MODEL THEORY OF DIFFERENTIAL FIELDS

David Marker
University of Illinois at Chicago

§1 Differential Algebra.

Throughout these notes *ring* will mean commutative ring with identity.

A *derivation* on a ring R is an additive homomorphism $D : R \to R$ such that $D(xy) = xD(y) + yD(x)$. A *differential ring* is a ring equipped with a derivation.

Derivations satisfy all of the usual rules for derivatives. Let D be a derivation on R.

Lemma 1.1. For all $x \in R$, $D(x^n) = nx^{n-1}D(x)$.

Proof.
By induction on n. $D(x^1) = D(x)$.

$$\begin{aligned} D(x^{n+1}) &= D(xx^n) = xD(x^n) + x^n D(x) \\ &= nx^n D(x) + x^n D(x) \\ &= (n+1)x^n D(x). \end{aligned}$$

Lemma 1.2. If b is a unit of R, $D(\frac{a}{b}) = \frac{bD(a) - aD(b)}{b^2}$.

Proof.
$D(a) = D(b \cdot \frac{a}{b}) = bD(\frac{a}{b}) + \frac{a}{b}D(b)$.
Thus $D(\frac{a}{b}) = \frac{1}{b}D(a) - \frac{a}{b^2}D(b) = \frac{bD(a) - aD(b)}{b^2}$.

examples.

1) (trivial derivation) $D : R \to \{0\}$.

2) Let C^∞ be the ring of infinitely differentiable real functions on $(0,1)$ and let D be the usual derivative.

3) Let U be a nonempty connected open subset of $\mathbf{C}$. Let O_U be the ring of analytic functions $f : U \to \mathbf{C}$ and let $D : O_U \to O_U$ be the usual derivative. [Note: O_U is an integral domain, while the ring of C^∞ functions is not.] Similarly the field of meromorphic functions on U is a differential field. In appendix A, we show that every countable differential field can be embedded into a field of germs of meromorphic functions.

4) Let $a \in R$. Let $D : R[X] \to R[X]$ by $D(\sum a_i X^i) = a(\sum i a_i X^{i-1})$. [Note: If $a = 1$, then D is $\frac{d}{dX}$.]

5) Let $D_0 : R \to R$ be a derivation. We form $R\{X\}$, the ring of *differential polynomials* as follows. $R\{X\} = R[X_0, X_1, \ldots]$. Let D extend D_0 by $D(X_n) = X_{n+1}$.

We identify X_0 with X and X_n with $X^{(n)}$, the n^{th} derivative of X.

Definition. If D is a derivation on R, we let C_R denote the kernel of D. We call C_R the *constants* of R. (If no ambiguity arises we will often drop the subscript R).

-C is a subring of R. Moreover if $b \in C$ is a unit in R and $a \in C$ then $\frac{a}{b}$ is in C. In particular, if R is a field then so is C.

-If $a \in C$, then $D(ax) = aD(x)$, thus D is C-linear.

Our first goal is to develop the basic ideal theory for differential ideals. We will be studying $K \subset L$ where K and L are differential fields. If $\alpha \in L$ we will want to consider the ideal of differential polynomials over K which vanish at α.

Definition. We say that an ideal $I \subset R\{X\}$ is a *differential ideal* if for all $f \in I$, $D(f) \in I$.

In general if $K \subset L$ and $\alpha \in L$ then the ideal $\{f(X) \in K\langle X\rangle : f(\alpha) = 0\}$ is a prime differential ideal. For $f(X) \in R\{X\}$, we let $\langle f(X)\rangle$ be the differential ideal generated by $f(X)$. Even if $f(X)$ is irreducible, $\langle f(X)\rangle$ may not be prime. For example let $f(X) = (X'')^2 - 2X'$. Then $D(f) = 2X''(X''' - 1)$ is in $\langle f(X)\rangle$, but neither $2X''$ nor $X''' - 1$ is in $\langle f(X)\rangle$.

Definition. If $f(X) \in R\{X\} \setminus R$, the *order* of f is the largest n such that $X^{(n)}$ occurs in f. (For completeness if f $f \in R$ we say f has order -1.) If f has order n we can write

$$f(X) = \sum_{i=0}^{m} g_i(X, X', \dots X^{(n-1)})(X^{(n)})^i$$

where $g_i \in R[X, X', \dots, X^{(n-1)}]$. If $g_m \neq 0$, we say that f has *degree* m.

We say that $f(X)$ is *simpler* that $g(X)$ and write $f \ll g$, if either the order of f is less that the order of g or the orders are equal and f has lower degree.

Definition. Let $f(X) \in R\{X\}$ have order $n \geq 0$. The *separant* of f is

$$s(X) = \frac{\partial f}{\partial X^{(n)}}.$$

For example if $f(X) = (X'')^2 - 2X'$, then $s(X) = 2X''$.

If $f(X) = \sum_{i=0}^{m} g_i(X, \dots, X^{(n-1)})\ (X^{(n)})^i$, then

$$s(X) = \sum_{i=0}^{m-1} (i+1) g_{i+1}(X, \dots, X^{(n-1)})\ (X^{(n)})^i.$$

So $s(X) \ll f(X)$.

Definition. For $f(X) \in R\{X\}$ let $I(f) = \{g \in R\{X\} : s^k g \in \langle f\rangle$ for some $k\}$.

We will show that if R is a differential field and $f \in R\{X\}$ is irreducible, then $I(f)$ is a prime differential ideal and that every prime differential ideal is of this form.

Lemma 1.3. $I(f)$ is a differential ideal.

Proof.

Clearly $R\{X\}I(f) \subseteq I(f)$. If $s^n g_0, s^m g_1 \in \langle f \rangle$, and $n \leq m$, then $s^m(g_0 + g_1) \in \langle f \rangle$. Thus $I(f)$ is an ideal.

If $s^n g \in \langle f \rangle$, then $D(s^{n+1}g) \in \langle f \rangle$. But $D(s^{n+1}g) = (n+1)s^n g D(s) + s^{n+1}g'$. Hence $s^{n+1}g' \in \langle f \rangle$. Thus if $g \in I(f)$, then $g' \in I(f)$.

The following division lemma is central to our analysis of differential ideals. For the rest of this section we will consider the case that is most important to us. We assume that R is a differential field K of characteristic zero. (The next lemma is false if K has characteristic $p > 0$.)

Lemma 1.4. If f is irreducible of order n and $g \in \langle f \rangle \setminus \{0\}$, then g has order at least n and if g has order n, then f divides g.

Proof.

Let s be the separant of f. We need the following claim.

claim: We can write $f^{(l)} = sX^{(n+l)} + f_l(X, \ldots, X^{(n+l-1)})$, for $l \geq 1$.

Let $f = \sum_{i=0}^{m} h_i \ (X^{(n)})^i$, where h_i has order at most $n-1$. Then

$$\begin{aligned} f' &= \sum_{i=0}^{m} (h_i'(X^{(n)})^i + ih_i(X^{(n)})^{i-1}X^{(n+1)}) \\ &= sX^{(n+1)} + f_1 \end{aligned}$$

where $f_1 = \sum h_i'(X^{(n)})^i$. Thus the claim is true for $l = 1$.

Given $f^{(l)} = sX^{(n+l)} + f_l$, where f_l has order at most $n + l - 1$, $l \geq 1$, we have $f^{(l+1)} = s'X^{(n+l)} + sX^{(n+l+1)} + f_l'$. Let $f_{l+1} = f_l' + s'X^{(n+l)}$. Then f_{l+1} has order at most $n + l$ and $f^{(l+1)} = sX^{(n+l+1)} + f_{l+1}$.

Let $g = a_0 f + \ldots + a_k f^{(k)}$. If $k = 0$, the lemma holds, so we assume $k \geq 1$. Assume g has order at most n.

Replace all instances of $X^{(n+k)}$ by $-\frac{f_k}{s}$. Since $X^{(n+k)}$ does not occur in g, and $f^{(k)} = sX^{(n+k)} + f_k$, we get a new equation (after clearing denominators)

$$s^m g = b_0 f + \ldots + b_{k-1} f^{(k-1)}.$$

We next replace all instances of $X^{(n+k-1)}$ by $-\frac{f_{k-1}}{s}$.

Continuing we find an m and $c \in K\langle X \rangle$ such that $s^m g = cf$. The degree of s is less than the degree of f. Thus f does not divide s. Since f is irreducible, f divides g. In particular, g has order exactly n.

Repeating the previous proof starting with $s^m g$, we can prove the following lemma.

Lemma 1.5. Let f be irreducible of order n and let $g \in I(f)$. Then g has order greater than or equal to n and if g has order n, then f divides g.

Lemma 1.6. Let f be irreducible of order n. For any differential polynomial g, we can find g_1 of order at most n such that for some m, $s^m g = g_1 \pmod{\langle f\rangle}$.

Proof. Suppose g has order $n+k$, where $k \geq 1$. Suppose the lemma is true for all $h \ll g$. As above we can find f_k of order at most $n+k-1$ such that $f^{(k)} = sX^{(n+k)} + f_k$. Suppose g has degree m and $g = \sum_{i=0}^{m} h_i (X^{(n+k)})^i$. Let $g_1 = s^m g - (f^{(k)})^m h_m$. Then $g_1 = s^m g \pmod{\langle f\rangle}$. Moreover g_1 is simpler than g (if $m = 1$, g_1 is of lower order, otherwise it is of lower degree). Thus, by induction on $\ll$, we are done.

Corollary 1.7. Let f be irreducible of order n. Then $I(f)$ is a prime differential ideal.

Proof.

Suppose $u_0 u_1 \in I(f)$. There are v_0, v_1 of order $\leq n$ and m_0 and m_1 such that $s^{m_i} u_i = v_i (\bmod\ \langle f\rangle)$. Thus $s^{m_0+m_1} u_0 u_1 = v_0 v_1 \pmod{\langle f\rangle}$. Since $u_0 u_1 \in I(f)$, $v_0 v_1 \in I(f)$. Since $v_0 v_1$ has order at most n, lemma 1.5 implies $f | v_0 v_1$. Since f is irreducible $f | v_0$ or $f | v_1$. If $f | v_i$, then $s^{m_i} u_i \in \langle f\rangle$ and $u_i \in I(f)$.

Lemma 1.8. Every nonzero prime differential ideal is of the form $I(f)$ for some irreducible f.

Proof.

Let I be a prime differential ideal. Let $f \in I$ be irreducible such that there is no $g \in I$ with $g \neq 0$ and $g \ll f$. We call f a *minimal polynomial* of I. We claim that $I = I(f)$.

Suppose $g \in I(f)$ and $s^m g \in \langle f\rangle \subseteq I$. Since I is prime and $s \notin I$, $g \in I$. Thus $I(f) \subseteq I$.

Let $g \in I$. Let g_1 have order at most the order of f and m be such that $s^m g = g_1 (\bmod\ \langle f\rangle)$. Let d be the degree of f. Using the division algorithm we can write $g_1 = af + r_1$, where $a, r_1 \in K(X \ldots X^{(n-1)})[X^{(n)}]$ and r_1 has degree $< d$. Clearing denominators, there are $a_1, a_2, r_2 \in K[X, \ldots X^{(n)}]$ such that r_2 has degree $< d$, a_1 is of order $< n$ and $a_1 g_1 = a_2 f + r_2$. Since $g \in I$ and $\langle f\rangle \subseteq I$, $g_1 \in I$. Thus $r_2 \in I$. But $r_2 \ll f$, so $r_2 = 0$. Thus $f | a_1 g_1$. Since a_1 has order $< n$, $f | g_1$. Hence $s^m g \in \langle f\rangle$ and $g \in I(f)$.

Definition. $RD(I)$, the *differential rank* of I, is the order of the minimal polynomial of I. If $I = \{0\}$, we define $RD(I) = \omega$.

Let L/K be differential fields with $\alpha \in L$. We let $I(\alpha/K)$ denote the ideal of differential polynomials in $K\langle X\rangle$ which vanish at α. Clearly $I(\alpha/K)$ is a prime differential ideal. If $I(\alpha/K)$ is not $\{0\}$, we say α is *differentially algebraic* over K. Otherwise α is *differentially transcendental*. [Warning: differentially algebraic does not imply algebraic in the model theoretic sense, as differential equations usually have infinitely many solutions.] We let $K\langle\alpha\rangle$ denote the differential field generated by α over K.

Lemma 1.9. If L/K are differential fields and $\alpha \in L$ then $RD(I(\alpha/K))$ is equal to the transcendence degree of $K\langle\alpha\rangle/K$.

Proof.

If $I(\alpha/K) = \{0\}$, then $K\langle\alpha\rangle$ is isomorphic to $K(X_0, X_1, X_2, \ldots)$, a purely transcendental extension of K. Thus $K\langle\alpha\rangle/K$ has transcendence degree ω.

If not we can assume $I(\alpha/K) = I(f)$ where f is a minimal polynomial. Then f has order $RD(I) = n$. Clearly $\alpha, \alpha', \ldots, \alpha^{(n-1)}$ are algebraically independent over K, so the transcendence degree is at least n. It is also clear that $\alpha^{(n)}$ depends on $\alpha, \alpha', \ldots, \alpha^{(n-1)}$ over K.

