has $\ker(g \circ \lambda) = \ker(\gamma_{C_G} \circ \tau)$. **q.e.d.**

The introduction of the mappings γ_C allows one to construct "partial" diagrams

(2.10)
$$\begin{array}{ccc} K[x] & \xrightarrow{\tau} & K(\alpha)[t] \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\gamma_C} \\ K(\alpha) & & K(\alpha) \end{array}$$

corresponding to the diagrams (2.1). These partial diagrams will be used to construct the algebraic subset $\mathcal{V} \subset \mathrm{GL}(n, K_C)$ and to prove that the representation $\rho : G \to \mathrm{GL}(n, K_C)$ has image $\mathcal{V}$. We can dispense with one of the important preliminaries immediately.

Proposition 2.11 :

(a) *Suppose* $C \in \mathrm{GL}(n, (K(\alpha))_C)$ *has the property that*

(i) $$\ker \lambda \subset \ker(\gamma_C \circ \tau).$$

Then there is a unique differential K*-algebra homomorphism* $\kappa_C : K[\alpha] \to K(\alpha)$ *such that the diagram*

(ii) $$\begin{array}{ccc} K[x] & \xrightarrow{\tau} & K(\alpha)[t] \\ {\scriptstyle \lambda_\alpha}\downarrow & & \downarrow{\scriptstyle \gamma_C} \\ K[\alpha] & \xrightarrow{\kappa_C} & K(\alpha) \end{array}$$

commutes.

(b) *Any* C *of the form* C_g *satisfies* (i)*, and in that case*

(iii) $$\kappa_C = g|_{K[\alpha]}.$$

Proof :

(a) The existence of the induced homomorphism under the assumption (i) is a fundamental ring-theoretic result which we assume is familiar to readers (see, e.g. [Lang, Chapter II, §1, p. 88] or [Hun, Chapter III, §2, Theorem 2.9, p. 125]). The differentiability property is a straightforward consequence of the definition of κ_C in terms of cosets (*ibid*).

To establish uniqueness assume that the diagram also commutes when κ_C is replaced by a K-algebra homomorphism $\phi : K[\alpha] \to K(\alpha)$. Choose any $p(\alpha) \in K[\alpha]$ and then $p(x) \in K[x]$ such that $\lambda_\alpha(p(x)) = p(\alpha)$. Then

$$\begin{aligned} \phi(p(\alpha)) &= \phi(\lambda_\alpha(p(x)) \\ &= (\phi \circ \lambda_\alpha)(p(x)) \\ &= (\gamma_C \circ \tau)(p(x)) \\ &= \gamma_C(p(\alpha t)) \\ &= p(\alpha C) \\ &= \kappa_C(p(\alpha)), \end{aligned}$$

hence $\phi = \kappa_C$, and uniqueness follows.

(b) The initial assertion is immediate from (i) of Proposition 2.9. The final assertion is a consequence of the commutativity of (2.1) and the uniqueness assertion of (a).

q.e.d.

Corollary 2.12 : *Suppose in* Proposition 2.11 *that the Picard-Vessiot extension* $K(\alpha) \supset K$ *is algebraic. Then* $K[\alpha] = K(\alpha)$ *and* $\kappa_C \in G$.

> **Proof :** The equality $K[\alpha] = K(\alpha)$ is standard algebra[5], and since fields have no non-trivial ideals the differential homomorphism κ_C must be an embedding. (It cannot be trivial since 1 must be carried to 1.)
>
> Since for any $p(x) \in K[x]$ one has $(\gamma_C \circ \tau)(p(x)) = p(\alpha C)$, this embedding can be described by $\alpha \mapsto \alpha C$. Since any $q(x) \in K[x]$ be expressed in the form $p(xC^{-1})$, it follows that κ_C is surjective, which completes the proof. **q.e.d.**

The basic ideas behind Kolchin's proof are: to define an algebraic set $\mathcal{V} \subset \mathrm{GL}(n, K_C)$ in such a way that (i) of Proposition 2.11 holds if and only if $C \in \mathcal{V}$, which by Corollary 2.12 would have $\rho(G) \subset \mathcal{V}$ as a consequence; and to then generalize Corollary 2.12 to cover non-algebraic extensions so as to ensure that $\rho(G) = \mathcal{V}$.

[5]E.g. see [W, Chapter 1, §1, Proposition 1.2.5, p. 30] or use induction on [Lang, Chapter V, §1, Proposition 1.4, p. 225].

3. More Specific Remarks on that Proof

In fact Kolchin's proof somewhat more involved than what we have outlined in the previous section. Rather than dealing exclusively with a Picard-Vessiot extension $L = K(\alpha) \supset K$ for (1.1) he begins with a tower

$$M \supset L = K(\alpha) \supset K \tag{3.1}$$

of differential fields in which $K(\alpha) \supset K$ is as before and $M \supset L$ is not necessarily a no new constant extension, i.e., does not necessarily satisfy $M_C = L_C$. Of course one does have

$$M_C \supset L_C = K_C, \tag{3.2}$$

and the important special case $M = L$ duplicates the context of the previous section. The $n \times n$ matrices $x = [x_{ij}]$ and $t = [t_{ij}]$ will now be assumed to consist of indeterminates over M rather than over L.

Set

$$\Sigma := \{\, \sigma \,:\, \sigma : K(\alpha) \to M \text{ is a differential embedding over } K. \,\} \tag{3.3}$$

This takes the place of the differential Galois group G, but of course is not a group.

If $\sigma : K(\alpha) \to M$ is a differential embedding over K then $\beta := \sigma(\alpha) \in \mathrm{GL}(n, M)$ must also be a fundamental matrix solution, as one sees from

$$\begin{aligned} \beta' &= (\sigma(\alpha))' \\ &= \sigma(\alpha') \\ &= \sigma(A\alpha) \\ &= \sigma(A)\sigma(\alpha) \\ &= A\sigma(\alpha) \qquad \text{(because } \sigma \text{ fixes } K\text{)} \\ &= A\beta. \end{aligned}$$

By repeating the calculation leading to (1.7) we now conclude that

$$\beta = \alpha C_\sigma, \qquad \text{where} \qquad C_\sigma = [c_{ij}] \in \mathrm{GL}(n, M_C). \tag{3.4}$$

Let the assignment $x \mapsto \alpha$ define K-algebra homomorphisms $\lambda : K[x] \to K(\alpha)$ and $\lambda_\alpha : K[x] \to K[\alpha]$ as before, but now use

$$\tau : x \mapsto \alpha t \tag{3.5}$$

to define a differential[6] K-algebra homomorphism $\tau : K(\alpha) \to M[t]$. Last but not least, for each $C \in \mathrm{GL}(n, L_C) = \mathrm{GL}(n, K_C)$ define a differential M-algebra homomorphism $\gamma_C : M[t] \to M$ by

$$\gamma_C : t \to C. \tag{3.6}$$

The analogues of the commutative diagrams (2.1) are the commutative diagrams

$$\begin{array}{ccc} K[x] & \stackrel{\tau}{\longrightarrow} & M[t] \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\gamma_{C_\sigma}} \\ K(\alpha) & \stackrel{\sigma}{\longrightarrow} & M \end{array} , \tag{3.7}$$

one for each $\sigma \in \Sigma$, wherein

$$C_\sigma := \alpha^{-1}\sigma(\alpha) \in \mathrm{GL}(n, M_C). \tag{3.8}$$

The analogue of Proposition 2.9 is precisely what one would expect.

Proposition 3.9 : *For all $\sigma \in \Sigma$ one has*

$$\text{(i)} \qquad \ker \lambda = \ker(\gamma_{C_\sigma} \circ \tau).$$

> **Proof :** The proof is also as one would expect: an easy adaptation of that of Proposition 2.9. **q.e.d.**

The analogues of the partial diagrams (2.10) are

$$\begin{array}{ccc} K[x] & \stackrel{\tau}{\longrightarrow} & M[t] \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\gamma_C} \\ K(\alpha) & & M \end{array} , \tag{3.10}$$

one for each $C \in \mathrm{GL}(n, M_C)$.

[6]The differential structure for $M[t]$ as well as the proofs of differentiability for λ, λ_α and γ_C and the commutativity of (3.7) are obvious modifications of the analogues found in the previous section, and are therefore omitted.

Proposition 3.11 :

(a) *Suppose* $C \in \mathrm{GL}(n, M_C)$ *has the property that*

(i) $$\ker \lambda \subset \ker(\gamma_C \circ \tau).$$

Then there is a unique differential K*-algebra homomorphism* $\kappa_C : K[\alpha] \to K(\alpha)$ *such that the diagram*

(ii) $$\begin{array}{ccc} K[x] & \xrightarrow{\tau} & M[t] \\ {\scriptstyle \lambda_\alpha}\downarrow & & \downarrow{\scriptstyle \gamma_C} \\ K[\alpha] & \xrightarrow{\kappa_C} & M \end{array}$$

commutes.

(b) *Any* C *of the form* C_α *satisfies* (i)*, and in that case*

(iii) $$\kappa_C = \sigma|_{K[\alpha]}.$$

Proof :

(a) The proof is an easy adaptation of that of Proposition 2.11.