For all $k \geq 1$ we can write $f^{(k)} = sX^{n+k} + f_k$, where f_k has order $< n+k$ (this is the claim in the proof of lemma 1.4). Then $f^{(k)} \in I(f)$, thus $f^{(k)}(\alpha) = 0$ for all $k \geq 1$. So

$$f^{(k)}(\alpha) = s(\alpha)\alpha^{(n+k)} + f_k(\alpha, \ldots, \alpha^{(n+k-1)}).$$

Thus $\alpha^{(n+k)}$ depends on $\alpha, \ldots, \alpha^{(n+k-1)}$ over K. Thus, by induction, $\alpha, \ldots, \alpha^{(n-1)}$ is a transcendence base for $K\langle\alpha\rangle/K$. So $K\langle\alpha\rangle/K$ has transcendence degree n.

Note that we have shown that in the later case $K\langle\alpha\rangle = K(\alpha, \alpha', \ldots, \alpha^{(n-1)})[\alpha^{(n)}]$.

We next show differential prime ideals extend when we extend the base field.

Lemma 1.10. Suppose L/K are differential fields. Let $f \in K\{X\}$ be irreducible and let $f_1 \in L\{X\}$ be an irreducible factor of f in $L\{X\}$. Then $I_K(f) = I_L(f_1) \cap K\{X\}$.

Proof.

Suppose f has order n. If f factors in $L\{X\}$, then f factors in $L[X, X', \ldots, X^{(n)}]$. Moreover any irreducible factor must have order n, since whenever $k \subset l$ are fields of characteristic zero, $f \in k[\overline{X}]$ is irreducible and X_n occurs in f, then X_n occurs in any irreducible factor of f in $l[\overline{X}]$. (This is an interesting exercise in Galois theory).

Let s_f and s_{f_1} be the separants of f and f_1. Suppose $g \in I_L(f_1) \cap K\{X\}$. Let g_1 be of order at most n such that for some m $s_f^m g = g_1 \pmod{\langle f\rangle}$. Then $s_f^m g = g_1 \pmod{\langle f_1\rangle}$ and $g_1 \in I_L(f_1)$. Thus $f_1|g_1$. Since $g_1 \in K\{X\}$, all conjugates of f_1 (over the algebraic closure of K) divide g_1. Thus $f|g_1$. So $g \in I_K(f)$.

Suppose $g \in I_K(f)$. Say $s_f^m g \in \langle f\rangle$. Let $f = f_1 f_2$. Since f is irreducible, $f_1 \not| f_2$. Since $s_f = f_2 s_{f_1} + f_1 s_{f_2}$, $s_f^m g = f_2^m s_{f_1}^m g \pmod{\langle f_1\rangle}$. Thus $f_2^m g \in I_L(f_1)$.

If $f_2 \in I_L(f_1)$, then, by 1.4, $f_1|f_2$, a contradiction.

If $f_2 \notin I_L(f_1)$, then $g \in I_L(f_1)$.

Our next goal is to prove a version of Hilbert's Basis Theorem for differential ideals. Strictly speaking this is false. Even in $K\{X\}$ we do not have ACC for differential ideals. For example consider the ideals, $I_0 \subset I_1 \subset \ldots$, where:

$$I_n = \langle X^2, (X')^2, \ldots (X^{(n)})^2\rangle.$$

For the rings we care about we will be able to prove ACC for radical differential ideals. Recall that if I is an ideal, then $\sqrt{I} = \{a : \exists n\ a^n \in I\}$. We say that I is a *radical* ideal if $I = \sqrt{I}$.

Let R be a differential ring.

Lemma 1.11. If I is a radical differential ideal and $ab \in I$, then $aD(b) \in I$ and $D(a)b \in I$.

Proof.
If $ab \in I$, then $aD(b) + bD(a) \in I$. Multiplying by $D(a)b$ we see that $D(a)D(b)ab + (D(a)b)^2 \in I$. Since I is radical, $D(a)b \in I$. Similarly $aD(b) \in I$.

Lemma 1.12. Let I be a radical differential ideal, let $S \subset R$ be closed under multiplication and let $T = \{x \in R : xS \subset I\}$. Then T is a radical differential ideal.

Proof.
Clearly T is an ideal. If $xS \subseteq I$, then, by lemma 1.11, $D(x)S \subseteq I$. Thus T is a differential ideal. Suppose $x^n \in T$. Then for all $s \in S, x^n s \in I$. In particular for all $s \in S$, $x^n s^n \in I$. Since I is radical, for all $s \in S$, $xs \in I$. Thus $x \in T$.

For any $S \subseteq R$, let $\{S\}$ denote the smallest radical differential ideal containing S.

Lemma 1.13. $a\{S\} \subseteq \{aS\}$.

Proof.
By lemma 1.12, $T = \{x : ax \in \{aS\}\}$ is a radical differential ideal. Since $S \subseteq T$, $\{S\} \subseteq T$.

Lemma 1.14. Let $S, T \subseteq R$. Then $\{S\}\{T\} \subseteq \{ST\}$.

Proof.
By the previous lemma $\{x : x\{T\} \subseteq \{ST\}\}$ contains $\{S\}$.

Lemma 1.15. Let $R \supseteq \mathbf{Q}$ be a differential ring. If I is a differential ideal, then $\sqrt{I}$ is a radical differential ideal.

Proof.
Suppose $a^n \in I$. We will prove by induction that $a^{n-k}D(a)^{2k-1} \in I$.

We know $D(a^n) \in I$. But $D(a^n) = na^{n-1}D(a)$. Since $\mathbf{Q} \subseteq R$, $a^{n-1}D(a) \in I$, so the claim is true for $k = 1$.

Suppose $a^{n-k}D(a)^{2k-1} \in I$. Then

$$(n-k)a^{n-(k+1)}D(a)^{2k} + (2k-1)a^{n-k}D(a)^{2k-2}D(D(a)) \in I.$$

Multiplying by by $D(a)$, we see that

$$(n-k)a^{n-(k+1)}D(a)^{2k+1} + (2k-1)a^{n-k}D(a)^{2k-1}D(D(a)) \in I.$$

But $(2k-1)a^{n-k}D(a)^{2k-1}D(D(a)) \in I$. So $(n-k)a^{n-(k+1)}D(a)^{2k+1} \in I$. Since $R \supseteq \mathbf{Q}$, $a^{n-(k+1)}D(a)^{k+1} \in I$.

Thus $D(a)^{2n-1} \in I$, so $D(a) \in \sqrt{I}$.

We can now prove the relevant version of Hilbert's Basis Theorem. We say that a radical differential ideal I is *finitely generated* if there are $\beta_1 \ldots \beta_n \in I$ such that $I =$

$\{\beta_1, \ldots, \beta_n\}$. It is easy to see that R has ACC on radical differential ideals if and only if every radical differential ideal is finitely generated.

Theorem 1.16 [Ritt-Raudenbush Basis Theorem]. Let $R \supseteq \mathbf{Q}$ be a differential ring such that every radical differential ideal is finitely generated. Then every radical differential ideal in $R\langle X\rangle$ is finitely generated.

Proof.

Suppose not. By Zorn's lemma there is a non-finitely generated radical differential ideal I which is maximal among the non-finitely generated radical differential ideals. We claim that I is prime. Suppose $ab \in I, a \notin I$, and $b \notin I$. Then $\{a, I\}$ and $\{b, I\}$ are larger radical differential ideals and hence finitely generated. Let $c_1, \ldots, c_r, d_1, \ldots, d_s \in I$ be such that $\{a, I\} = \{a, c_1, \ldots, c_r\}$ and $\{b, I\} = \{b, d_1, \ldots, d_s\}$. [In general: suppose $\{a, S\}$ is generated by $\alpha_1 \ldots \alpha_s$. By lemma 1.15 $\{a, S\} = \sqrt{\langle a, S\rangle}$. Thus for each i, there are $b_{i,j} \in S$ and $r_j, r_{i,j,k} \in R$ such that:

$$\alpha_i^{n_i} = \sum r_j a^{(j)} + \sum r_{i,j,k} b_{i,j}^{(k)}.$$

In this case $\{a, S\} = \{a, b_{i,j}\}$.]

Thus $\{a, I\}\{I, b\} \subseteq \{ab, \ldots, c_r d_s\} \subseteq I$, by lemma 1.14. If $z \in I$, then $z^2 \in \{a, I\}\{b, I\}$ which is contained in $\{ab, \ldots, c_r d_s\}$, a radical ideal. Thus $z \in \{ab, \ldots, c_r d_s\}$, so $\{ab, \ldots, c_r d_s\} = I$. Since I is not finitely generated we have a contradiction. Thus I is prime.

To complete the proof we need the following stronger form of lemma 1.6:

Lemma 1.17. Let $R \supseteq \mathbf{Q}$ be a differential ring and let $f \in R\{X\} \setminus R$ be irreducible. Suppose $f(X) = \sum_{i=0}^{d} a_i (X^{(n)})^i$, where each a_i has order at most $n-1$. Let s be the separant of f. For any $g \in R\{X\}$ there is $g_1 \in R\{X\}$ such that $g_1 \ll f$ and for some l and t, $a_d^l s^t g = g_1 (\mathrm{mod}\ \langle f\rangle)$.

Proof. We first note that the proof of lemma 1.6 we will work since $R \supseteq \mathbf{Q}$. Thus we can find g_2 of order at most n such that $s^t g = g_2$ (mod $\langle f\rangle$). Using the standard division algorithm for polynomials we can find g_1 of degree $< d$ such that $a_d^l g_2 = g_1$ (mod $\langle f\rangle$).

We return to the proof of 1.16.

We have I a non-finitely generated differential prime ideal. By assumption $I \cap R$ is finitely generated. Let J be the finitely generated radical differential ideal of $R\{X\}$ generated by $I \cap R$. Let $f(X) \in I - J$ be of minimal order and degree. Say $f(X) = a(X^{(n)})^d + f_0(X)$, where $f_0(X) \ll f(X)$. If $a \in I$, then $f_0 \in I$, contradicting the choice of f. Thus $a \notin I$.

Further, s, the separant of f, is not in I. If $s \in I$, then, since $s \ll f$, $s \in J$. But then $f(X) - \frac{1}{d} X^{(n)} s$ would be in $I - J$, contradicting the minimality of f. Since I is prime $as \notin I$. Thus $\{as, I\}$ is a radical differential ideal extending I and hence finitely generated. Let $\{as, I\} = \{as, c_1, \ldots, c_m\}$, where each $c_i \in I$.

Let $g(X) \in I$. There are l, t such that $a^l s^t g = g_1 (\mathrm{mod}\ \langle f\rangle)$, where $g_1 \ll f$. Thus $g_1 \in I$. Since $g_1 \ll f$, we must have $g_1 \in J$. Thus $a^l s^t g \in \{J, f\}$. Since this is a radical ideal, $asg \in \{J, f\}$. Thus $asI \subseteq \{J, f\}$. Thus

$$\begin{aligned} I^s &\subseteq I\{as, I\} = I\{as, c_1, \dots, c_m\} \\ &\subseteq \{asI, Ic_1, \dots, Ic_m\} \\ &\subseteq \{J, f, c_1, \dots, c_m\} \subseteq I. \end{aligned}$$

If $z^2 \in I$, then $z^2 \in I^2$. Thus $z^2 \in \{J, f, c_1 \dots, c_m\}$. Since this is a radical ideal, $z \in \{J, f, c_1 \dots c_m\}$. Thus I is finitely generated.

Let k be a differential field. We say that $X \subseteq k^n$ is D-closed if there are $f_1, \dots, f_m \in k\{\overline{X}\}$ such that

$$X = \{\overline{x} \in k^n : f_1(\overline{x}) = \cdots = f_m(\overline{x}) = 0\}.$$

The basis theorem insures that the intersection of any collection of D-closed sets is equal to the intersection of a finite subcollection. Thus the D-topology is Noetherian.

The next theorem gives the differential version of primary decomposition in Noetherian rings.

Theorem 1.19 [Decomposition Theorem]. Let R be a differential ring with ACC on radical differential ideals. Any radical differential ideal is the intersection of a finite number of prime differential ideals.

Proof.

Suppose not. By ACC there is a radical differential ideal I which is not the intersection of finitely many prime differential ideals and is maximal with this property. As I is not prime, we have $ab \in I, a, b \notin I$. Then $\{I, a\}$ and $\{I, b\}$ are intersections of finitely many prime differential ideals.

Note than $\{I, a\}\{I, b\} \subseteq \{ab, I\} \subseteq I$. For $c \in \{I, a\} \cap \{I, b\}$, $c^2 \in I$, so $c \in I$. Thus $\{I, a\} \cap \{I, b\} = I$, and I is a finite intersection of prime differential ideals.

As usual there is a unique irredundant representation of I as a finite intersection of prime differential ideals. We say that a D-closed set is *irreducible* if it can not be written as the union of two proper D-closed subsets. The decomposition theorem implies that any D-closed set is a finite union of irreducible D-closed sets.

References

For the most part the work in this section is due to Ritt.

Kaplansky's monograph *Differential Algebra* is an excellent reference for the material in this section. It is very thin and elegantly written. In particular our treatment of the Ritt basis theorem is taken from there. Kolchin's *Differential Algebra and Algebraic Groups* is encyclopedic but notationally dense.

Buium's *Differential Algebra and Diophantine Geometry* and Magid's *Lectures on Differential Galois Theory* are two excellent recent references.

Much of the basic material on differential polynomial rings can also be found in Poizat's book *Cours de Théorie des Modèles.*

§2 Basic Model Theory of Differentially Closed Fields.

We begin by defining the theory of differentially closed fields (DCF). Let $\mathcal{L}$ be the language with binary function symbols $+, \cdot, -$, unary function symbol D, and constant symbols 0 and 1. DCF is axiomatized as follows:

i) axioms for algebraically closed fields of characteristic zero

ii) $\forall x, y\ D(x+y) = D(x) + D(y)$

iii) $\forall x, y\ D(xy) = xD(y) + yD(x)$.

iv) For any non-constant differential polynomials $f(X)$ and $g(X)$ where the order of g is less than the order of f, there is an x such that $f(x) = 0 \wedge g(x) \neq 0$.

One could also consider the theory DCF_p of differentially closed fields of characteristic $p > 0$. This theory is much less well behaved (see [Wood]). Henceforth all fields will be assumed to have characteristic 0.

Suppose K is a differentially closed field. Then as a pure field $(K, +, \cdot)$ is algebraically closed. Moreover the next lemma shows that the field of constants is also algebraically closed. To avoid confusion between the field theoretic and model theoretic notions of "algebraic", we say that a is *strongly algebraic* over k if there is a polynomial $p(X) \in k[X] - \{0\}$ such that $p(a) = 0$. [In §5 we will give the precise relation between algebraic and strongly algebraic.]

Lemma 2.1. Let K be a differentially closed field. If $a \in K$ is strongly algebraic over C the field of constants, then $a \in C$.

Proof.

Let $p(X) = \sum_{i=0}^{m} b_i X^i$ be the minimal polynomial of a over C. Since $p(a) = 0$, $D(p(a)) = 0$. But $D(p(a)) = (\sum_{i=0}^{m-1}(i+1)b_{i+1}a^i)D(a)$. Since p is the minimal polynomial of a, $\sum_{i=0}^{m-1}(i+1)b_{i+1}a^i \neq 0$. Thus $D(a) = 0$, so $a \in C$.

Lemma 2.2. Every differential field k has an extension K which is differentially closed.

Proof.

Given k let f be of order n and let g be of order $< n$. Let f_1 be an irreducible factor of f of order n. Let $I = I(f_1)$. Then $g \notin I$. Let F be the fraction field of $k\{X\}/I$. [Note: the quotient rule gives us a way of extending a derivation on an integral domain to its fraction field.] Let $a \in F$ be the image of $X(\text{mod } I)$. Since $f \in I$, $f(a) = 0$. Since $g \notin I$, $g(a) \neq 0$.

Iterating this process we can build $K \supseteq k$ a differentially closed field.

The next lemma is crucial for quantifier elimination.

Lemma 2.3. Let K and L be ω-saturated models of DCF. Let $\overline{a} \in K$, $\overline{b} \in L$, $k = \mathbf{Q}\langle \overline{a} \rangle$ and $l = \mathbf{Q}\langle \overline{b} \rangle$. Suppose $\sigma : k \to l$ is an isomorphism such that $\sigma(\overline{a}) = \overline{b}$. For all $\alpha \in K$ there is an extension of σ to an isomorphism σ^* from $k\langle \alpha \rangle$ into L.

Proof.

Let $\alpha \in K$. First suppose α is differentially algebraic over K. Let f be the minimal polynomial of $I(\alpha/k)$, the ideal of differential polynomials in $K\{X\}$ which vanish at α. Say f has order N. Let g be the image of f under σ. Let $\Gamma(v) = \{g(v) = 0\} \cup \{h(v) \neq 0 : h(X) \in l\{X\}$ where h has order $< N\}$. For any $h_1, \ldots, h_n \in l\{X\}$, where each h_i has order $< N$, we can find $\beta \in L$ such that $g(\beta) = 0 \wedge \prod h_i(\beta) \neq 0$. Thus by ω-saturation there is β in L realizing $\Gamma(v)$. Extend σ by setting $\sigma^*(\alpha) = \beta$. It is easy to see that $I(\beta/l)$ is the image under σ of $I(\alpha/k)$. Thus $k\langle\alpha\rangle \cong l\langle\beta\rangle$.

If α is differentially transcendental over k, we use ω-saturation to find $\beta \in L$, β differentially transcendental over l. We can now extend σ by sending $\alpha \mapsto \beta$.

Theorem 2.4. DCF has elimination of quantifiers.

Proof.

It sufficed to show that if $K, L \models DCF$, $k \subseteq K$, $k \subseteq L$, $\overline{a} \in k$, $b \in K$, $\phi(v, \overline{w})$ is quantifier free and $K \models \phi(b, \overline{a})$, then $L \models \exists v\ \phi(v, \overline{a})$ (see [Marker] 1.5).

Since we may replace K and L by elementary extensions if necessary, we may without loss of generality assume that they are ω-saturated. We may also assume that k is the differential field generated by $\overline{a}$. By lemma 2.3, we can find $\beta \in L$ such that $k\langle b\rangle \cong k\langle\beta\rangle$. Thus $L \models \phi(\beta, \overline{a})$. So $L \models \exists v\ \phi(v, \overline{a})$.

Corollary 2.5. DCF is complete and model complete.

Proof. Let K and L be models of DCF. Then $\mathbf{Q}$ (with the trivial derivation) is a substructure of both fields. Every sentence ϕ is provably equivalent with a quantifier free sentence ψ. But

$$\begin{aligned} K \models \phi &\Leftrightarrow K \models \psi \\ &\Leftrightarrow \mathbf{Q} \models \psi \\ &\Leftrightarrow L \models \psi \\ &\Leftrightarrow L \models \phi \end{aligned}.$$

Thus $K \equiv L$, so DCF is complete.

Every quantifier eliminable theory is model complete.

Quantifier elimination leads to the following Nullstellensatz of Seidenberg.

Corollary 2.6 (Differential Nullstellensatz). If k is a differential field and Σ is a system of differential equations and inequations over k such that Σ has a solution in some $l \supseteq k$, then Σ has a solution in any differentially closed $K \supseteq k$.

Proof.

By quantifier elimination the assertion that there is a solution to Σ is equivalent in DCF to a quantifier free formula with parameters from k. Thus if there is any differentially closed $L \supseteq k$ containing a solution to Σ, then every differentially closed $K \supseteq k$ contains a solution to Σ. But if there is any differential field $l \supseteq k$ containing a solution to Σ , then by lemma 2.2 there is a differentially closed $L \supseteq l$. Thus Σ has a solution in any differentially closed $K \supseteq k$.

Exercise. Let K be differentially closed. Let Σ be any set of differential polynomials in $X_1 \ldots X_n$. Let $V(\Sigma) = \{\overline{x} \in K^n : f(\overline{x}) = 0 \text{ for all } f \in \Sigma\}$ and let $I(V) = \{g \in K\langle X_1 \ldots X_n\rangle : g(\overline{x}) = 0 \text{ for all } \overline{x} \in V(\Sigma)\}$. Then $I(V(\Sigma)) = \{\Sigma\}$ the smallest radical differential ideal containing Σ.

Let's make the quantifier elimination explicit. The atomic formulas in $\mathcal{L}$ are of the form $f(\overline{x}) = 0$ where f is a differential polynomial. Thus by quantifier elimination every formula $\phi(\overline{v}, \overline{a})$ over a differential field k is equivalent to one of the form:

$$\bigvee_{i=1}^{n} [\bigwedge_{j=1}^{m_i} f_{i,j}(\overline{v}) = 0 \wedge \bigwedge_{k=1}^{r_i} g_{i,j}(\overline{v}) \neq 0],$$

where $f_{i,j}, g_{i,j} \in k\langle\overline{X}\rangle$. Of course $\bigwedge g_{i,j}(\overline{v}) \neq 0$ if and only if $\prod g_{i,j}(\overline{v}) \neq 0$. Thus every formula is equivalent to one of the form:

$$\bigvee_{i=1}^{n} [\bigwedge_{j=1}^{m_i} f_{i,j}(\overline{v}) = 0 \wedge g_i(\overline{v}) \neq 0].$$

We next show that there is an intimate relationship between types for DCF and differential prime ideals. Let k be a differential field and let $S_1(k)$ be the 1-types of DCF with parameters from k. For each 1-type $p(v) \in S_1(k)$. Let $I_p = \{f \in k\langle X\rangle$: "$f(v) = 0$" $\in p\}$. It is easy to see that I_p is a prime differential ideal.

Lemma 2.7. $p \mapsto I_p$ is a bijection from $S_1(k)$ to the space of prime differential ideals over $k\langle X\rangle$.

Proof.
Suppose $p, q \in S_i(k)$ and $p \neq q$. Then there is a formula $\phi(v, \overline{a}) \in p \setminus q$. By quantifier elimination there are differential polynomials $f_{i,j}, g_i$ such that

$$\phi(v, \overline{a}) \Leftrightarrow \bigvee [\bigwedge f_{i,j}(v) = 0 \wedge g_i(v) \neq 0].$$

Thus $\phi(v, \overline{a}) \in p$ if and only if for some i all $f_{i,j} \in I_p$ but $g_i \notin I_p$. Since $\phi(v, \overline{a}) \in p - q$, we must have $I_p \neq I_q$. Thus $p \mapsto I_p$ is one to one.

For any differential ideal I, let K be a differentially closed field containing the fraction field of $k\{X\}/I$. Let p be the type over k realized by the image of the indeterminate X. Then $I_p = I$, so $p \mapsto I_p$ is onto.

For $p \in S_1(k)$ we let $RD(p) = RD(I_p)$.

Let $K \supset k$. If $\alpha \in K, f \in k\langle X\rangle$, and $f(\alpha) = 0$, we say that α is a *generic solution* of f, if and only if for all $g \in k\langle X\rangle$ if $g \ll f$ then $g(\alpha) = 0$. For f irreducible, α is a generic solution of f if and only if $I(\alpha/k) = I(f)$.

Definition. Let k be a differential field. We say that $K \supseteq k$ is a *differential closure* of k if $K \models$ DCF and for any $L \models$ DCF, if $L \supseteq k$, then there is an embedding $\sigma : K \to L$.

Of course DCF is a model complete theory. Thus any embedding $\sigma : K \to L$ is necessarily an elementary embedding. Therefore a differential closure of k is a model of DCF which is prime over k. Model theoretic considerations will allow us to prove that every k has a differential closure.

Recall that a theory T is ω-stable if for any $M \models T$ and $A \subset M$, $|S_n(A)| = |A| + \aleph_0$.

Lemma 2.8. DCF is ω-stable.

Proof.

Let k be a differential field. We must show that $|S_1(k)| = |k|$. But there is a bijection between $S_1(k)$ and the space of differential prime ideals on $k\{X\}$. By lemma 1.8, each prime differential ideal is of the form $I(f)$ for some $f \in k\{X\}$. Thus $|S_1(k)| = |k\{X\}| = |k|$.

We may now appeal to the following important basic results from the model theory of ω-stable theories. If $M \supseteq A$ we say that M is *prime* over T if and only if for any $N \models T$ with $N \supseteq A$, there is an elementary map $j : M \to N$ fixing A. We say that M is *atomic* over A if and only if every $\overline{m} \in M$ realizes an isolated type in $S_n(A)$.

Theorem 2.9 Let T be an ω-stable theory.

a) (Morley) For any A a substructure of a model of T, there is $M \models T$, such that $M \supset A$ and M is prime and atomic over A.

b) (Shelah) If M and N are prime over A, then there is an isomorphism $\sigma : M \to N$, which is the identity on A.

Corollary 2.10. If k is a differential field then k has a differential closure K. If K and L are two differential closures of k, then there is an isomorphism $\sigma : K \cong L$ such that σ is the identity on k. Moreover K is *atomic* over k.

<u>**Excercise**</u>. a) Show that a type $p \in S_1(k)$ is isolated if and only if there is g of order less than $RD(I_p)$ such that I_p is the only prime differential ideal containing the minimal polynomial of I_p and not containing g.

b) Show directly that the isolated types are dense. [hint: For $\phi(v, \overline{a})$, let $p \in S_1(k)$ be such that $RD(p)$ is minimal. Let f be the minimal polynomial of I_p. Show that $\phi(v, \overline{a}) \wedge f(v) = 0$ isolates p.]

[Note: The above arguments can be used to show that DCF$_p$ has prime models even though DCF$_p$ is not ω-stable.]

The following lemma will be useful when we begin differential Galois theory.

Lemma 2.11. Let k be a differential field and let K be the differential closure of k. Then C_K is algebraic over C_k. In particular, if C_k is algebraically closed, then $C_K = C_k$.