(b) The initial assertion is immediate from (i) of Proposition 3.9; the second from the the existence of the commutative diagrams (3.7) and the uniqueness assertion in (a).

q.e.d.

Corollary 3.12 : *Suppose in* Proposition 3.11 *that the Picard-Vessiot extension* $K(\alpha) \supset K$ *is algebraic. Then* $K[\alpha] = K(\alpha)$*, and* $\kappa_C : K(\alpha) \to M$ *is therefore a differential field embedding over* K*.*

Proof : The proof is an easy adaptation of that of Proposition 2.12.

q.e.d.

4. Preliminaries on Transcendence Bases and Transcendence Degrees

In this section there are no differentiability assumptions. R *is an integral domain with quotient field* F*, and* E *is a subring of* R *which is also a field. The case* $R = F$ *is not excluded.* n *is a positive integer, and* $x_1, x_2, \ldots, x_n$ *are indeterminates over* F*.*

In this section we detail some background material on field extensions which Kaplansky assumes is familiar to his readers. We also reproduce, with detailed proofs, several of his key lemmas.

We begin by establishing our notation, recalling a few definitions, and gathering a few needed facts about transcendence bases and transcendence degrees. The crucial result is Corollary 4.17: readers comfortable with that statement might do better to skip immediately to the next section.

Let S be a subset of F, with $S = \emptyset$, $S \subset R$, $S \subset E$, $S = R$ and $S = F$ being distinct possibilities. Then:

- $E(S)$ denotes the subfield of F generated by E and S, i.e. the intersection of all subfields of F containing $E \cup S$.

- The set S is *algebraically dependent* (*over* E) if there is a positive integer n, elements $s_1, s_2, \ldots, s_n \in S$, and a non-zero polynomial $p(x) = p(x_1, x_2, \ldots, x_n) \in E[x] = E[x_1, x_2, \ldots, x_n]$ such that $p(s_1, s_2, \ldots, s_n) = 0$. One refers to any such $p(x_1, x_2, \ldots, x_n)$ as a[7] *dependence relation* (*on* S).

  From the definition one sees that a singleton set $S = \{s\}$ is algebraically dependent (over E) if and only if the sole element s is algebraic (over E). Since $R \subset F$, it makes sense to refer to an element of R as being algebraic over E.

- S is *algebraically independent* (*over* E) if it is not algebraically dependent over E. Example: $S = \emptyset$. When this property holds for a singleton $S = \{s\}$ the element s is *transcendental* (*over* E). Specifically, $s \in F$ is transcendental over E if it is not a zero of any polynomial in $E[x]$. Since $F \supset R$, it makes sense to refer to any element of R as being transcendental over E.

[7] In our subject a "relation (over E)" between variables generally refers to such an equality, i.e. one of the form $p(s_1, s_2 \ldots, s_n) = 0$ for some polynomial $p(x_1, x_2, \ldots, x_n)$ $(\in E[x_1, x_2, \ldots, x_n])$. The terminology is borrowed from classical algebraic geometry.

Note that if S is algebraically independent over E, and if T is any subset of S, then T is also algebraically independent over E.

- S is a *transcendence base* (*for* [or *of*] F *over* E) if S is algebraically independent over E and maximal (w.r.t. inclusion) among all subsets of F which are algebraically independent over E.

- Let $A \supset B$ be an extension of integral domains and let T be a subset of A. An element $a \in A$ is[8] *algebraically dependent on* T *over* B if a is a root of a non-zero polynomial $\sum_{j=0}^{n} m_j x^j \in B[T][x]$. Specifically: the m_j are "polynomials in the elements of (finite subsets of) T with coefficients in B", which we understand to mean "elements of B" when $T = \emptyset$. In this special ($T = \emptyset$) case one simply says that a is *algebraically dependent over* B. In particular, when $A \supset B$ is a field extension and $T = \emptyset$ an element $a \in A$ is algebraically dependent over B if and only if it is algebraic over B.

Examples 4.1 :

(a) Any two elements of F which are algebraic over E are algebraically dependent over E. For suppose $\ell_1, \ell_2 \in F$ are algebraic over E. Then (as is assumed familiar to readers) the sum $\ell_1 + \ell_2$ is also algebraic over E, and as a result there is a polynomial $q(x) \in E[x]$ such that $q(\ell_1 + \ell_2) = 0$. For $p(x_1, x_2) := q(x_1 + x_2) \in E[x_1, x_2]$ we therefore have $p(\ell_1, \ell_2) = 0$.

(b) Let $E = \mathbb{R}$ and let R be the ring of analytic functions $f : \mathbb{R} \to \mathbb{R}$. Then $\cos t$, $\sin t \in R \subset F$ are algebraically dependent over $\mathbb{R}$. (Elements of $\mathbb{R}$ are identified with constant [analytic] functions.) Indeed, for $p(x_1, x_2) = x_1^2 + x_2^2 - 1$ one sees from the standard identity $\cos^2 t + \sin^2 t = 1$ that $p(\cos t, \sin t) = 0$.

On the other hand, the element $\cos t \in R \subset F$ is transcendental over $\mathbb{R}$. Otherwise there is a positive integer n and elements $r_0, r_1, \ldots, r_{n-1} \in \mathbb{R}$ such that

(i) $$\cos^n t + \textstyle\sum_{j=0}^{n-1} r_j \cos^j t = 0,$$

[8] This definition is adapted from [vdW, Chapter 10, §3, pp. 220-1], wherein $A \supset B$ is assumed a field extension. This field formulation is also found in [W, Chapter 1, §6, Definition 1.6.1, p. 38]. The concept is used by Kaplansky in our more general context, yet one will not find the necessary background in either [Hun] or [Lang], which for purposes of these notes are the basic references for algebra.

and we may assume n is minimal w.r.t. these properties. Differentiating this identity w.r.t. t gives

$$n\cos^{n-1}t\sin t+\sum_{j=0}^{n-1}r_j j\cos^{j-1}t\sin t=0,$$

whereupon multiplication by $\frac{1}{n\sin t}$ results in

$$\cos^{n-1}t+\sum_{j=0}^{n-1}\tfrac{r_j j}{n}\cos^j t=0.$$

Unless $r_j=0$ for $j=0,1,\ldots,n-1$ this contradicts the minimality of n, whereas if $r_j=0$ for all j then (i) would imply $\cos^n t=0$, which is clearly not the case.

(c) For any (single indeterminate) x the singleton $\{x\}$ is a transcendence base for $E(x)$ over E. To see this[9] let $q(x)/r(x)\in E(x)$ be arbitrary, where $q(x),r(x)\in E[x]$, and let $p(t_1,t_2)=r(t_1)t_2-q(t_1)\in E[t_1,t_2]$. Then from

$$p(x,q(x)/r(x))=r(x)\cdot q(x)/r(x)-q(x)=q(x)-q(x)=0$$

we see that $\{x,q(x)/r(x)\}$ is algebraically dependent, and the result follows.

One can also see from this example that a transcendence base for F over E need not be a vector space basis for F over E. Indeed, the collection $\{1,x,x^2,x^3,\ldots\}\subset E(x)$ is linearly independent over E, and any such basis must therefore be infinite.

(d) Let $A\supset B$ be an extension of commutative rings with unities. In algebraic number theory an element $a\in A$ is said to be *integral* over B if a is a zero of a monic polynomial with coefficients in B. Any such a is automatically algebraically dependent on B (take $T=\emptyset$), but the converse is false. For example, for $A=\mathbb{Q}$ and $B=\mathbb{Z}$ one sees that $1/2\in\mathbb{Q}$ is algebraically dependent over $\mathbb{Z}$, but is not integral over $\mathbb{Z}$.

Proposition 4.2 : *Suppose $S\subset R$ is algebraically dependent over E and $f:R\to M$ is a E-algebra homomorphism into a ring containing E. Then $f(S)\subset M$ is algebraically dependent over E.*

Proof : By assumption there is a positive integer n, a non-zero polynomial $p(x)=p(x_1,x_2,\ldots,x_n)\in E[x]$, and elements $s_1,s_2,\ldots,s_n\in S$ such that $p(s_1,s_2,\ldots,s_n)=0$. Since $f:R\to M$ is assumed a E-algebra homomorphism we have $0=f(0)=f(p(s_1,s_2,\ldots,s_n))=p(f(s_1),\ldots,f(s_n))$, and the proposition follows. **q.e.d.**

[9]Here we follow [Hun, Chapter VI, §1, the example on p. 313].

Corollary 4.3 : *Suppose* $f : R \to M$ *is as in the statement of* Proposition 4.2 *and* $T \subset M$ *is algebraically independent over* E. *Then the same is true of* $f^{-1}(T) \subset R$.

Proposition 4.4 : *Suppose* $S \subset F$ *is a non-empty transcendence base for* F *over* E. *Then any element* $\ell \in F$ *is algebraic over* $E(S)$.