Proof.

Let $a \in C_K$. Since K is atomic over k, $p = t(a/k)$ is atomic. Clearly "$D(v) = 0$" $\in p$. Thus $RD(p) \leq 1$.

If $RD(p) = 1$, then, by the excercise above, there must be $f(X)$ of order 0 (ie. $f \in k[X]$) such that "$D(v) = 0 \wedge f(v) \neq 0$" isolates p. But there are $c \in C_k$ such that

$f(c) \neq 0$ so this is impossible. Thus $RD(p) = 0$.

Thus there is $f(X) \in k[X]$ such that $f(a) = 0$. We claim that a is strongly algebraic over C_k. We may assume that f is the minimal polynomial of a over k. Thus $f(X) = \sum_{i=0}^{n} b_i X^i$, where $b_n = 1$. Since $f(a) = 0$, $D(f(a)) = 0$. But

$$D(f(a)) = D(a) \sum_{i=0}^{n-1} (i+1) b_{i+1} a^i + \sum_{i=0}^{n} D(b_i) a^i.$$

Since $D(a) = 0$, $D(f(a)) = \sum_{i=0}^{n} D(b_i) a^i$. Since $b_n = 1$, $\sum_{i=0}^{n-1} D(b_i) a^i = 0$. Since f is the minimal polynomial of a over k, we must have all $D(b_i) = 0$. Thus all of the $b_i \in C_k$. So a is strongly algebraic over C_k.

The next lemma is another useful consequence of the fact that the differential closure of K is atomic over K.

Lemma 2.12. Let K be a differential field. Every element of the differential closure of K is differentially algebraic over K.

Proof.

Suppose a is in the differential closure F of K and a is differentially transcendental over K. Let $\psi(v)$ isolate $tp(a/K)$. Since a satisfies no differential polynomial equations over K, $\psi(v)$ we can assume that $\psi(v)$ is "$f(v) \neq 0$" for some $f \in K\langle X\rangle$. Suppose f has order n. There is $b \in F$ such that $b^{(n+1)} = 0 \wedge f(b) \neq 0$. Clearly a and b have different types over a, contradicting the fact that ψ isolates the type of a over K.

Definition. A type $p(\overline{v}) \in S(A)$ is *definable* if for each formula $\phi(\overline{v}, \overline{w})$ there is a formula $d\phi(\overline{w})$ with parameters from A such that for all $\overline{a} \in A$ $\phi(\overline{v}, \overline{a}) \in p$ if and only if $d\phi(\overline{a})$.

In a stable theory all types are definable. This has a very simple proof for differentially closed fields.

<u>Excercise</u>. Let k be a differential field and let $p \in S_n(K)$. Show that p is definable. [Hint: Use the Ritt basis theorem to find $f_1, \ldots, f_m \in k\langle\overline{X}\rangle$ such that $\{g : \text{"}g(\overline{v}) = 0\text{"} \in p\}$ is the smallest radical differential ideal containing $f_1, \ldots, f_m$. For $h \in k\langle\overline{X}\rangle$, if $\phi(\overline{v})$ is "$g(\overline{v}) = 0$", then $d\phi$ is $\forall \overline{x}\ (\bigwedge f_i(\overline{v}) = 0 \ \rightarrow g(\overline{v}) = 0)$. Use quantifier elimination to get definitions of all formulas.]

We conclude this section by proving that differentially closed fields satisfy uniform bounding.

Theorem 2.13. Let $K \models$ DCF. Suppose $\phi(x_1, \ldots, x_m, y_1, \ldots, y_l)$ is an $\mathcal{L}$-formula then there is an N such that for any $\overline{a} \in K$ if $\{\overline{x} : \phi(x, \overline{a})\}$ is finite then it has cardinality at most N.

Proof.

We first note that it suffices to prove this for $m = 1$. If we can find uniform bounds for $\phi_1, \ldots, \phi_n$, then we can find uniform bounds for $\bigvee \phi_i$. Thus by quantifier elimination it suffices to consider

$$\phi(x, \overline{y}) = \bigwedge f_i(x, \overline{y}) = 0 \wedge g(\overline{x}, \overline{y}) \neq 0.$$

Let $\psi(x, u, \overline{y}, v)$ be the formula

$$\bigwedge f_i(x, \overline{y}) = 0 \wedge u(x - v)g(x, \overline{y}) = 1.$$

Suppose $\overline{a} \in K^l$ and

$$\{x : \bigwedge f_i(x, \overline{a}) = 0\} = \{b_1, \ldots, b_n\}.$$

Then the collection of formulas $\{\phi(x, u, \overline{a}, b_1), \ldots, \phi(x, u, \overline{a}, b_n)\}$ is inconsistent, while every proper subset is consistent. This shows that theorem 2.13 is a consequence of the following lemma.

Lemma 2.14. Let K be a differentially closed field. Let $f_1, \ldots, f_n \in K\{\overline{X}, \overline{Y}\}$ and let $\phi(\overline{x}, \overline{y})$ be the formula $\bigwedge f_i(\overline{x}, \overline{y}) = 0$. There is a number s such that if $\{\phi(\overline{x}, \overline{c}_1), \ldots, \phi(\overline{x}, \overline{c}_m)\}$ is inconsistent, then some subset of size at most s is inconsistent.

Proof.

Let $m_1, \ldots, m_M$ be a listing of monomials in $X_i^{(j)}$ containing all monomials occuring in any f_l (in particular assume $m_1 = 1$). Thus we can find $a_{i,j}$ differential polynomials in $\overline{Y}$ such that $f_i = \sum_{j=1}^{M} a_{i,j} m_j$.

Suppose $N \geq M + 2$. We will show that for any $\overline{c}_1, \ldots, \overline{c}_N$, if $\{\phi(\overline{v}, \overline{c}_i) : 1 \leq i \leq N\}$ is inconsistent, then there is a subset of size $M + 1$ which is inconsistent.

Consider $F_i(Z_1, \ldots, Z_M, \overline{y}) = \sum a_{i,j} Z_j$. For each $\overline{c}_j$, let σ_j be the system of linear equations

$$\bigwedge_{i=1}^{n} F_i(\overline{Z}, \overline{c}_j) = 0$$

and let

$$\Sigma = \bigwedge_{j=1}^{N} \sigma_j.$$

Using elementary linear algebra we see that if Σ is inconsistent, there are $i_1, \ldots, i_{M+1}$ such that $\bigwedge_{j=1}^{M+1} \sigma_{i_j}$ is inconsistent. In this case surely $\bigwedge_{j=1}^{M+1} \phi(\overline{v}, \overline{c}_{i_j})$ is also inconsistent.

On the other hand if Σ is consistent there are $i_1, \ldots, i_M$ such that the solutions to Σ are exactly the solutions to $\bigwedge_{j=1}^{M} \sigma_{i_j}$. Suppose $\{\phi(\overline{x}, \overline{c}_{i_j}) : j = 1, \ldots, M\}$ is consistent. Let $\overline{\alpha}$ be a solution. Building up monomials from $\overline{\alpha}$ we get $(1, \beta_2, \ldots, \beta_M)$ a solution to $\bigwedge_{j=1}^{M} \sigma_{i_j}$. But then $(1, \beta_2, \ldots, \beta_M)$ is a solution to Σ and $\overline{\alpha}$ is a solution to $\bigwedge_{j=1}^{N} \phi(\overline{x}, \overline{c}_j)$.

Thus if every $M + 1$ element subset of $\{\phi(\overline{x}, \overline{c}_j) : j = 1, \ldots, N\}$ is consistent then the entire set is consistent.

Lemma 2.14 is a special case of a more general fact.

Definition. Let T be a first order theory. We say that $\phi(\overline{x}, \overline{a})$ has the *finite cover property* if for arbitrarily large N there are $a_1, \ldots, a_N$ such that $\{\phi(\overline{x}, \overline{a}_i) : i \leq N\}$ is inconsistent with T while every subset of size $N-1$ is consistent. We say that T has the finite cover property (FCP) if there is a formula with the finite cover property. Otherwise T is said to be NFCP.

In T is unstable then T has the finite cover property. Both uniform bounding and lemma 2.14 are weak forms of NFCP. Poizat showed using the method of pairs that the theory of differentially closed fields has NFCP. In fact, by a result of Shelah, if T has uniform bounding and elimination of imaginaries (which we will prove for DCF in the next chapter), then T has NFCP.

References

The first work on the model theory of differentially closed fields was done by Robinson, though this work was influenced by earlier work of Seidenberg. Blum (see [Blum]) considerably simplified Robinson's axioms and was the first to use stability theoretic methods. The proof of uniform bounding given here is due to van den Dries and works equally well for separably closed fields.

The model theoretic results of Morley and Shelah can be found in Sacks' *Saturated Model Theory* or Lascar's *Stability in Model Theory.*

Differentially closed fields of prime characteristic are also interesting. They have a stable non-superstable theory and we can show existence and uniqueness of differential closures. See [Wood] for more information on DCF_p.

§3. Elimination of Imaginaries

Shelah introduced the structure M^{eq} obtained by adding imaginary elements which are names for equivalence classes of $\emptyset$-definable equivalence relations. Imaginaries smooth out many arguments from stability theory. In some cases we can show that the introduction of imaginary elements is unnecessary. Elimination of imaginaries turns out to be one of the central ideas in the model theory of fields. In particular if we can eliminate imaginaries then we may represent definable quotients as definable objects.

We will show that differentially closed fields have elimination of imaginaries. We first work in a general setting.

Definition. Let T be any theory and let M be a suitably saturated model of T. Let p be a (possibly incomplete) type over M. We say that B is a *canonical base* for p if B is definably closed and whenever σ is an automorphism of M, σ fixes the realizations of p (setwise) if and only if it fixes B pointwise.

Since we do not require p to be complete it makes sense to talk about canonical bases for formulas.

Lemma 3.1. Suppose B is a canonical base for $\phi(\overline{v},\overline{a})$. Then there is a formula $\psi(\overline{v},\overline{w})$ and $\overline{b}\in B$ such that $\phi(\overline{v},\overline{a})\leftrightarrow\psi(\overline{v},\overline{b})$ and $\psi(\overline{v},\overline{b})\not\leftrightarrow\psi(\overline{v},\overline{b}')$ for all $\overline{b}'\neq\overline{b}$.

Proof.

Let $\Gamma(\overline{v})=\{\psi(\overline{v}):\psi$ has parameters from B and $\phi(\overline{v},\overline{a})\rightarrow\psi(\overline{v})\}$. We will show that $\Gamma(\overline{v})\rightarrow\phi(\overline{v},\overline{a})$. Suppose not. Then by saturation there is $\overline{c}\in M$ such that $\Gamma(\overline{c})$ and $\neg\phi(\overline{c},\overline{a})$. If $t(\overline{c}'/B)=t(\overline{c}/B)$, then there is an automorphism of M fixing B and sending $\overline{c}$ to $\overline{c}'$. Since any automorphism which fixes B normalizes $\phi(\overline{v},\overline{a})$, we have $\neg\phi(\overline{c}',\overline{a})$. Thus $t(\overline{c}/B)\rightarrow\neg\phi(\overline{v},\overline{a})$. Hence there is a formula $\theta(\overline{v})$ with parameters from B such that $\theta(\overline{v})\in t(\overline{c}/B)$ and $\theta(\overline{v})\rightarrow\neg\phi(\overline{v},\overline{a})$. But then $\neg\theta(\overline{v})\in\Gamma$, contradicting $\Gamma(\overline{c})$. Thus $\Gamma(\overline{v})\rightarrow\phi(\overline{v},\overline{a})$ and by compactness there is a formula $\psi_0(\overline{v},\overline{b})$ with $\overline{b}\in B$ such that $\phi(\overline{v},\overline{a})\leftrightarrow\psi_0(\overline{v},\overline{b})$. (Here we have just reproven the well known fact that a set X is definable from A if and only if in any saturated enough model every automorphism that fixes A, normalizes X).

If $\overline{b}$ and $\overline{b}'$ realize the same type over the empty set then there is an automorphism σ taking $\overline{b}$ to $\overline{b}'$. Since this automorphism does not fix B, it does not normalize $\phi(\overline{v},\overline{a})$. Thus $\psi_0(\overline{v},\overline{b})\not\leftrightarrow\psi_0(\overline{v},\overline{b}')$. Thus there is $\theta(\overline{w})\in t(\overline{b})$, such that

$$\theta(\overline{c})\wedge\overline{c}\neq\overline{b}\rightarrow(\psi_0(\overline{v},\overline{b})\not\leftrightarrow(\psi_0(\overline{v},\overline{c})).$$

Let $\psi(\overline{v},\overline{w})=\psi_0(\overline{v},\overline{w})\wedge\theta(\overline{w})$.

In particular the canonical base for a formula will be the definable closure of a finite set.

Defintion. A theory T admits *elimination of imaginaries* if every formula $\phi(\overline{v},\overline{a})$ has a canonical base.

The next lemma gives the connection between elimination of imaginaries and equivalence relations.

Lemma 3.2. Suppose T admits elimination of imaginaries and has two constant symbols. Let $M \models T$ and let E be a $\emptyset$-definable equivalence relation on M^n. There is a $\emptyset$-definable $f : M^n \to M^m$ such that $xEy \Leftrightarrow f(x) = f(y)$.

Proof.

By elimination of imaginaries and 3.1, for each formula $\phi(\overline{v}, \overline{a})$, there is a formula $\psi_{\overline{a}}(\overline{v}, \overline{w})$ and a unique $\overline{b}$ such that $\phi(\overline{v}, \overline{a}) \leftrightarrow \psi_{\overline{a}}(\overline{v}, \overline{b})$. By compactness we can find $\psi_1, \ldots, \psi_n$ such that for all $\overline{a}$ there is an i and a unique $\overline{b}$ such that $\phi(\overline{v}, \overline{a}) \leftrightarrow \psi_i(\overline{v}, \overline{b})$. By the usual coding tricks we can reduce to a single formula ψ (a sequence made up of the distinguished constants is added to the witnesses $\overline{b}$ to code up the least i such that ψ_i works).

To prove the lemma let $\phi(\overline{v}, \overline{w})$ be $\overline{v}E\overline{w}$ and let f be the functions $\overline{a} \mapsto \overline{b}$, where $\overline{b}$ is unique such that $\overline{v}E\overline{a} \Leftrightarrow \psi(\overline{v}, \overline{b})$.

The next lemma gives a test for elimination of imaginaries. We say that B is a canonical base for a finite set of types if and only if an automorphism permutes the types if and only if it fixes B.

Lemma 3.3. Let T be an ω-stable theory and let $M \models T$ be suitably saturated. If every finite set of conjugate complete types over M has a canonical base, then T admits elimination of imaginaries.

Proof.

For any formula $\phi(\overline{x}, \overline{y})$, let $E_\phi(\overline{y}, \overline{z}) \Leftrightarrow \forall \overline{x}\ (\phi(\overline{x}, \overline{y}) \leftrightarrow \phi(\overline{x}, \overline{z}))$. An automorphism of M fixes $\phi(\overline{x}, \overline{a})$ if and only if it preserves the E_ϕ-class of $\overline{a}$. Let $p_1, \ldots, p_n$ be the global types of maximal rank that contain $E_\phi(\overline{y}, \overline{a})$.

We can partition $\{p_1, \ldots, p_n\}$ into finitely many conjugacy classes. For each class we can find a canonical base B.

Let A be the union of the canonical bases. Clearly an automorphism permutes the p_i if and only if it fixes A. An automorphism of M permutes $p_1, \ldots, p_n$ if and only if it fixes the E_ϕ class of $\overline{a}$. Thus A is a canonical base for $\phi(\overline{x}, \overline{a})$.

Elimination of imaginaries for algebraically closed fields, differentially closed fields and separably closed fields can be proved using the following classical theorem from algebraic geometry.

Definition. Let K be a field and let I be an ideal in $K[\overline{X}]$. We say that k is a field of definition for I if I is generated by polynomials in $k[\overline{X}]$.

Theorem 3.4. Every ideal I in $K[\overline{X}]$ has a unique smallest field of definition k. Any automorphism of K which fixes I fixes k pointwise.

Proof. Let M be a basis of monomials for $K[\overline{X}]/I$ as a vector space over K. Each monomial $u \in K[\overline{X}]$ can be written as $\sum a_{u,i}m_i + g_u$ where $a_{u,i} \in K$, $m_i \in M$ and $g_u \in I$.

Let k be the subfield of K generated by all the $a_{u,i}$.

For any $f \in K[\overline{X}]$, f can be written as $\sum b_u u$, where each u is a monomial. Thus

$$\begin{aligned} f &= \sum b_u u = \sum b_u(u - \sum a_{u,i}m_i) + \sum b_u(\sum a_{u,i}m_i) \\ &= \sum b_u(u - \sum a_{u,i}m_i) + \sum c_i m_i. \end{aligned}$$

If f is in I, then, since each $u - \sum a_{u,i}m_i$ is in I and the m_i are a basis for $K[\overline{X}]/I$, each of the $c_i = 0$. Thus the $u - \sum a_{u,i}m_i$ generate the ideal I, but $u - \sum a_{u,i}m_i \in k[\overline{X}]$. So k is a field of definition for I.

Suppose l is a second field of definition for I. Let $f_1, \ldots, f_s \in l[\overline{X}]$ generate I. For each monomial u, there are $g_{u,1}, \ldots, g_{u,s}$ in $K[\overline{X}]$ such that $u - \sum a_{u,i}m_i = \sum g_{u,i}f_i$. Viewing the $a_{u,i}$ and $g_{u,i}$ as variables, we get a system of linear equations over $l[\overline{X}]$. This system has a solution in K and hence in l. But then the m_i form a basis for $K[\overline{X}]/I$, so if $u - \sum c_{u,i}m_i \in I$ we must have $c_{u,i} = a_{u,i}$. Thus $k \subset l$.

Let α be an automorphism of K fixing $V(I)$. We can lift α to an automorphism of $K[\overline{X}]$. For each monomial u, $\alpha(u - \sum a_{u,i}m_i) = u - \sum \alpha(a_{u,i})m_i \in I$. Again since the m_i form a basis for $K[\overline{X}]/I$, we must have $\alpha(a_{u,i}) = a_{u,i}$. Thus α fixes k.

Corollary 3.5. Let $\{I_1, \ldots, I_n\}$ be a set of conjugate prime ideals in $K[\overline{X}]$. There is a subfield k such that if α is an automorphism of K, α permutes $I_1, \ldots, I_n$ if and only if α fixes k pointwise.

Proof.

Let $I = \bigcap I_j$. Since the I_j are conjugate, this is an irredundant primary decomposition of I. Let k be the field of definition of I. Any automorphism of K which permutes the I_j fixes I and hence fixes k pointwise. On the other hand, if α fixes k pointwise, α fixes I. Hence by the uniqueness of primary decomposition (there is a unique way to write a radical ideal as an intersection of prime ideals), α must permute the I_j.

We next give a version for differential fields.

Corollary 3.6. Let $\{I_1, \ldots, I_n\}$ be a set of conjugate differential prime ideals of $K\{X_1, \ldots, X_m\}$. There is a subfield $k \subseteq K$ such that an automorphism of K permutes the ideal I_j if and only if it fixes k pointwise.

Proof.

Let $J = \bigcap I_j$. J is a radical differential ideal. Thus by the Ritt basis theorem it is the radical of a finitely generated differential ideal. Let $f_1, \ldots, f_s$ be such that $J = \{f_1, \ldots, f_s\}$. There is an N such that all $f_i \in K[X_i^{(j)} : i \le m, j \le N]$. Let $J_0 = J \cap K[X_i^{(j)} : i \le m, j \le N]$. Let k be the field of definition of J_0. Clearly any automorphism of K fixes J if and only if it fixes J_0 if and only if it fixes k pointwise. By theorem 1.19 and the uniqueness of the decomposition for radical ideals, an automorphism fixes J if and only if it permutes the I_j.

Theorem 3.7. The theory of algebraically closed fields and the theory of differentially closed fields admit elimination of imaginaries.

Proof.

a) algebraically closed fields:

Let K be algebraically closed. For $p \in S_n(K)$, let $I_p = \{f(\overline{X}) \in K[X_1, \ldots, X_n] :$ "$f(\overline{v}) = 0$" $\in p\}$. This map is a bijection between n-types and prime ideals in $K[\overline{X}]$. If $p_1, \ldots, p_n$ is are conjugate complete types, we get a canonical base for the set by taking the field of defintion for $I_{p_1}, \ldots, I_{p_n}$ given by 3.5. By lemma 3.3, the theory has elimination of imaginaries.

b) differentially closed field:

Similar using 3.6.

References

All of the material on elimination of imaginaries is due to Poizat. It was first proved in [Poizat 3], though our treatment here more closely follows that in *Cours de Théorie des Modèles*. A different proof of elimination of imaginaries for algebraically closed fields is given in §4 of [Marker].

The proof given here on the existence of fields of definition for ideals is from Lang's *Introduction to Algebraic Geometry*.

§4. Linear Differential Equations

In this short section we will review some of the basic theory of linear differential equations. This will be used in our analysis of ranks in §5.

Let k be a differential field.

Definition: We define the *Wronskian* of $X_0, \ldots, X_n$ to be the determinant

$$W(X_0, \ldots, X_n) = \begin{vmatrix} X_0 & X_1 & \ldots & X_n \\ X_0' & X_1' & \ldots & X_n' \\ \vdots & \vdots & \ddots & \vdots \\ X_0^{(n)} & X_1^{(n)} & \ldots & X_n^{(n)} \end{vmatrix}$$

Lemma 4.1: Let $x_0, \ldots, x_n \in k$, then $W(x_0, \ldots, x_n) = 0$ if and only if $x_0, \ldots, x_n$ are linearly dependent over C_k.

proof:

($\Leftarrow$) Suppose $c_0, \ldots, c_n \in C_k$ are not all zero and $\sum c_i x_i = 0$. Taking the derivative: $0 = D(\sum c_i x_i) = \sum c_i x_i'$. Continuing we see that

$$\sum c_i \begin{pmatrix} x_i \\ \vdots \\ x_i^{(n)} \end{pmatrix} = 0.$$

Since the columns of the matrix are linearly dependent, $W(x_0, \ldots, x_n) = 0$.

($\Rightarrow$) We proceed by induction on n. Suppose $W(x_0, \ldots, x_n) = 0$, then there are $a_i \in k$, not all zero such that

$$\sum a_i \begin{pmatrix} x_i \\ \vdots \\ x_i^{(n)} \end{pmatrix} = 0.$$

Without loss of generality we assume that $a_0 = 1$. By induction we may assume that $W(x_1, \ldots, x_n) \neq 0$. Thus $x_0^{(j)} + \sum_{i=1}^n a_i x_i^{(j)} = 0$ for each $j < n$. Taking the derivative we see that

$$x_0^{(j+1)} + \sum_{i=1}^n a_i x_i^{(j+1)} + \sum_{i=1}^n D(a_i) x_i^{(j)} = 0.$$

But

$$x_0' + \sum_{i=1}^n a_i x_i' = 0.$$

Thus

$$\sum_{i=1}^n D(a_i) \begin{pmatrix} x_i \\ \vdots \\ x_i^{(n)} \end{pmatrix} = 0.$$

But then the columns of the Wronskian determinant for $x_1, \ldots, x_n$ are linearly dependent unless all $D(a_i) = 0$.

Let $L(X) = X^{(n)} + \sum_{i=0}^{n-1} a_i X^{(i)}$. We consider first the homogeneous linear equation $L(X) = 0$

Lemma 4.2: If $x_0, \ldots, x_n \in k$ are solutions of $L(X) = 0$, then $x_0, \ldots, x_n$ are linearly dependent over C_k.

proof:

$$W(x_0 \ldots x_n) = \begin{vmatrix} x_0 & x_1 & \cdots & x_n \\ x_0' & x_1' & \cdots & x_n' \\ \vdots & \vdots & \ddots & \vdots \\ -\sum a_i x_0^{(i)} & -\sum a_i x_1^{(i)} & \cdots & -\sum a_i x_n^{(i)} \end{vmatrix} = 0,$$

as the rows are linearly dependent over k.

Let $K \supset k$ be differentially closed.

Lemma 4.3: In K there are $x_1, \ldots, x_n$ linearly independent solutions to $L(X) = 0$.

proof:
Given $x_1, \ldots, x_m$ with $m < n$. We can find $x_{m+1} \in K$ such that $L(x_{m+1}) = 0$ but $W(x_1, \ldots, x_{m+1}) \neq 0$. ($W(x_1, \ldots, x_{m+1})$ has order m so this system can be solved in any differentially closed field.)

It is also easy to see that if $x_1, \ldots, x_n$ are solutions to $L(X) = 0$. Then $L(\sum c_i x_i) = 0$ for any constants $c_1, \ldots, c_n$. Summarizing:

Theorem 4.4: If $K \supset k$ is differentially closed then there are $x_1, \ldots, x_n \in K$ which are linearly independent over C_K such that the solution set for $L(X) = 0$ is exactly the span of $x_1, \ldots, x_n$ over C_K.

We call $\{x_1 \ldots x_n\}$ a *fundamental system* of solutions to $L(X) = 0$.

If $b \in K$ and y_0, y_1 are solutions to $L(X) = b$, then $L(y_0 - y_1) = L(y_0) - L(y_1) = 0$. Thus if y is a fixed solution to $L(X) = b$, then every other solution is of the form $x + y$ where x is a solution to $L(X) = 0$. In particular if $x_1, \ldots, x_n \in K$ is a fundamental system of solutions to $L(X) = 0$ then $\{y + \sum c_i x_i : c_i \in C_K\}$ is the set of solutions to $L(X) = b$ in K.