> **Proof :** If $\ell \in E(S)$ this is obvious, so assume otherwise.
>
> Since S is maximal w.r.t. algebraic independence over E the subset $S \cup \{\ell\} \subset F$ must be algebraically dependent over E. Specifically, there must be a non-empty collection of elements $t_1, t_2, \ldots, t_n \in S \cup \{\ell\}$ and a polynomial $p(x) = p(x_1, x_2, \ldots, x_n) \in E[x] = E[x_1, x_2, \ldots, x_n]$ such that $p(t) := p(t_1, t_2, \ldots, t_n) = 0$. Note that $\ell \in \{t_1, t_2, \ldots, t_n\}$; otherwise the algebraic independence of S is contradicted. By relabeling (if necessary) we may assume $\ell = t_n$. If we subsequently re-express $p(x)$ in the form $\sum_j q_j(x_1, x_2, \ldots, x_{n-1}) x_n^j$ the condition that $p(t) = 0$ then becomes $\sum_j q_j(t_1, t_2, \ldots, t_{n-1}) \ell^j = 0$, and ℓ is therefore a zero of the polynomial $q(x) := \sum_j q_j(t_1, t_2, \ldots, t_{n-1}) x^j \in E(S)[x]$. From the algebraic independence condition on S we see that $q_j(t_1, t_2, \ldots, t_{n-1}) \neq 0$ for all j, hence that $0 \neq q(x) \in E(S)[x]$, and the proof is complete. **q.e.d.**

Theorem 4.5 : *Suppose* $T \subset F$ *is a subset such that* $F \supset E(T)$ *is algebraic and* $S \subset T$ *is a subset which is algebraically independent over* E. *Then there is a transcendence base* B *of* F *over* E *satisfying* $S \subset B \subset T$.

> **Proof :** This formulation of the existence of transcendence bases appears (using different notation) as Theorem 1.1 on pages 356-7 of [Lang, Chapter VIII, §1], but the proof which accompanies that statement falls far short of establishing the complete result. One can construct a complete proof from [Z-S, Chapter II, §12, pp. 95-102]. (See, in particular, Corollary 2, p. 99 of that reference.) **q.e.d.**

Corollary 4.6 : *When the field extension $F \supset E$ is not algebraic the following assertions hold:*

(a) *there is an element $s \in R$ which is transcendental over E;*

(b) *for any element $s \in R$ as in* (a) *there is a transcendence base of F over E which contains s and is contained within R;*

(c) *there is a transcendence base of F over E contained within R;*

(d) *if $S \subset F$ is any set such that F is algebraic over $E(S)$ then S contains a transcendence base of F over E; and*

(e) *if the set S in* (d) *generates F, i.e. if $F = E(S)$, then S contains a transcendence base of $E(S)$ over E.*

A special case of (c) is found in [G, Appendix A, Corollary A.0.23, p. 173].

Proof :

(a) By assumption there is an element $t \in F \setminus E$ which is transcendental over E. If $t \in R$ then $s := t$ will satisfy our requirements; otherwise choose $r_1, r_2 \in R$ such that $t = r_1/r_2$. This gives $r_2 t - r_1 = 0$, from which we see that t is algebraic over $E(r_1, r_2)$. If both r_1 and r_2 are algebraic over E then (by a standard result on algebraic extensions) t must also be algebraic over E, thereby contradicting the transcendency of t over E. At least one of r_1 and r_2 is therefore transcendental over E, and a choice for an s as asserted in (a) now becomes evident.

(b) Take $S = \{s\}$ and $T = R$ in Theorem 4.5.

(c) By (a) and (b).

(d) If $E(S)$ is algebraic over E the same is true of F over E by the transitivity of algebraic extensions. $E(S)$ therefore contains at least one element $t \in E(S)$ which is transcendental over E. But t can be expressed as a quotient $p(s_1, s_2, \ldots, s_r)/q(s_1, s_2, \ldots, s_r)$, where $p(x), q(x) \in E[x_1, x_2, \ldots, x_r]$ and $s_1, s_2, \ldots, s_r \in S$. If all the s_j are algebraic over E it would follow that the same is true of t, thereby contradicting the choice of t. S therefore contains an element s_0 transcendental over E. Assertion (d) now results from Theorem 4.5 with $\{s_0\}$ and S assuming the roles of S and T in that statement.

(e) This is a(n important) special case of (d).

q.e.d.

Corollary 4.7 : *If $F \supset R$ is algebraic then R contains a transcendence base for F over E.*

Any such transcendence base will be called a *transcendence base for* (or *of*) R *over* E.

The hypothesis of Theorem 4.5 that F is algebraic over $E(T)$ can appear in different forms. For our purposes condition (c) of the following statement will prove useful.

Proposition 4.8 : *For any non-empty subset $T \subset R$ the following statements are equivalent:*

(a) *F is algebraic over $E(T)$;*

(b) *each $\ell \in F$ is algebraically dependent on T over E; and*

(c) *each $r \in R$ is algebraically dependent on T over E.*

Kaplansky makes implicit use of this result in [Kap, Chapter V, the proof of Lemma 5.3, p. 34].

Proof :

(a) $\Rightarrow$ (b) : Pick any $\ell \in F \setminus T$. By assumption there is a positive integer n and a polynomial $p(x) = x^n + p_{n-1}(T)x^{n-1} + \cdots + p_0(T) \in E(T)[x]$ such that $p(\ell) = 0$. Each of the coefficients $p_j(T)$ is a quotient $r_j(T)/s_j(T)$ of polynomials in $E[T]$, and since each of these polynomials involves only finitely many elements of T we can assume that each is a polynomial in variables $t_1, t_2, \ldots, t_m$ belonging to a common finite (ℓ-dependent) subset $\{t_1, t_2, \ldots, t_m\} \subset T$. We therefore assume, for the remainder of this portion of the proof, that $T = \{t_1, t_2, \ldots, t_m\}$, and we write T as t accordingly. We then have

(i) $$\ell^n + \textstyle\sum_{j=0}^{n-1} \frac{r_j(t)}{s_j(t)} \ell^j = 0,$$

where the $r_j(t)$ and $s_j(t)$ are polynomials with coefficients in E. Multiplying (i) by the product of the denominators then makes evident a polynomial in $E[T][x]$ which is satisfied by ℓ, thereby establishing (b).

(b) $\Rightarrow$ (c) : Obvious from $R \subset F$.

(c) $\Rightarrow$ (a) : (The beginning of this portion of the proof shares similarities with that of Corollary 4.6(a).) Choose any $\ell \in F$ and write ℓ as r_1/r_2, where $r_1, r_2 \in R$. From $r_2\ell - r_1 = 0$ we see that ℓ is algebraic over $E(r_1, r_2)$, and ℓ is therefore algebraic over $E(T)(r_1, r_2)$. On the other hand, from (c) we see that each of r_1 and r_2 is algebraic over $E(T)$, and the extension $E(T)(r_1, r_2) \supset E(T)$ is therefore algebraic. The element $\ell \in F$ is therefore algebraic over $E(T)$, and (a) follows.

q.e.d.

Proposition 4.9 : *Suppose $S \subset R$ is a transcendence base for F over E, A is an integral domain containing E, and $f : R \to A$ is a surjective E-algebra homomorphism. Then $f(S) \subset A$ contains a transcendence base for A over E.*

Proof : Choose any $t \in A \setminus f(S)$. We claim that t (when considered an element of the quotient field of A) is algebraic over $E(f(S))$.

To prove this invoke the surjectivity hypothesis to choose a pre-image $r \in R \setminus S$ of t. Since S is a transcendence base for F over E, the element r must be algebraic over $E(S)$ by Proposition 4.4, hence algebraically dependent on S over E by Proposition 4.8(c). As a result there is a polynomial $p(x_0, x_1, \ldots, x_n) \in E[x_0, x_1, \ldots, x_n]$ and elements $s_1, s_2, \ldots, s_n \in S$ such that

$$p(r, s_1, s_2, \ldots, s_n) = 0.$$

Applying f then gives

$$p(f(r), f(s_1), f(s_2), \ldots, f(s_n)) = p(t, f(s_1), f(s_2), \ldots, f(s_n)) = 0,$$

showing that t is algebraically dependent on $f(S)$ over E, whereupon from a second appeal to Proposition 4.8 we conclude that t (when considered as an element of the quotient field of A) is algebraic over E.

The result is now immediate from Corollary 4.6(d). **q.e.d.**

We next review the definition of the transcendence degree of a field extension and establish a slight generalization (used by Kaplansky).

Theorem 4.10 : *Any two transcendence bases for F over E have the same cardinality.*

Proof : See, e.g. [Z-S, Chapter II, §12, Theorem 25, p. 99]. **q.e.d.**

The cardinality of a (and therefore any) transcendence base for F over E is called the *transcendence degree of F over E,* and will be denoted[10]

$$\operatorname{tr\,deg}_E(F). \tag{4.11}$$

Of course one has

$$\operatorname{tr\,deg}_E(F) = 0 \quad \Leftrightarrow \quad \text{the field extension } F \supset E \text{ is algebraic.} \tag{4.12}$$

Corollary 4.13 : *Any two transcendence bases for R over E have the same cardinality.*

> **Proof :** By definition a transcendence basis for R over E must be a transcendence basis for F over E, and by Theorem 4.10 any two such transcendence bases have the same cardinality. **q.e.d.**

This cardinal appearing in Corollary 4.13 is called the *transcendence degree of R over E* and is denoted $\operatorname{tr\,deg}_E(R)$. One therefore has

$$\operatorname{tr\,deg}_E(R) := \operatorname{tr\,deg}_E(F). \tag{4.14}$$

Finite transcendence degrees play an important role in the proof of Kolchin's theorem. The following result provides examples of extensions with this property.

Proposition 4.15 : *Suppose r is a positive integer and $f_1, f_2, \ldots, f_r$ are elements of F. Then the transcendence degree of $E(f_1, f_2, \ldots, f_r)$ over E is finite, as is the transcendence degree of $E[f_1, f_2, \ldots, f_r]$ over E.*

> **Proof :** For the initial assertion take $T := \{f_1, f_2, \ldots, f_r\}$ in Theorem 4.5 to conclude that $\operatorname{tr\,deg}_E(E(f_1, f_2, \ldots, f_r)) \leq r < \infty$. The second assertion is seen from the first by replacing R and F by $E[f_1, f_2, \ldots, f_r]$ and $E(f_1, f_2, \ldots, f_r)$ respectively in (4.14). **q.e.d.**

[10] The notation used for transcendence degrees varies from author to author. Kolchin and Kaplansky would write $\operatorname{tr\,deg}_E(F)$ as $\partial F/E$ (e.g. see [Kap, Chapter V, §21, p. 35]).

Proposition 4.16 : *Suppose* $\operatorname{tr\,deg}_E(R)$ *is non-zero and finite,* $s \in R$ *is transcendental over* E*,* A *is an integral domain extending* E*, and* $f : R \to A$ *is a* E*-algebra epimorphism satisfying* $f(s) = 0$*. Then*

(i) $$\operatorname{tr\,deg}_E(A) < \operatorname{tr\,deg}_E(R).$$

Proof : By Corollary 4.6(b) we can extend $\{s\}$ to a transcendence base $S = \{s, s_1, s_2, \ldots, s_n\}$ of R over E, and by Proposition 4.9 the set $f(S) \subset A$ must contain a transcendence base for A over E. Since $f(s) = 0$ and a transcendence base cannot contain 0 (or, for that matter, any other element of E), inequality (i) follows. **q.e.d.**

Corollary 4.17 : *Suppose* $\operatorname{tr\,deg}_E(R)$ *is non-zero and finite,* A *is an integral domain extending* E*, and* $f : R \to A$ *is a* E*-algebra epimorphism with non-trivial kernel. Then*

(i) $$\operatorname{tr\,deg}_E(A) < \operatorname{tr\,deg}_E(R).$$

This is [Kap, Chapter V, §20, Lemma 5.3, p. 34].

Proof : We claim that any non-zero element $s \in \ker f$ is transcendental over E. Otherwise there is a positive integer n and elements $e_j \in E$, $j = 0, 1, \ldots, n-1$, such that

$$s^n + \textstyle\sum_{j=0}^{n-1} e_j s^j = 0.$$

By expressing this as

$$e_0 = -s^n - \textstyle\sum_{j=1}^{n-1} e_j s^j = s \cdot \big(- s^{n-1} - \sum_{j-1}^{n-1} e_j s^{j-1} \big)$$

and using the fact that $\ker f$ is an ideal we see that $e_0 \in \ker f$, hence that $1 = e_0^{-1} e_0 \in \ker f$, which is clearly impossible. Since $A \simeq R/\ker f$, the result is now immediate from Proposition 4.16. **q.e.d.**

We end this section by recording the following standard property of transcendence degrees.

Proposition 4.18 (Additivity of Transcendence Degrees): *When* $M \supset F$ *is any field extension and both* $\operatorname{tr\,deg}_F(M)$ *and* $\operatorname{tr\,deg}_E(F)$ *are finite the same is true of* $\operatorname{tr\,deg}_E(M)$*, and one has*

$$\operatorname{tr\,deg}_E(M) = \operatorname{tr\,deg}_F(M) + \operatorname{tr\,deg}_E(F).$$

Proof : See, e.g. [Z-S, Chapter II, §12, Theorem 26, p. 100]. **q.e.d.**

5. Miscellany Involving Constants

In this section $M \supset L$ *is a differential field extension.*

We begin with a standard result on elements algebraic over L_C and a simple consequence which will prove important in our later work.

Proposition 5.1 : *A constant* $c \in M_C$ *is algebraic over* L *if and only if it is algebraic over* L_C*.*

Proof : To avoid trivialities we assume $c \neq 0$.

$\Rightarrow$ By assumption there is a minimal positive integer n for which there exist elements $\ell_0, \ell_1, \ldots, \ell_{n-1} \in L,$ at least one of which is non-zero, such that

$$\text{(i)} \qquad 0 = c^n + \textstyle\sum_{j=0}^{n-1} \ell_j c^j.$$

Differentiating this equality gives

$$\begin{aligned} 0 &= (c^n)' + \textstyle\sum_{j=0}^{n} (\ell_j c^j)' \\ &= nc^{n-1}c' + \textstyle\sum_{j=0}^{n-1} (j\ell_j c^{j-1}c' + \ell_j' c^j) \\ &= 0 + \textstyle\sum_{j=0}^{n-1} (0 + \ell_j' c^j) \quad (\text{because } c \in M_C) \\ &= \textstyle\sum_{j=0}^{n-1} \ell_j' c^j. \end{aligned}$$

From the minimal property of n in (i) we conclude that $\ell_j' = 0$ for $j = 0, 1, \ldots, n,$ hence that $\ell_j \in L_C$ for all such j.

$\Leftarrow$ Obvious. (If the ℓ_j appearing in (i) belong to L_C they also belong to L.)

q.e.d.

Corollary 5.2 : *Suppose* r *is a positive integer and* $c_1, c_2, \ldots, c_r \in M_C$ *are algebraic over* L*. Then* $c_1, c_2, \ldots, c_r$ *are algebraic over* L_C*. More generally, one has both*

$$\text{(i)} \qquad \operatorname{tr\,deg}_L(L(c_1, c_2, \ldots, c_r)) = \operatorname{tr\,deg}_{L_C}(L_C(c_1, c_2, \ldots, c_r)) = 0$$

and

$$\text{(ii)} \qquad \operatorname{tr\,deg}_{L_C}(L) = \operatorname{tr\,deg}_{L_C(c_1, c_2, \ldots, c_r)}(L(c_1, c_2, \ldots, c_r))$$

when the transcendence degrees in (ii) *are finite.*

Proof : The argument is by induction on r.

When $r = 1$ we see from (4.12) and Proposition 5.1 that

$$\begin{aligned} 0 = \operatorname{tr\,deg}_L(L(c_1)) &\Leftrightarrow c_1 \text{ is algebraic over } L \\ &\Leftrightarrow c_1 \text{ is algebraic over } L_C \\ &\Leftrightarrow 0 = \operatorname{tr\,deg}_{L_C}(L_C(c_1)). \end{aligned}$$

Equality (i) therefore holds for $r = 1$. Equality (ii) then follows (for $r = 1$) from the additivity of transcendence degrees (Proposition 4.18) and the commutativity of the diagram

$$\begin{array}{ccccc} & & L(c_1) & & \\ & \overset{0}{\nearrow} & & \nwarrow & \\ L & & & & L_C(c_1) \\ & \nwarrow & & \overset{0}{\nearrow} & \\ & & L_C & & \end{array}$$

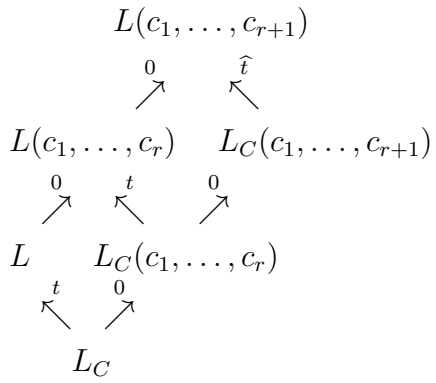
of field inclusions, wherein the $0s$ denote transcendence degrees.

Now assume $r \geq 1$ and that the results hold for any choice of at most r constants $c_j \in M_C$. Choose any $c_1, c_2, \ldots, c_{r+1} \in M_C$, each algebraic over L. Then (i) and (ii) hold, and we therefore have a commutative diagram

$$\begin{array}{ccccc} & & L(c_1, \ldots, c_r) & & \\ & \overset{0}{\nearrow} & & \overset{t}{\nwarrow} & \\ L & & & & L_C(c_1, \ldots, c_r) \\ & \overset{t}{\nwarrow} & & \overset{0}{\nearrow} & \\ & & L_C & & \end{array}$$

of field inclusions, wherein the 0 and t represent the associated transcendence degrees. Since c_{r+1} is algebraic over L it must be algebraic over L_C by Proposition 5.1, and therefore algebraic over both $L(c_1, \ldots, c_r)$ and $L_C(c_1, \ldots, c_r)$. We can therefore extend this last commutative dia-

gram to the commutative diagram



Using the additivity of transcendency degrees on the upper right square we see that $\widehat{t} = t$, hence that (ii) holds when n is replaced by $n+1$, and using that same result on the upper left and lower right diagonal compositions we see that (i) holds when r is replaced by $r+1$.