Definition: Let K/k be differential fields. We say that K is a *Picard-Vessiot extension* of k if there is a linear differential equation $L(X) = 0$ and $\{x_1, \ldots, x_n\} \subset K$ a fundamental system of solutions such that $K = k\langle x_1, \ldots, x_n\rangle$ and $C_k = C_K$. We say that K/k is a Picard-Vessiot extension for L.

The following theorem of Kolchin follows easily from the construction of differential closures.

Theorem 4.5: Let k be a differential field with C_k algebraically closed and let $L(X) = 0$ be a homogeneous linear differential equation over k. There is K/k a Picard-Vessiot extension for L. Moreover K is unique.

proof:

Let F be the differential closure of k. By lemma 2.13 $C_L = C_k$. By theorem 4.4 we can find $x_1, \ldots, x_n \in F$ a fundamental system of solutions for $L(X) = 0$. Thus $K = k\langle x_1, \ldots, x_n\rangle$ is a Picard-Vessiot extension of k.

Suppose K_1 is a second Picard-Vessiot extension of k. Let F_1 be the differential closure of K_1. By lemma 2.12 $C_{F_1} = C_{K_1} = C_k$.

Since F is the differential closure of k, we can embedded F in F_1. Let $y_1 \ldots y_n$ be a fundamental system of solutions of $L(X) = 0$ such that $K_1 = k\langle y_1 \ldots y_n\rangle$. But then each x_i is in the span of $(y_1, \ldots, y_n)$ over C_k and each y_i is in the span of $(x_1 \ldots x_n)$ over C_k. Thus $K = K_1$. Thus $L(X) = 0$ determines a unique Picard-Vessiot extension of k.

References

Most of the material in this section can be found in any basic differential equations text (for example [Hirsh-Smale]). Kolchin's theorem on Picard-Vessiot extensions is in [Kolchin 1].

§5. **Types and Ranks in Differentially Closed Fields**

Throughout this section we work inside $\mathbf{K}$ a very saturated differentially closed field.

Recall that a is *algebraic* over a set B if and only if there is a formula $\phi(v, \overline{w})$ and $\overline{b} \in B$ such that $\phi(a, \overline{b})$ and $\{x : \phi(x, \overline{b})\}$ is finite. We say that a is *strongly algebraic* over B if a is a zero of an ordinary polynomial with coefficients in the subfield generated by B. For any b, $D(b)$ is algebraic over b but not necessarily strongly algebraic over b. The next lemma sorts out the relationship between these notions.

Lemma 5.1: Let k be the differential field generated by B. Then a is algebraic over B if and only if it is strongly algebraic over k.

Proof:

Suppose a is algebraic over B. Consider $I = I(a/k)$. If $RD(I) = 0$, then a is strongly algebraic over k. Suppose $RD(I) \geq 1$. Let $f(X)$ be the minimal polynomial of I. Let K be the differential closure of k. Let $f_1 \in K\{X\}$ be an irreducible factor of f. Then f_1 and f have the same order. By saturation there is $b \in \mathbf{K}$ such that $I(b/K) = I(f_1)$. By lemma 1.10, $I(b/K) \cap k\{X\} = I$. Thus b and a realize the same type over k. But $b \notin K$, while, since a is algebraic over k, anything with the same type over k must be in the differential closure K, a contradiction.

The other direction is obvious.

Exercise. As a corollary show that the definable closure of $B \subset K \models DCF$ is just the differential field generated by B.

We next give a concrete algebraic characterization of forking for one types. Suppose $K \subset L$, $q \in S_1(K)$, $p \in S_1(L)$ and $q \subseteq p$. We will show that p forks over K if and only if $RD(p) < RD(q)$. We begin by recalling some basic facts and definitions from stability theory. [Alternatively, the reader could just take this as the definition of forking.]

Definition: Let $p \in S_1(k)$. We say that $\phi(v, \overline{w})$ is *represented* in p if and only if for some $\overline{a} \in k$, $\phi(v, \overline{a}) \in p$.

We say that $q \supseteq p$ is an *heir* of p if every formula represented in q is represented in p.

If $K \models$ DCF and $k \supseteq K$, then any $p \in S_1(K)$ has a unique heir in $S_1(k)$.

We use the following as our definition of forking.

Definition: Let $k \subseteq l$, $p \in S_1(k)$, $q \in S_1(l)$ and $p \subseteq q$. We say that q *does not fork* over k if for all $M, N \models DCF$ such that $k \subseteq M$, $M \cup l \subseteq N$, there is $p_1 \in S_1(M)$, $q_1 \in S_1(N)$ such that $p \subseteq p_1$, $q \subseteq q_1$ and q_1 is the heir of p_1.

We will also use the following lemma.

Lemma 5.2: Let k, l, p, q be as above. Suppose for every $K \models$ DCF with $l \subseteq K$ there is $p_1 \in S_1(K)$ such that $p_1 \supseteq p$ and for all $q_1 \in S_1(K)$, if $q_1 \supseteq q$, then q_1 represents a formula not represented in p_1. Then q forks over k.

We can now give our characterization of forking.

Theorem 5.3 Let $k \subseteq l$ be differential fields, let $p \in S_1(k), q \in S_i(l)$ and $p \subseteq q$. Then q forks over k if and only if $RD(q) < RD(p)$.

Proof:

Suppose $RD(q) < RD(p)$. Let $K \models$ DCF, with $K \supseteq l$. Let f be the minimal polynomial of I_p. Let $f_1 \in K\{X\}$ be an irreducible factor of the same order. Let $p_1 \in S_1(K)$ be the type of a generic solution of f_1. Then $I_{p_1} = I(f_1)$ and $I(f_1) \cap k\{X\} = I(f)$, so $p \subseteq p_1$. Then $RD(p_1) = RD(p)$. Let $q_1 \in S_1(K)$ be any extension of q. Since q contains some equation of order less than $RD(p)$, q_1 represents a formula not represented in p_1 (namely a formula asserting that a non-trivial differential polynomial of order less than $RD(p)$ vanishes). Thus by lemma 5.2, q is a forking extension of p.

Suppose $RD(p) = RD(q)$. Let $K, L \models$ DCF with $K \supseteq k$ and $L \supseteq l \cup K$. Let f be the minimal polynomial of I_p, and g be the minimal polynomial of I_q. Then $g|f$ (by lemma 1.4). Let g_1 be an irreducible factor of g in $L\langle X\rangle$ of the same order and let q_1 be the type of a generic solution to g_1. Then $p \subseteq q_1$ and $RD(q_1) = RD(p)$. Let p_1 be the restriction of q_1 to K. It suffices to show that q_1 is the heir of p_1.

Let f_1 be the minimal polynomial of p_1. Then f_1 is irreducible in $K\{X\}$ and remains irreducible in $L\{X\}$. But since $f_1 \in I(g_1)$, $g_1|f_1$. Thus $g_1 = af_1$ for some $a \in L$. Without loss of generality, we may assume that $g_1 = f_1$.

Let $\phi(v, \overline{a})$ be a formula in q_1. By quantifier elimination, there is a differential polynomial $h(v, \overline{a})$ of order $< RD(q_1)$ such that

$$\text{DCF} \vdash (f_1(v) = 0 \wedge h(v, \overline{w}) \neq 0) \to \phi(v, \overline{w}).$$

But $f_1(v) = 0 \in p_1$ and $h(v, \overline{b}) \neq 0 \in p_1$ for any $\overline{b}$. Thus $\phi(v, \overline{b})$ is represented in p_1. Thus q_1 is the heir of p_1 and q is a nonforking extension of p.

Exercise: For n-types we can give the following characterization of forking. For $p \in S_n(K)$. Let K be a differentially closed field, $p(\overline{x}) \in S_n(K)$, and $k \subseteq K$. Then p does not fork over k if and only if $V(I_{p|k})$ is an irreducible component of $V(I_p)$, where $V(I) = \{\overline{x} : f(\overline{x}) = 0$ for all $f \in I\}$.

We now define several notions of rank.

a) *U-rank*:

Let $p \in S_1(k)$. We say $RU(p) \geq \alpha + 1$ if and only if there is q a forking extension of p with $RU(q) \geq \alpha$. For β a limit ordinal $RU(p) \geq \beta$ if and only if for all $\alpha < \beta$, $RU(p) \geq \alpha$. In particular $RU(p) = 0$ if and only if p is algebraic.

b) *Morley rank*:

Let $p \in S_1(k)$. For β a limit ordinal $RM(p) \geq \beta$ if and only if for all $\alpha \leq \beta$, $RM(p) \geq \alpha$. We say $RM(p) \geq \alpha + 1$ if and only if for any $K \supseteq k$, if$K \models DCF$, then p is a limit point of the types $q \in S_1(K)$ with $RM(q) \geq \alpha$.

If q is a forking extension of p then $RM(q) < RM(p)$. Thus $RM(p) \geq RU(p)$.

c) *depth*:

For P a differential prime ideal in $k\{X\}$, let the depth of P be the largest N such that there are differential prime ideals $P \subset P_1 \subset P_2 \ldots \subset P_N$.

We can define $RH(p)$ to be the supremum of the depths of differential prime ideals $P \subset K\{X\}$ where $K \supseteq k$ and $P \cap k\{X\} = I_p$. [Note in [Poizat 2] there are three possibly inequivalent definitions of depth. Poizat refers to this notion as "height" though we find "depth" more descriptive.]

Lemma 5.4 Let $p \in S_1(k)$. Then $RU(p) \leq RM(p) \leq RH(p) \leq RD(p)$.

Proof:

1) We always have $RU(p) \leq RM(p)$.

2) We claim that for any differentially closed field K the depth of a differential prime ideal is at most $RD(p)$. Suppose $P_0 \subseteq P_1$ are differential prime ideals. Let f_i be the minimal polynomial of P_i. If the order of f_1 is equal to the order of f_0 then f_1 divides f_0. Since P_0 is prime this contradicts the fact that f_0 is the minimal polynomial of P_0.

3) We claim that $RM(p) \leq RH(p)$. It suffices to prove this for types over a suitably saturated $K \models$ DCF. In this case $RM(p) \geq \alpha + 1$ if and only if p is a limit point of the types of Morley rank at least α.

Let $D^n(K)$ be the types of rank at least n. By induction, if $p \in D^n(K)$, then $RH(p) \geq n$. Suppose $p \in D^n(K)$ and I_p has depth n. Let f be the minimal polynomial of I_p and let s be the separant of f.. Suppose $q \in D^n(K)$ and "$f(v) = 0 \wedge s(v) \neq 0$" $\in q$. Then $I_q \supseteq I_p$. Since, I_p has depth n and I_q has depth at least n, we must have $p = q$. Thus "$f(v) = 0 \wedge s(v) \neq 0$" isolates p in $D^n(K)$ so $RM(p) = n$.

Note in particular that p is an algebraic type if and only if $RU(p) = RM(p) = RH(p) = RD(p) = 0$. This yields a simple but useful corollary.

Corollary 5.5: If $RD(p) = 1$, then $RU(p) = RM(p) = RH(p) = 1$.

In algebraically closed fields there are analogous notions of rank: U-rank, Morley rank, depth and Krull dimension (transcendence degree) and these notions are all equal.

We next argue that the constant field of a differentially closed field is a pure algebraically closed field.

Lemma 5.6 Let K be a differentially closed field. Suppose $A \subseteq C_K^n$ is K-definable. Then A is definable in the pure field $(C_K, +, \cdot)$.

Proof:

By quantifier elimination, it suffices to prove this for sets of the form $f(\overline{x}) = 0$, where $f \in K\{\overline{X}\}$. Say $f(\overline{X}) = g(\overline{X}) + h(\overline{X})$, where $g(\overline{X}) \in K[\overline{X}]$, $h(\overline{X}) \in K\{\overline{X}\}$ and every monomial in h involves some $X_i^{(j)}$ where $j \geq 1$. Thus for $\overline{x} \in C_K$, $h(\overline{x}) = 0$. Thus without loss of generality the definable set A is just the points in C_K which are solutions to a polynomial equation over K.

By definability of types (in the theory of algebraically closed fields), if $B \subseteq K^n$ is definable in the pure field K, then $C_K^n \cap B$ is definable in the pure field C_K. Thus our set A is definable in the pure field C_K.

Corollary 5.6: If $p \in S_n(K)$ is a type of an n-tuple of constants, then $RU(p)$ is equal to the transcendence degree of $K\langle\alpha\rangle/K$ where α realizes p.

Corollary 5.7: If p is the type of a generic solution of an n^{th} order linear differential equation $L(X) = 0$, then $RD(p) = RU(p) = n$.

Proof:

Let $RD(p) = n$. Let $K \models$ DCF with $L(X) \in K\{X\}$. Let $x_1, \ldots, x_n \in K$ be a fundamental system of solutions for $L(X) = 0$. There is a definable bijection between solutions to $L(X) = 0$ and $C^n_{\mathbf{K}}$. Thus the rank of the set of solutions is equal to the rank of C^n. But $RU(C^n)$ is the same as the rank computed in the pure algebraically closed field. For a generic solution, $\overline{c}$ are algebraically independent, thus $RU(p) = n$.

Corollary 5.8. If p is the type of a differential transcendental, then $RU(p) = RD(p) = \omega$.