The corollary is thereby established. **q.e.d.**

Proposition 5.3 : *Suppose $M \supset L$ is a differential field extension, r is a positive integer, and $c_1, c_2, \ldots, c_r \in M_C$ are algebraically independent over L. Then*

(i) $$\big(L(c_1, c_2, \ldots, c_r)\big)_C = L_C(c_1, c_2, \ldots, c_r).$$

Proof : To ease notation in the proof we write $(c_1, c_2, \ldots, c_r)$ as c.

From $L_C \subset L$ we have $L_C(c) \subset \big(L(c)\big)_C$. To establish (i) it therefore suffices to verify that

(ii) $$\big(L(c)\big)_C \subset L_C(c).$$

We first prove that

(iii) $$\big(L[c]\big)_C = L_C[c].$$

As above, it is enough to establish the inclusion

$$\big(L[c]\big)_C \subset L_C[c].$$

Since $c_1, c_2, \ldots, c_r$ are algebraically independent over L any $m \in L[c]$ can be uniquely represented as a finite sum $m = \sum_i \ell_i \widetilde{c}_i$ wherein $\ell_i \in L$

and $\widetilde{c}_i$ is a product of non-negative powers of the various c_j. When $m \in \big(L[c]\big)_C$ we see from the assumption that the c_j are constants that differentiation yields

$$\text{(iv)} \qquad \begin{cases} 0 &= m' \\ &= \sum_i (\ell_i \widetilde{c}_i)' \\ &= \sum_i (\ell_i \widetilde{c}_i' + \ell_i' \widetilde{c}_i) \\ &= \sum_i (\ell_i \cdot 0 + \ell_i' \widetilde{c}_i) \\ &= \sum_i \ell_i' \widetilde{c}_i, \end{cases}$$

By uniqueness we conclude that $\ell_i' = 0$ for all i, hence that $\ell_i \in L_C$, and (iii) follows.

Now suppose $m = u/v \in \big(L(c)\big)_C$, where $u, v \in L[c]$. Then from

$$0 = m' = \frac{vu' - v'u}{v^2}$$

we see that $vu' - v'u = 0$. But this would be a dependence relation on c if $u' \neq 0$ and/or $v' \neq 0$, thereby contradicting the algebraic independence assumption on $c_1, c_2, \ldots, c_r$. This gives $u, v \in \big(L[c]\big)_C$, whence $u, v \in L_C[c]$ by (iii), and (ii) is thereby established. **q.e.d.**

6. A Preliminary Involving Field Extension Bases

In this section $F \supset E$ *is an extension of* (not necessarily differential) *fields.*

A good deal of Kolchin's arguments rest on the following simple observation, which we formulate in a manner inspired by Kaplansky. In contemporary terms the statement would most likely involve tensor products, but these entities are not assumed familiar to readers.

Proposition 6.1 : *Let* $\{x_1, x_2, \ldots, x_r\}$ *be algebraically independent elements over* F *and let* $\mathbf{b} = (b_\omega)$ *be a* (vector space) *basis of* F *over* E*. Then any polynomial in* $F[x] := F[x_1, x_2, \ldots, x_r]$ *has a unique expression as a finite linear combination of elements of* $\mathbf{b}$ *having polynomials in* $E[x]$ *as coefficients.*

Proof : Choose any polynomial

$$\text{(i)} \qquad p(x) = \textstyle\sum_m f_m x^m \in F[x],$$

where $m := (m_1, m_2, \ldots, m_r) \in \mathbb{N}^r$ and $x^m := x_1^{m_1} x_2^{m_2} \cdots x_r^{m_r}$. By assumption we can write each scalar f_m in the form

$$\text{(ii)} \qquad f_m = \textstyle\sum_j e_{mj} b_{mj}, \qquad \text{where} \qquad e_{mj} \in E \qquad \text{and} \qquad b_{mj} \in \mathbf{b}.$$

Since there are at most finitely many non-zero coefficients f_m appearing in (i), and since there are only finitely many b_{mj} involved with each f_m, the union of the collections $\{b_{mj}\}$ is finite. To ease notation we express this union as $\{b_1, b_2, \ldots, b_s\}$, thereby enabling us to rewrite (ii) as

$$f_m = \textstyle\sum_j \widetilde{e}_{mj} b_j, \qquad \widetilde{e}_{mj} \in E, \qquad b_1, \ldots, b_s \in \mathbf{b}.$$

From (i) we then have

$$\begin{aligned} p(x) &= \textstyle\sum_m f_m x^m \\ &= \textstyle\sum_m \big(\sum_j \widetilde{e}_{mj} b_j \big) x^m \\ &= \textstyle\sum_j \big(\sum_m \widetilde{e}_{mj} x^m \big) b_j, \end{aligned}$$

and this gives the existence of an expression as required.

If some $p(x) \in F[x]$ can be expressed, as stated, in two distinct ways, then by subtracting we can represent the polynomial 0 in the form

$$0 = \textstyle\sum_j \left(\sum_m \widehat{e}_{,mj} x^m \right) b_j,$$

wherein

(iii) $\widehat{e}_{mj} \neq 0$ for at least one index mj.

It follows that

$$\begin{aligned} 0 &= \textstyle\sum_j \left(\sum_m \widehat{e}_{mj} x^m\right) b_j \\ &= \textstyle\sum_m \left(\sum_j \widehat{e}_{mj} b_j\right) x^m. \end{aligned}$$

Since 0 is the zero polynomial this forces $\sum_j \widehat{e}_{mj} b_j = 0$ for all m, and since $\mathbf{b}$ is a basis of F over E this in turn forces $\widehat{e}_{mj} = 0$ for all mj, thereby contradicting (iii). **q.e.d.**

7. Dependence over Constants

We begin this section with a standard result having ramifications which, in the experience of this author, tend to be vastly under appreciated.

Proposition 7.1 : *Let L be a differential field and let $\ell_1, \ell_2, \ldots, \ell_n \in L$. Then $\ell_1, \ell_2, \ldots, \ell_n$ are:*

(a) *linearly dependent over L_C if and only if the Wronskian determinant*

$$W(\ell_1, \ell_2, \ldots, \ell_n) = \det \begin{bmatrix} \ell_1 & \ell_2 & \cdots & \ell_{n-1} & \ell_n \\ \ell_1' & \ell_2' & \cdots & \ell_{n-1}' & \ell_n' \\ \vdots & & & & \vdots \\ \ell_1^{(n-1)} & \ell_2^{(n-1} & \cdots & \ell_{n-1}^{(n-1)} & \ell_n^{(n-1)} \end{bmatrix}$$

is zero;

(b) *linearly independent over L_C if any only if the Wronskian determinant $W(\ell_1, \ell_2, \ldots, \ell_n)$ does not vanish.*

Proof :

(a) See, e.g. [Kap, Chapter III, §10, Theorem 3.7, p. 21].

(b) Immediate from (a).

q.e.d.

Corollary 7.2 : *The vanishing or non-vanishing of the Wronskian of any n elements of a differential field is independent of the choice of the field. More precisely, suppose $\ell_1, \ell_2, \ldots, \ell_n$ are elements of the intersection of two differential fields L and M, with the associated derivations coinciding on that intersection. Then the following statements are equivalent:*

(a) *$\ell_1, \ell_2, \ldots, \ell_n$ are linearly dependent* (resp. *linearly independent*) *over L_C;*

(b) *$\ell_1, \ell_2, \ldots, \ell_n$ are linearly dependent* (resp. *linearly independent*) *over M_C;*

(c) $W(\ell_1, \ell_2, \ldots, \ell_n) = 0$ (resp. $\neq 0$).

To indicate that any (and therefore all) of (a)-(c) holds one says that "*$\ell_1, \ell_2, \ldots, \ell_n$ are linearly dependent* (resp. *independent*) *over constants.*"

Corollary 7.3 : *Suppose* $M \supset L$ *is a differential field extension,* r *is a positive integer,* $t = (t_1, t_2, \ldots, t_r)$ *are* (ordinary) *indeterminates over* M*, and* $c_1, c_2, \ldots, c_r$ *are distinct elements of* M_C*. The the following results hold:*

(a) *for any polynomial* $q(t) = q(t_1, t_2, \ldots, t_r) \in L_C[t] = L_C[t_1, t_2, \ldots, t_r]$ *one has* $q(c_1, c_2, \ldots, c_r) \in M_C$*;*

(b) *the collection* $\{c_1, c_2, \ldots, c_r\}$ *is algebraically dependent over* L *if and only if it is algebraically dependent over* L_C*; and*

(c) *the collection* $\{c_1, c_2, \ldots, c_r\}$ *is algebraically independent over* L *if and only if it is algebraically in independent over* L_C*.*

Item (b) is Lemma 5.2 of Kaplansky [Kap, Chapter V, §20, p. 33]. His proof [pp. 33-4] covers less than four lines.

Proof :

(a) The coefficients of the polynomial $q(t)$ are by hypothesis in $L_C \subset M_C$, and by assumption we have $c_1, c_2, \ldots, c_r \in M_C$.

(b) Since $L_C \subset L$ the converse implication is obvious; only the forward implication requires a proof.

By the definition of "algebraically dependent" there is a non-zero polynomial $p(t) = p(t_1, t_2, \ldots, t_r) \in L[t]$ such that $p(\ell) := p(c_1, c_2, \ldots, c_r) = 0$. Choose a vector space basis $\mathbf{b} = (b_\omega)$ for L over L_C. By Proposition 6.1 we can write $p(t)$ as a finite sum $\sum_j q_{b_{\omega_j}}(t) b_{\omega_j}$, wherein each $q_{b_{\omega_j}}(t) \in L_C[t]$ and at least one of these polynomial coefficients is non-zero. We therefore have

$$\text{(i)} \qquad 0 = p(c_1, c_2, \ldots, c_r) = \textstyle\sum_j q_{b_{\omega_j}}(c_1, c_2, \ldots, c_r) b_{\omega_j}.$$

From item (a) we see that each of the coefficients $q_{b_{\omega_j}}(c_1, c_2, \ldots, c_r)$ appearing in (i) belongs to M_C.

Since $\mathbf{b} = (b_\omega)$ is a basis of L over L_C the finite collection $(b_{\omega_j})_j$ must be linearly independent over L_C. It then follows from Corollary 7.2 that the collection $(b_{\omega_j})_j$ is linearly independent over M_C. From the claim of the previous paragraph and (i) we conclude that $q_{b_{\omega_j}}(c_1, c_2, \ldots, c_r) = 0$ for all b_{ω_j}. Since at least one of the $q_{b_{\omega_j}}(t)$ is non-zero, (b) is thereby established.

(c) Immediate from (b).

q.e.d.

Corollary 7.4 : *Let $M \supset L$ be a differential field extension, let m be a positive integer, and let $c_1, c_2, \ldots, c_m$ be distinct elements of M_C. Then*

(i) $$\operatorname{tr\,deg}_L L(c_1, c_2, \ldots, c_m) = \operatorname{tr\,deg}_{L_C} L_C(c_1, c_2, \ldots, c_m).$$

This is the final assertion in [Kol$_1$, Chapter II, §14, Theorem 2, p. 26].

Proof : If all c_j are algebraic over L the result is simply restates (i) of Corollary 5.2 (with K and L in that statement replaced by L and M respectively). We therefore assume at least one c_j is transcendental over L.

By (e) of Corollary 4.6 the set $c = \{c_1, c_2, \ldots, c_m\}$ contains a transcendence base $c_{\rm tb}$ for $L(c) \supset L$, which by re-indexing (if necessary) we may assume is of the form $\{c_1, c_2, \ldots, c_r\}$ for some positive integer $r \leq m$. Since $c_{\rm tb}$ is algebraically independent over L it must also be algebraically independent over L_C (by Corollary 7.3(b)), and we therefore have

(ii) $$r = \operatorname{tr\,deg}_L(L(c)) \leq \operatorname{tr\,deg}_{L_C}(L_C(c)).$$

If the inequality in (ii) is strict choose $S = c_{\rm tb}$ and $T = c$ in Theorem 4.5 to produce a transcendence base $\widehat{c}_{\rm tb} \subset c$ for $L_C(c) \supset L_C$ which properly contains $c_{\rm tb}$. By an additional re-indexing (again if necessary) we may assume

$$\widehat{c}_{\rm tb} = \{c_1, c_2, \ldots, c_r, c_{r+1}, \ldots, c_s\} = c_{\rm tb} \cup \{c_{r+1}, \ldots, c_s\}$$

for some positive integer s satisfying $r < s \leq m$. From the definition of a transcendence base the collection $\widehat{c}_{\rm tb}$ must be algebraically independent over L_C, and therefore algebraically independent over L by Corollary 7.3(c). On the other hand, since the set $c_{\rm tb}$ is a transcendence base for $L(c)$ over L the subset $c_{\rm tb} \cup \{c_{r+1}\} \subset \widehat{c}_{\rm tb}$ must be algebraically dependent over L, hence the same must hold for $\widehat{c}_{\rm tb}$, and we have achieved a contradiction. **q.e.d.**

Our final corollary to Theorem 7.1 is crucial to Kolchin's proof of Theorem 1.10.

Corollary 7.5 : *Let M be a differential field, let r be a positive integer, and let $t = (t_1, t_2, \ldots, t_r)$ be* (ordinary) *indeterminates over M. Then the following results hold.*

(a) *Given any subset $\mathcal{Q} \subset M[t]$, one can choose an ideal $\mathcal{J}_\mathcal{Q} \subset M_C[t]$, not uniquely determined by $\mathcal{Q}$, having the following property: for any $c_1, c_2, \ldots, c_r \in M_C$ the r-tuple $c := (c_1, c_2, \ldots, c_r) \in M_C^r$ is a zero of (each element of) $\mathcal{Q}$ if and only if it is a zero of the ideal $\mathcal{J}_\mathcal{Q}$.*

(b) *If $\mathcal{Q} \subset M[t]$ and $\mathcal{J}_\mathcal{Q} \subset M_C[t]$ are related as in* (a) *the same is true for $\mathcal{Q}$ and the radical $\sqrt{\mathcal{J}_\mathcal{Q}}$ of $\mathcal{J}_\mathcal{Q}$.*

(c) *For each subset $\mathcal{Q} \subset M[t]$ and each ideal $\mathcal{J}_\mathcal{Q} \subset M_C[t]$ associated with $\mathcal{Q}$ as in* (a) *there is an ideal $\mathcal{J}_\mathcal{Q}^{\max} \subset M_C[t]$ containing $\mathcal{J}_\mathcal{Q}$ which is maximal under inclusion w.r.t. the conditions on r-tuples $c \in M_C^r$ stated in* (a). *Moreover, any such ideal $\mathcal{J}_\mathcal{Q}^{\max}$ is radical.*

The notation $\mathcal{J}_\mathcal{Q}^{\max}$ is designed to remind readers of the maximal property stated in (c), but could admittedly cause confusion: there is no claim that that this ideal is maximal (differential or otherwise).

This result is extracted from [Kol$_1$, §14, Theorem 2, pp. 26-7]. It is not stated precisely as in that reference, but rather as used at the top of page 30 of that work.

Proof :

(a) It suffices to prove the result when $\mathcal{Q}$ in the statement is replaced by the ideal $(\mathcal{Q}) \subset M[t]$ generated by $\mathcal{Q}$.

By the Hilbert Basis Theorem $(\mathcal{Q})$ is finitely generated, say by $(\mathcal{Q})_{\text{gen}} := \{q_1(t), q_2(t), \ldots, q_u(t)\} \subset (\mathcal{Q})$. (The various $q_j(t)$ may or may not be in $\mathcal{Q}$.)

Choose a (vector space) basis $\mathbf{b} = (b_\omega)$ of M over M_C and let $b_{\omega_1}, \ldots, b_{\omega_s}$ be those basis elements involved in expressing the coefficients of the finitely many $q_i(t)$ as M_C-linear combinations of the elements of $\mathbf{b}$. To ease notation abbreviate b_{ω_j} as b_j, $j = 1, 2, \ldots, v$. By Proposition 6.1 each $q_i(t) \in (\mathcal{Q})_{\text{gen}}$ can be expressed in the form

$$q_i(t) = q_{i1}(t)b_1 + \cdots + q_{it}(t)b_v,$$

wherein $q_{ij}(t) \in M_C[t]$ for $1 \le i \le u$ and $1 \le j \le v$. For any r-tuple $c = (c_1, c_2, \ldots, c_r) \in M_C^r$ we therefore have

$$q_i(c) = q_{i1}(c)b_1 + \cdots + q_{iv}(c)b_v.$$

By Theorem 7.1 the elements $b_1, b_2, \ldots, b_v$ are linearly independent over M_C, and by Corollary 7.3(a) the elements $q_{ij}(c)$ belong to M_C. Thus $q_i(c) = 0$ if and only if all $q_{ij}(c) = 0$. We can therefore take $\mathcal{J}_\mathcal{Q}$ to be the ideal in $M_C[t]$ generated by the finite set $\{q_{ij}(t)\}$.

The non-uniqueness qualification in the statement of (a) is evident from the fact that our construction of $\mathcal{J}_\mathcal{Q}$ involved choosing a vector space basis.