Proof.

For each n, p has a forking extension where for some new element a we look at the generic solution of $X^{(n)} = a$. This is a type of U-rank n.

Corollary 5.9 DCF has Morley rank $\omega + 1$.

We next give two bad examples. The first shows that it is possible to have $RM(p) = 1$ with $RH(p) = 2$. In the second we show that it is possible to have $RH(p) = 1$ and $RD(p) = 2$.

<u>Open Problem</u>. Do we always have $RM(p) = RU(p)$?

We first give a non-linear example where U-rank is equal to the differential rank. Let $f(X) \in C[X]$ be a polynomial with constant coefficients and consider the differential equation $X'' = X'f(X)$. Let $g(X) \in C[X]$ be a primitive of f, that is $\frac{dg}{dX} = f$. Let K be a differentially closed field and let p be the type of a generic solution of $X'' = X'f$. Suppose $F \supset K$ and let $c \in C_F - C_K$. Let q be the type of a generic solution to $X' = g(X) + c$. It is easy to see that q is a forking extension of p and $RD(q) = 1$. Thus $RU(p) = RD(p) = 1$.

Consider next the differential equation $X'' = \frac{X'}{X}$. If we apply the same ideas we are tempted to say that for c a new constant any solution to $X' = \ln(X) + c$ is a solution to the original equation. This does not work since the second equation is not an algebraic differential equation and hence does not make sense over an arbitrary differential field. We will see that in fact the type of a generic solution to $X'' = \frac{X'}{X}$ has Morley rank one.

We first argue that this type has depth two. Let P_0 be the ideal $I(XX'' - X')$ and let $P_1 = I(X')$. Clearly if $X' = 0$, $X'' = 0$. So $XX'' - X' = 0$. Thus $P_0 \subseteq P_1$. Further for any constant c, $I(X - c) \supseteq P_1$, thus P_0 has depth at least two. But the depth of P_0 is bounded above by $RD(P_0) = 2$. Thus P_0 has depth two. Lemma 5.11 shows that $I(X')$ is the only depth one prime ideal containing $XX'' - X'$. Before that we give a simple lemma about differentiating polynomials.

Definition. Suppose $f(X) \in K[\overline{X}]$. Let $f^*(\overline{X}) \in K[\overline{X}]$ be the polynomial obtained by differentiating the coefficients of f. That is if $f(X) = \sum a_i m_i$, where m_i is a monomial in the various $X_i^{(j)}$, then $f^*(X) = \sum D(a_i)m_i$.

Lemma 5.10. For $f(X) \in K[X]$, $D(f(X)) = f^*(X) + \frac{\partial f}{\partial X}X'$.

More generally: If $f(X) \in K[X, X' \dots X^{(n)}]$, then

$$D(f) = \sum_{i=0}^{n} \frac{\partial f}{\partial X^{(i)}} X^{(i+1)} + f^*.$$

Proof.

Let $f(X) = \sum a_i X^i$. Then:

$$\begin{aligned} D(f(X)) &= \sum (D(a_i)X^i + ia_i X^{i-1}X') \\ &= \sum D(a_i)X^i + X' \sum ia_i X^{i-1} \\ &= f^*(X) + X' \frac{\partial f}{\partial X}. \end{aligned}$$

The general case can be proved inductively in a similar manner.

Lemma 5.11. Let $f(X) = XX'' - X'$. Suppose $g(X)$ is irreducible of order one and $f \in I(g)$, then $X' \in I(g)$.

Proof.

Let $g(X) = \sum_{n=0}^{N} a_n(X)(X')^n$, where $a_n \in K[X]$, $N > 0$ and $a_N \neq 0$. Then, by lemma 5.10,

$$D(g(X)) = \sum_{n=0}^{N} a_n^*(X')^n + \sum_{n=0}^{N} \frac{\partial a_n}{\partial X}(X')^{n+1} + X'' \sum_{n=0}^{N} na_n(X')^{n-1}.$$

Let

$$f_1(X) = \sum_{n=0}^{N} na_n(X')^n + X(\sum_{n=0}^{N} a_n^*(X')^n + \sum_{n=0}^{N} \frac{\partial a_n}{\partial X}(X')^{n+1}).$$

Consider $XD(g(X))$. Substituting $\frac{X'}{X}$ for X'', we see that $XD(g(X)) = f_1 (\mathrm{mod}\ \langle f \rangle)$. Since $D(g(X))$ and $f(X)$ are in $I(g)$, we must have $f_1 \in I(g)$. Since f_1 has order one, g must divide f_1.

The leading term of f_1 is $X\frac{\partial a_N}{\partial X}X'^{N+1}$, while the leading term of g is $a_N X'^N$. Thus for some $\lambda \in K$ we must have $X\frac{\partial a_N}{\partial X} = \lambda a_N$. Suppose $a_N = \sum_{i=0}^{m} b_i X^i$. Then $X\frac{\partial a_N}{\partial X} = \sum ib_i X^i$. Then $\lambda b_m = mb_m$, so $\lambda = m$. It is then easy to see that for all $i < m$, $b_i = 0$. Thus $a_N = b_m X^m$. Replacing g by $\frac{g}{b_m}$ if necessary, we may assume that $a_N = X^m$.

case 1. $m = 0$.

In this case $a_N = 1$ and f_1 has degree N.

The coefficient of ${X'}^N$ in f_1 is

$$Na_N + a_N^* X + \frac{\partial a_{N-1}}{\partial X} X = N + \frac{\partial a_{N-1}}{\partial X} X.$$

Thus $f_1 = (N + \frac{\partial a_{N-1}}{\partial X} X)g$.

Consider the coefficients of $(X')^0$ on both sides of the equation. We get that

$$a_0^* X = \Big(N + \frac{\partial a_{N-1}}{\partial X} X\Big) a_0.$$

Suppose $a_0 \neq 0$. There is a largest M such that X^M divides a_0. Then $X^{M+1} | a_0^* X$, but then we must have $X | (N + \frac{\partial a_{N-1}}{\partial X} X)$, which is impossible. Thus $a_0 = 0$. But if $a_0 = 0$, then $X' | g$. Since g is irreducible and $a_N = 1$, $X' = g$, as desired.

case 2. $m > 0$

Then $f_1 = m(X' + u(X))g$, for some $u(X) \in K[X]$. Considering the coefficients of $(X')^0$ we see that $X a_0^* = mu(X) a_0$. As in case one, this tells us that either $a_0 = 0$ or $X | u(X)$. If $a_0 = 0$, then as above $g(X) = X'$, contradicting the fact that $a_N = X^m$. Thus we may assume there is $v(X) \in K[X]$ such that $u(X) = Xv(X)$.

Looking at the coefficients of ${X'}^N$ we see that:

$$Na_N + Xa_N^* + X\frac{\partial a_{N-1}}{\partial X} = ma_{N-1} + mvXa_N.$$

Since $a_N = X^m$, $a_N^* = 0$, thus

$$X\frac{\partial a_{N-1}}{\partial X} - ma_{N-1} = mvX^{m+1} - NX^m.$$

Thus X^m divides $X\frac{\partial a_{N-1}}{\partial X} - ma_{N-1}$. An easy calculation shows that $X^m | a_{N-1}$. Say $a_{N-1} = w(X)X^m$, where $w \in K[X]$. Then

$$\frac{\partial a_{N-1}}{\partial X} = mwX^{m-1} + \frac{\partial w}{\partial X} X^m.$$

Thus $\frac{\partial w}{\partial X} = mv - \frac{N}{X}$. But this is impossible since v and w are polynomials. Thus we have a contradiction.

Corollary 5.12. Let p be the type of a generic solution to $XX'' = X'$. Then p has Morley rank one.

Proof.

The formula $XX'' = X' \wedge X' \neq 0$ isolates p from all other non-algebraic types.

We next consider an example of an order two equation where the depth is one. Let F be a differential field and let $x \in F$ be such that $D(x) = 1$. Consider the Painlevé equation $X'' = 6X^2 + x$.

Theorem 5.13 (Kolchin) If η is a solution to the Painlevé equation then the transcendence degree of $F\langle\eta\rangle/F$ is either two or zero.

Corollary 5.14 If p is the type of a generic solution to the Painlevé equation, then p has depth one.

Proof. If $RH(p) = 2$, then there is a differential prime ideal I such that $I_p \subseteq I$ and $RH(I) = 1$. But if μ is a generic solution for I, then μ satisfies the Painlevé equation and the transcendence degree of $F\langle\mu\rangle/F$ is one.

proof of 5.13.

Suppose not. Then $RD(I(\eta/F))$ is one. Let f be the minimal polynomial of $I(\eta/F)$. f has order one. By lemma 5.10,

$$D(f(X)) = \frac{\partial f}{\partial X'}X'' + \frac{\partial f}{\partial X}X' + f^*.$$

But $\eta'' = 6\eta^2 + x$. Thus

$$\begin{aligned} 0 &= D(f(\eta)) \\ &= \frac{\partial f}{\partial X}\eta' + (6\eta^2 + x)\frac{\partial f}{\partial X'} + f^*(\eta). \end{aligned}$$

Thus $\frac{\partial f}{\partial X}X' + (6X^2 + x)\frac{\partial f}{\partial X'} + f^*(X)$ is in $I(\eta/F)$. Thus f must divide $\frac{\partial f}{\partial X}X' + (6X^2 + x)\frac{\partial f}{\partial X'} + f^*(X)$. The next lemma shows that this is impossible.

The next lemma is about polynomial rings.

Lemma 5.15. Let $p(X, Y) \in F[X, Y] - F$. Let $q(X, Y) = Y\frac{\partial p}{\partial X} + (6X^2 + x)\frac{\partial p}{\partial Y} + p^*$. Then q is not divisible by p.

Proof.

Suppose p divides q. The degree (in the usual sense) of q is at most the degree of $p + 1$, thus $q = (a + bX + cY)p$.

Let j be largest such that Y^j occurs in some term of p.

Let i be largest such that dX^iY^j is a term of p. The coefficient of X^iY^{j+1} in q is zero, while the coefficient ot X^iY^{j+1} in $(a + bX + cY)p$ is cd. Thus $c = 0$. Similarly the coefficient of $X^{i+1}Y^j$ in q is zero, while in $(a + bX)p$ it is bd. Thus $b = 0$. Thus for some $a \in F$, $q = ap$.

Let $p = \sum_{j=0}^{n} p_jX^j$, where $p_j \in F[Y]$ and $p_n \neq 0$. For notational simplicity we let $p_i = 0$ for $i < 0$ or $i > n$.

Since $q = ap$,

$$Y\sum jp_jX^{j-1} + \sum \frac{dp_j}{dY}(6X^{j+2} + xX^j) + \sum(p_j^* - ap_j)X^j = 0.$$

This yields the system of differential equations:

$$6\frac{dp_{j-2}}{dY} = -p_j^* + ap_j - x\frac{dp_j}{dY} - (j+1)p_{j+1}Y.$$

We solve for $j = n+2, n+1$ and n.

<u>j=n+2</u>

$6\frac{dp_n}{dY} = 0$. Thus $p_n = u_0$, for some $u_0 \in F$ with $u_0 \neq 0$.

<u>j=n+1</u>

$6\frac{dp_{n-1}}{dY} = 0$. Thus $p_{n-1} = v_0$, for some $v_0 \in F$.

<u>j=n</u>

$6\frac{dp_{n-2}}{dY} = -u_0' + au_0$. Thus $p_{n-2} = w_0 Y + t_0$, where $w_0 = -\frac{1}{6}(u_0' - au_0)$ and $t_0 \in F$.

We claim that for any k we can write:

$$\begin{aligned} p_{n-3k} &= u_k Y^{2k} + r_k Y^{2k-1} + \dots \\ p_{n-3k-1} &= v_k Y^{2k} + s_k Y^{2k-1} + \dots \\ p_{n-3k-2} &= w_k Y^{2k+1} + t_k Y^{2k} + \dots. \end{aligned}$$

The above arguments show that it is true for $k = 0$. Assume it is true k.