(b) Suppose $c \in M_C^r$. Then

$$\begin{aligned} c \text{ is a zero of each element of } \mathcal{Q} &\Leftrightarrow c \text{ is a zero of } \mathcal{J}_\mathcal{Q} \quad \text{(by (a))} \\ &\Leftrightarrow q(c) = 0 \text{ for all } q(t) \in \mathcal{J}_\mathcal{Q} \\ &\Leftrightarrow p^w(c) = 0 \text{ for each } p(t) \in \sqrt{\mathcal{J}_\mathcal{Q}} \\ &\qquad \text{and some } w = w(p) \in \mathbb{Z}^+ \\ &\Leftrightarrow p(c) = 0 \text{ for all } p(t) \in \sqrt{\mathcal{J}_\mathcal{Q}}. \end{aligned}$$

(c) For a given $\mathcal{J}_\mathcal{Q}$ the existence of a (not necessarily radical) ideal $\mathcal{J}_\mathcal{Q}^{\max}$ with the stated properties is a straightforward application of Zorn's lemma. The radical nature of this maximal element is immediate from (b).

q.e.d.

8. The Main Result

The organization of this section follows that of the initial portion of [Kap, Chapter V, §21, pp. 34-6]: the proof of Theorem 1.10 becomes a special case of a more general result which Kaplansky presents as a lemma [Kap, Chapter V, §21, Lemma 5.4, pp. 34-6].

For ease of reference we offer a quick summary of relevant items from §1 and §3.

We began §1 by introducing a Picard-Vessiot (field) extension $L \supset K$ for a linear (ordinary) differential equation

$$x' = Ax, \tag{8.1}$$

where $A \in \mathfrak{gl}(n, K)$, and a fundamental matrix solution $\alpha \in \mathrm{GL}(n, L)$ for (8.1). We let G denote the associated differential Galois group, and defined a faithful representation $\rho : G \to \mathrm{GL}(n, K_C)$ by

$$\rho : g \in G \mapsto C_g := \alpha^{-1}(g \cdot \alpha) \in \mathrm{GL}(n, K_C). \tag{8.2}$$

Kolchin's theorem (Theorem 1.10) is that the image $\rho(G)$ is an algebraic subgroup of $\mathrm{GL}(n, K_C)$.

In §3 we adjoined a differential field extension $M \supset L = K(\alpha)$ to this mix, not excluding $M = L$ and not assuming $M_C = K_C$, defined Σ as the set of differential embeddings of $K(\alpha)$ into M over K, and established the membership

$$C_\sigma := \alpha^{-1}\sigma(\alpha) \in M_C \qquad \text{for all} \qquad \sigma \in \Sigma. \tag{8.3}$$

We introduced $n \times n$ matrices $x = [x_{ij}]$ and $t = [t_{ij}]$ of indeterminates over M, and used assignments of these indeterminates to define differential algebra homomorphisms as follows.

- $\lambda : K[x] \to K(\alpha) = L$ and λ_α are the differential K-algebra homomorphisms from $K[x]$ to $K(\alpha)$ and $K[\alpha]$ respectively uniquely determined by the assignments

  $$\lambda : x \mapsto \alpha \qquad \text{and} \qquad \lambda_\alpha : x \mapsto \alpha. \tag{8.4}$$

- $\tau : K[x] \to K(\alpha)[t]$ is the differential K-algebra homomorphism uniquely determined by the assignment

  $$\tau : x \mapsto xt. \tag{8.5}$$

- For each $C \in \mathrm{GL}(n, M_C)$ we defined $\gamma_C : M[t] \to M$ to be the differential M-algebra homomorphism uniquely determined by the assignment

$$\gamma_C : t \to C. \tag{8.6}$$

As a result of these definitions we obtained a family of commutative diagrams of differential algebra homomorphisms

$$\begin{array}{ccc} K[x] & \stackrel{\tau}{\longrightarrow} & M[t] \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\gamma_{C_\sigma}} \\ K(\alpha) & \stackrel{\sigma}{\longrightarrow} & M \end{array} , \tag{8.7}$$

one for each $\sigma \in \Sigma$, and verified (as Proposition 3.9) that

$$\ker\lambda = \ker(\gamma_{C_\sigma} \circ \tau) \qquad \text{for all} \qquad \sigma \in \Sigma. \tag{8.8}$$

We extended this family by introducing a "partial diagram"

$$\begin{array}{ccc} K[x] & \stackrel{\tau}{\longrightarrow} & M[t] \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\gamma_C} \\ K(\alpha) & & M \end{array} \tag{8.9}$$

for each $C \in \mathrm{GL}(n, M_C)$, and then restricted attention to those C satisfying

$$\ker\lambda \subset \ker(\gamma_C \circ \tau). \tag{8.10}$$

The key result on this final collection of matrices C was Proposition 3.11, which for convenience we repeat here (with a fresh reference number).

Proposition 8.11 :

(a) *Suppose* $C \in \mathrm{GL}(n, M_C)$ *has the property that*

(i) $$\ker\lambda \subset \ker(\gamma_C \circ \tau).$$

Then there is a unique differential K*-algebra homomorphism* $\kappa_C : K[\alpha] \to K(\alpha)$ *such that the diagram*

(ii) $$\begin{array}{ccc} K[x] & \stackrel{\tau}{\longrightarrow} & M[t] \\ {\scriptstyle\lambda_\alpha}\downarrow & & \downarrow{\scriptstyle\gamma_C} \\ K[\alpha] & \stackrel{\kappa_C}{\longrightarrow} & M \end{array}$$

commutes.

(b) *Any* C *of the form* C_α *satisfies* (i), *and in that case*

(iii) $$\kappa_C = \sigma|_{K[\alpha]}.$$

It also proves convenient to repeat Corollary 3.12 (again with a new reference number).

Corollary 8.12 : *Suppose in* Proposition 8.11 *that the Picard-Vessiot extension* $K(\alpha) \supset K$ *is algebraic. Then* $K[\alpha] = K(\alpha)$, *and* $\kappa_C : K(\alpha) \to M$ *is therefore a differential field embedding over* K.

From this author's perspective the key step in Kolchin's proof is an unexpected geometric characterization of those $C \in \mathrm{GL}(n, M_C)$ for which (i) of Proposition 8.11 holds. His solution will be seen in Proposition 8.20.

Let

$$\mathcal{P} := \ker \lambda \subset K[x], \tag{8.13}$$

and set

$$\mathcal{Q} := \tau(\mathcal{P}) \subset M[t]. \tag{8.14}$$

From (8.4) and (8.5) one sees that an equivalent definition of $\mathcal{Q}$ is

$$\mathcal{Q} := \{\, p(\alpha t) \in M[t] \,:\, p(x) \in K[x] \text{ and } p(\alpha) = 0 \,\}. \tag{8.15}$$

By Corollary 7.5(a) there is an associated ideal[11] $\mathcal{J}_\mathcal{Q} \subset K_C[x]$, not uniquely determined, having the property that for any matrix[12] $C \in \mathrm{GL}(n, M_C)$ one has that

$$C \text{ is a zero of } \mathcal{Q} \quad \Leftrightarrow \quad C \text{ is a zero of } \mathcal{J}_\mathcal{Q}. \tag{8.16}$$

Let

$$\mathcal{V} := \mathcal{V}(\mathcal{J}_\mathcal{Q}) \tag{8.17}$$

[11] At this point we have no need for the radical ideal $\mathcal{J}_\mathcal{Q}^{\max}$ of Corollary 7.5(c), although one could certainly make that choice.

[12] Corollary 7.5 was formulated in terms of n-tuples and what we now write as a matrix $C = [c_{ij}]$ was expressed as $c = (c_1, c_2, \ldots, c_r)$. It was felt that the notation now being introduced might have caused confusion in that more general context.

be the algebraic subset of $\mathrm{GL}(n, K_C)$ defined by $\mathcal{J}_{\mathcal{Q}}$. Then from (8.13)−(8.17) we see that

$$(8.18) \qquad C \in \mathcal{V} \quad \Leftrightarrow \quad p(\alpha C) = 0 \quad \text{for all} \quad p(\alpha t) \in \mathcal{Q} = \tau(\mathcal{P})$$

or, equivalently, that

$$(8.19) \qquad C \in \mathcal{V} \quad \Leftrightarrow \quad p(\alpha C) = 0 \quad \text{for all} \quad p(x) \in \mathcal{P}.$$

The following result ties these ideas to Proposition 2.11.

Proposition 8.20 : *For any* $C \in \mathrm{GL}(n, M_C)$ *the following two statements are equivalent:*

(a) $C \in \mathcal{V}$*; and*

(b) $\ker \lambda \subset \ker(\gamma_C \circ \tau)$.

Proof : For $C \in \mathrm{GL}(n, M_C)$ one has

$$\begin{aligned} C \in \mathcal{V} &\Leftrightarrow p(\alpha C) = 0 \text{ for all } p(x) \in \mathcal{P} && \text{(by (8.19))} \\ &\Leftrightarrow p(x) \in \mathcal{P} \Rightarrow p(\alpha C) = 0 \\ &\Leftrightarrow p(x) \in \mathcal{P} \Rightarrow \gamma_C(p(\alpha t)) = 0 && \text{(by (8.6))} \\ &\Leftrightarrow p(x) \in \mathcal{P} \Rightarrow (\gamma_C \circ \tau)(p(x)) = 0 \\ &\Leftrightarrow p(x) \in \ker \lambda \Rightarrow p(x) \in \ker(\gamma_C \circ \tau) \\ &\Leftrightarrow \ker \lambda \subset \ker(\gamma_C \circ \tau). \end{aligned}$$

q.e.d.

Corollary 8.21 : *To any* $C \in \mathcal{V}$ *there corresponds a unique differential* K*-algebra homomorphism* $\kappa_C : K[\alpha] \to K(\alpha)$ *such that the diagram*

$$\text{(i)} \qquad \begin{array}{ccc} K[x] & \xrightarrow{\tau} & M[t] \\ {\scriptstyle \lambda_\alpha}\downarrow & & \downarrow{\scriptstyle \gamma_C} \\ K[\alpha] & \xrightarrow{\kappa_C} & M \end{array}$$

commutes.

Proof : Recall Proposition 8.11. **q.e.d.**

Theorem 8.22 : *The following results hold.*

(a) *For each* $\sigma \in \Sigma$ *one has* $C_\sigma \in \mathcal{V}$*; and*

(b) *for each* $C \in \mathcal{V}$ *there is a differential embedding* $\sigma : K(\alpha) \to M$ *over* K *such that* $C = C_\sigma$.

Kolchin's theorem (Theorem 1.10) is the case $M = L\ (= K(\alpha))$. This theorem is formulated as a lemma by Kaplansky, but this author feels it deserves a higher status (see [Kap, Chapter V, §21, Lemma 5.4, pp. 34-5]).

Proof :

(a) Use the initial assertion of Proposition 8.11(b) together with the (b) $\Rightarrow$ (a) implication of Proposition 8.20.

(b) For each $C \in \mathcal{V}$ there is, by Proposition 8.11(a), a unique differential K-algebra homomorphism $\kappa_C \to M$ which renders the diagram

$$\begin{array}{ccc} K[x] & \xrightarrow{\tau} & M[t] \\ {\scriptstyle \lambda_\alpha}\downarrow & & \downarrow{\scriptstyle \gamma_C} \\ K[\alpha] & \xrightarrow{\kappa_C} & M \end{array}$$

commutative.

If the extension $K(\alpha) \supset K$ is algebraic then $\kappa_C : K[\alpha] = K(\alpha) \to M$ is a differential field embedding over K by Corollary 3.12, thereby establishing (b). We therefore assume the extension is transcendental, in which case we see from Proposition 4.15 that the transcendence degree must be finite. It suffices to prove, under these additional assumptions, that κ_C is injective: it can then be extended to a field embedding of $\sigma : K(\alpha) \to M$ over K in the usual way, and that would establish (b).

If injectivity fails then

$$\text{(i)} \qquad \operatorname{tr\,deg}_K(K(\alpha)) > \operatorname{tr\,deg}_K(K(\alpha C))$$

by (4.14) and Corollary 4.17. Let

$$\text{(ii)} \qquad K(\alpha, \alpha C) = K(\alpha)(C) = K(\alpha C, C)$$

denote the subfield[13] of M generated by α and αC. (Recall that $C \in \mathrm{GL}(n, M_C)$, whereas $C \in \mathrm{GL}(n, L_C) = \mathrm{GL}(n, K_C)$ is not necessarily

[13] $K(\alpha, \alpha C)$ is in fact a differential subfield of M, as can be seen from the fact that both α and αC are fundamental matrix solutions of (8.1). This additional structure is not required in this proof.

the case.) From a second appeal to Proposition 4.15 we see that the transcendence degree of $K(\alpha, \alpha C)$ over K is finite, whereupon from (i), the diagram

$$\begin{array}{ccc} & K(\alpha, \alpha C) & \\ \nearrow & & \nwarrow \\ K(\alpha) & & K(\alpha C) \\ \nwarrow & & \nearrow \\ & K & \end{array}$$

and the additivity of transcendence degrees (Proposition 4.18) we find that

$$\operatorname{tr\,deg}_{K(\alpha)}(K(\alpha, \alpha C)) < \operatorname{tr\,deg}_{K(\alpha C)}(K(\alpha, \alpha C)).$$

Now check that

$$\begin{array}{rcll} \operatorname{tr\,deg}_{K(\alpha)}(K(\alpha, \alpha C)) & = & \operatorname{tr\,deg}_{K(\alpha)}(K(\alpha)(C)) & \text{(by (ii))} \\ & = & \operatorname{tr\,deg}_{K(\alpha)_C}(K(\alpha)_C(C)) & \text{(by Corollary 7.4)} \\ & = & \operatorname{tr\,deg}_{L_C}(L_C(C)) & \text{(because } K(\alpha) = L\text{)} \\ & = & \operatorname{tr\,deg}_{K_C}(K_C(C)) & \text{(because } L_C = K_C\text{),} \end{array}$$

and as a result that

(iii) $$\operatorname{tr\,deg}_{K_C}(K_C(C)) < \operatorname{tr\,deg}_{K(\alpha C)}(K(\alpha, \alpha C)).$$

Next check that

$$\begin{array}{rcll} \operatorname{tr\,deg}_{K(\alpha C)}(K(\alpha, \alpha C)) & = & \operatorname{tr\,deg}_{K(\alpha C)}(K(\alpha C, C)) & \text{(by (ii))} \\ & = & \operatorname{tr\,deg}_{K(\alpha C)_C}(K(\alpha C)_C(C)) & \text{(by Corollary 7.4),} \end{array}$$

which by (iii) gives

(iv) $$\operatorname{tr\,deg}_{K_C}(K_C(C)) < \operatorname{tr\,deg}_{K(\alpha C)_C}(K(\alpha C)_C(C)).$$

Now consider the (commutative) diagram of inclusions

$$\begin{array}{ccc} & K(\alpha C)_C(C) & \\ \nearrow & & \nwarrow \\ K(\alpha C)_C & & K_C(C) \\ \nwarrow & & \nearrow \\ & K_C & \end{array}$$

From (iv) and the additivity of transcendence degrees it must be the case that

$$\text{tr deg}_{K_C}(K(\alpha C)_C) < \text{tr deg}_{K_C(C)}(K(\alpha C)_C(C)),$$

whereas by Corollary 5.2 these last two transcendence degrees must be equal. We have achieved a contradiction. **q.e.d.**

Acknowledgments

I would like to thank Dr. Phyllis Cassidy of the City College of New York for numerous conversations on this material, and for straightening me out on several serious misconceptions. Any errors which remain are my responsibility.

The talk is only a minor modification of that given to the Department of Mathematics and Statistics at the University of Calgary on 20 August 2014. I would like to thank Drs. Karen Seyffarth and Kristine Bauer of that department for arranging that presentation.

Notes and Comments

Commutative diagrams were not standard when [Kol$_2$] and [Kap] were published, but they are immediately evident to contemporary readers. For example, in the paragraph labeled (1) in the proof of [Kap, Chapter V, §21, Lemma 5.4, pp. 34-5] Kaplansky writes[14]: "Perform the homomorphism from $K[x]$ to $K(\alpha)$ followed by g ... (and then) ... take the mapping given by $x \mapsto \alpha t$ followed by t maps to C. ... The product is the same ... ."

On a different matter: Kaplansky asserts, using different notation[15], that the set $\mathcal{Q}$ introduced in (8.14) is an ideal (I assume of $M[t]$) (see [Kap, Chapter V, §21, line 8 of p. 35]). I have serious doubts about that. Up to that point Kaplansky seems to be following Kolchin's arguments, but Kolchin never makes such a statement.

[14] I have changed his notation, but nothing else.

[15] His notation for my $\mathcal{Q}$ is Δ.

References

[C] R.C. Churchill, *A Geometric Approach to Linear Ordinary Differential Equations*, posted on the website of the Kolchin Seminar on Differential Algebra, 13 October 2006.

[G] D.M. Goldschmidt, *Algebraic Functions and Projective Curves*, GTM 215, Springer, New York, 2003.

[Hun] T.W. Hungerford, *Algebra*, GTM 73, Springer-Verlag, New York, 1974.

[Kap] I. Kaplansky, *An Introduction to Differential Algebra*, Second Edition, Revised, Corrected and Enlarged, Paris, Hermann, 1976.

[Kol_1] E.R. Kolchin, Algebraic matric groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations, *Ann. of Math.* **49** (1948), 1-42.

[Kol_2] E.R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973.

[Lang] S. Lang, *Algebra*, Revised Third Edition, Springer, New York, 2002.

[vdW] B.L. van der Waerden, *Algebra*, Volume I, Seventh Edition, Springer-Verlag, New York, 1991.

[W] D.J. Winter, *The Structure of Fields*, GTM 16, Springer-Verlag, New York, 1974.

[Z-S] O. Zariski and P. Samuel, *Commutative Algebra*, Volume I, GTM 28, Springer, New York, 1958.

R.C. Churchill
Department of Mathematics and Statistics
Hunter College, the Graduate Center of CUNY,
and the University of Calgary

5 September 2014