<u>j= n-3k-1</u>

Using the inductive assumptions we see that

$$6\frac{dp_{n-3k-3}}{dY} = (n-3k)u_k Y^{2k+1} + (-v_k' + av_k + (n-3k)r_k)Y^{2k} + \dots.$$

Thus $p_{n-3k-3} = u_{k+1}Y^{2k+2} + r_{k+1}Y^{2k+1} + \dots$, where

$$u_{k+1} = -\frac{1}{6}\left(\frac{n-3k}{2k+2}\right) u_k, \tag{1}$$

and

$$r_{k+1} = -\frac{1}{6}\left(\frac{v_k' - av_k - (n-3k)r_k}{2k+1}\right). \tag{2}$$

Similar arguments for the cases $j = n-3k-2$ and $j = n-3k-3$ yield

$$p_{n-3(k+1)-1} = v_{k+1}Y^{2k+2} + s_{k+1}Y^{2k+1} + \dots$$

and

$$p_{n-3(k+1)-2} = w_{k+1}Y^{2k+3} + t_{k+1}Y^{2k+2} + \dots$$

where:

$$v_{k+1} = -\frac{1}{6}\left(\frac{w_k' - aw_k + (n-3k-1)v_k}{2k+2}\right) \tag{3}$$

$$s_{k+1} = -\frac{1}{6}\left(\frac{t'_k - at_k + (2k+1)xw_k + (n-3k-1)s_k}{2k+1}\right) \tag{4}$$

$$w_{k+1} = -\frac{1}{6}\left(\frac{u'_{k+1} - au_{k+1} + (n-3k-2)w_k}{2k+3}\right) \tag{5}$$

and

$$t_{k+1} = -\frac{1}{6}\left(\frac{r'_{k+1} - ar_{k+1} + (2k+2)xu_{k+1} + (n-3k-2)t_k}{2k+2}\right). \tag{6}$$

(1) gives a recursive definition of u_k. This yields:

$$u_k = \left(\frac{-1}{6}\right)^k \prod_{i=1}^{k} \frac{n-3i+3}{2i}\ u_0. \tag{7}$$

We know that u_0 is nonzero. If n is not divisible by three, then (7) would imply that for all $k, u_k \neq 0$. Since $p_{n-3k} = 0$ for $k > \frac{n}{3}$, we must have $n = 3m$ for some m. Then by equation (7) for $u_k = 0$ if and only if $k \geq m+1$.

Using (7) and (5) we have

$$w_{k+1} = \left(\frac{-1}{6}\right)^{k+2} \left(\frac{1}{2k+3}\right) \prod_{i=1}^{k+1} \frac{n-3i+3}{2i}\ (u'_0 - au_0) - \frac{1}{6}\left(\frac{n-3k-2}{2k+3}\right) w_k.$$

This giver a recurrence relation for the w_k. Solving this we get:

$$w_k = \left(\frac{-1}{6}\right)^k (u'_0 - au_0) \sum_{h=1}^{k} \left(\frac{1}{2h+3} \prod_{i=1}^{h} \frac{n-3i+3}{2i} \prod_{i=h+1}^{k} \frac{n-3i+1}{2i+1}\right). \tag{8}$$

For $1 \leq l \leq 3$, $p_{n-3m-l} = p_{-l} = 0$, thus $u_m = r_m = v_m = s_m = w_m = t_m = 0$. Since $w_m = 0$, equation (8) implies that $u'_0 - au_0 = 0$ (note that all of the terms in the product are l nonzero). But then (8) implies that for all k,

$$w_k = 0. \tag{9}$$

and (7) implies that for all k,

$$u'_k - au_k = 0. \tag{10}$$

Since all of the $w_k = 0$, (3) implies that for all k $v_k = 0$ and then (2) implies that all of the $r_k = 0$.

Using (7) and the fact that all of the $r_k = 0$ we can simplify (6) to

$$t_{k+1} = \left(\frac{-1}{6}\right)^{k+2} x \prod_{i=1}^{k} \frac{n-3i+3}{2i}\ u_0 - \frac{1}{6}\left(\frac{n-3k-2}{2k+2}\right) t_k.$$

Solving this reccurence relation for t_k we get:

$$
\begin{aligned}
t_k = \left(\frac{-1}{6}\right)^{k+1} x u_0 \sum_{h=0}^{k} &\left(\prod_{i=1}^{h} \frac{n-3i+3}{2i} \prod_{i=h+1}^{k} \frac{n-3i+1}{2i} \right) \\
&+ \left(\frac{-1}{6}\right)^{k} t_0 \prod_{i=1}^{k} \frac{n-3i+1}{2i}.
\end{aligned} \tag{11}
$$

Since $t_m = 0$, the above equation yields:

$$t_0 = \frac{1}{6} x u_0 \sum_{h=1}^{m} \prod_{i=1}^{h} \frac{n-3i+3}{n-3i+1}.$$

Substituting the above into (11) and simplifying we have that if $1 \leq k < m$ then:

$$t_k = \left(\frac{-1}{6}\right)^{k+1} x u_0 \left(\prod_{i=1}^{k} \frac{n-3i+1}{2i} \right) \sum_{h=k+1}^{m} \left(\prod_{i=1}^{h} \frac{n-3i+3}{n-3i+1} \right).$$

In particular for each k such that $a \leq k < m$, there is a positive rational number β_k such that $(-1)^{k+1} t_k = \beta_k x u_0$. Thus $(-1)^k t'_k = \beta_k (x u'_0 + u_0)$ [note: this is the one point in the proof where we use the fact that $D(x) = 1$ (though any positive rational would do)].

Thus

$$(-1)^{k+1}(t'_k - a t'_k) = \beta_k \big(x(u'_0 - a u_0) + u_0 \big).$$

But $u'_0 - a u_0 = 0$, so $(-1)^{k+1}(t'_k - a t'_k)$ is a positive rational multiple of u_0.

Since all of the $w_k = 0$, (4) simplifies to:

$$s_{k+1} = \left(\frac{-1}{6} \, \frac{1}{2k+1} \right) \big((t'_k - a t_k) + (n - 3k - 1) s_k \big).$$

So

$$(-1)^{k+1} s_{k+1} = (-1)^k \left(\frac{1}{6(2k+1)} \right) (t'_k - a t_k) + (-1)^k \left(\frac{n-3k-1}{6(2k+1)} \right) s_k.$$

But for $1 \leq k < m$, $(-1)^k t'_k - a t_k$ is a negative rational multiple of u_0. Using this and the fact that $s_0 = 0$, it is easy to show by induction that if $1 \leq k \leq m$, then $(-1)^k s_k$ is a positive rational multiple of u_0. In particular $s_m \neq 0$, a contradiction. This concludes the proof.

Note: The 6 in the Painlevé equation plays no role in the above proof. (ie. it would work just as well for $X'' = X^2 + x$).

Lemma 5.15 can also be used to show that $C_{F\langle\eta\rangle} = C_F$.

References

All of the details on forking and ranks can be found in Lascar's book *Stability in Model Theory*. Most of the material in this section is taken from [Poizat 2]. The analysis of the Painlevé equation is due to Kolchin, extending work of Kovacic. As far as I know it is unpublished. The version I have seen is in a letter from Kolchin to Carol Wood.

§6. Non-minimality of differential closures

In this section we will show that differential closures need not be minimal. We will find a differential field k with differential closure K such that there is a differentially closed $L \supset k$ with L properly contained in K. In this case L is also a differential closure of k, so K and L are isomorphic over k. Thus we can properly embed K into itself fixing k. This theorem was proved independently by Kolchin, Shelah and Rosenlicht. We will follow Rosenlicht's proof.

The first lemma gives a criteria for telling if a prime model is minimal.

Lemma 6.1. Let T be an ω-stable theory. Suppose $M \models T$ is prime over A. If M is minimal over A, then whenever $I \subset M$ is a set of indiscernibles over A, then I is finite.

proof.

Suppose M is minimal over A and $I \subset M$ is an infinite set of indiscernibles over A. Let $b \in I$ and let $J = I \setminus \{b\}$. Let $N \models T$ be prime over $A \cup J$. There is an elementary embedding of N into M fixing $A \cup J$. Thus, since M is minimal over A, $N = M$ and M is prime and atomic over $A \cup J$. There is $\overline{a} \in A$, $c_1, \ldots, c_n \in J$ and a formula $\phi(v, \overline{a}, \overline{c})$ isolating the type of b over $A \cup J$. Let $d \in J \setminus \{c_1, \ldots, c_n\}$. Since $\phi(v, \overline{a}, \overline{c})$ isolates $t(b/A \cup J)$,

$$M \models \phi(v, \overline{a}, \overline{c}) \rightarrow v \neq d$$

and

$$M \models \phi(b, \overline{a}, \overline{c}).$$

Since b and d are indiscernible over $A \cup \{c_1, \ldots, c_n\}$, we must have $M \models \phi(d, \overline{a}, \overline{c})$, a contradiction.

The next theorem is the algebraic core of the proof. This result will also be useful in the next section when we build many models.

Theorem 6.2 (Rosenlicht). Let $k \subset K$ be differential fields such that the C_K is algebraic over C_k. Let C denote C_k. Suppose $f \in C(X)$, $c_1, \ldots, c_n \in C$, $u_1, \ldots, u_n, v \in C(X)$ and

$$\frac{1}{f(X)} = \sum_{i=1}^{n} c_i \frac{\frac{\partial u_i}{\partial X}}{u_i} + \frac{\partial v}{\partial X}.$$

Suppose $x_1, x_2 \in K$ are solutions to $X_i' = a_i f(X_i)$, where $a_1, a_2 \in k$. If x_1 and x_2 are algebraically dependent over k, then each x_i is algebraic over k or $a_2 v(x_1)' = a_1 v(x_2)'$.

We give two partial fraction decompositions which will prove useful.

Ex 1): $f(X) = \frac{X}{1+X}$.

$$\begin{aligned}\frac{1}{f(X)} &= \frac{1}{X} + 1 \\ &= \frac{\frac{\partial}{\partial X}(X)}{X} + \frac{\partial}{\partial X}(X).\end{aligned}$$

Ex 2): $f(X) = X^3 - X^2$.

Let $u(X) = \frac{X-1}{X}$ and $v(X) = \frac{1}{X}$.

Then

$$\frac{\partial u}{\partial X} = \frac{-1}{X^2}.$$

So

$$\frac{\frac{\partial u}{\partial X}}{u} = \frac{1}{X-1} - \frac{1}{X}$$

and

$$\begin{aligned}\frac{1}{f(X)} &= \frac{1}{X^3 - X^2}\\ &= \frac{1}{X-1} - \frac{1}{X} - \frac{1}{X^2}\\ &= \frac{\frac{\partial u}{\partial X}}{u} + \frac{\partial v}{\partial X}.\end{aligned}$$

Corollary 6.3. Let C be a field of constants and $f(X) = \frac{X}{1+X}$ or $f(X) = X^3 - X^2$. Let K be the differential closure of C and let $x_1, \ldots, x_n \in K$ be nonconstant solutions to $X_i' = a_i f(X_i)$, where $a_i \in C \setminus 0$. Then $x_1, \ldots, x_n$ are algebraically independent over C.

proof.

By 2.13 C_K is algebraic over C.

We first examine the case where $f(X) = \frac{X}{X+1}$. In this case $v(X) = X$ and $v'(x_i) = x_i' = a_i \frac{x_i}{1+x_i}$.

If $a_j v(x_i) = a_i v(x_j)$, then

$$a_i a_j \frac{x_i}{1+x_i} = a_j a_i \frac{x_j}{1+x_j}.$$

In this case $x_i = x_j$.

Suppose c is a constant solution to $X' = a_i f(X)$. Then $f(c) = 0$, so $c = 0$.

Let $x_1, \ldots, x_n \in K$ be nonconstant such that $x_i' = a_i f(x_i)$ and n is minimal such that $x_1, \ldots, x_n$ are algebraically dependent over C.

$\underline{n = 1}$. Then x_1 is algebraic over C. But then x_1 is constant (by 2.1), a contradiction.

$\underline{n > 1}$. Then x_n and x_{n-1} are algebraically dependent over $C(x_1, \ldots, x_{n-2})$. Neither x_{n-1} nor x_n is algebraic over $C(x_1, \ldots, x_{n-2})$, so by Theorem 6.2, $a_n v(x_{n-1})' = a_{n-1} v(x_n)'$. But then, $x_{n-1} = x_n$, a contradiction.

In the second case $v(x) = \frac{1}{x}$ and $v(x)' = a_i(1 - x_i)$. Thus if $a_i v(x_j)' = a_j v(x_i)'$, $x_i = x_j$. The only constant solutions of $X' = a_i f(X)$ are zero and one. The remainder of the proof is similar.

Corollary 6.4. Let C be a field of constants. Let K be the differential closure of C. Then K is not minimal over C.

proof.

Since K is differentially closed it contains infinitely many solutions to $y' = f(y)$, where f is one of the above functions. Let $x_1, x_2, \ldots$ be $\aleph_0$ nonconstant solutions. By 6.3 the x_i are algebraically independent over C. For any $x_{j_1}, \ldots, x_{j_m}$, since $x_i' = f(x_i)$ and $f(X) \in C(X)$, $C\langle x_{j_1}, \ldots, x_{j_m}\rangle = C(x_{j_1}, \ldots, x_{j_m})$. Thus the type of $x_{j_1}, \ldots, x_{j_m}$ is determined by

$$\bigwedge (v_i' = f(v_i) \wedge v_i' \neq 0) \wedge p(v_1, \ldots, v_m) \neq 0,$$

for p a nonzero polynomial over C. Thus the x_i are a set of indiscernibles. So, by 6.1, K is not minimal over C.

The proof of Rosenlicht's theorem uses the abstract theory of differential forms.

Suppose $k \subset K$ are fields. We define $\Omega_{K/k}$ the space of differential forms on K over k (when no ambiguity arises we will drop the subscripts).

Let Ω be the K-vector space generated by the set $\{dx : x \in K\}$, where we mod out by the relations:

$d(x+y) = dx + dy$,

$d(xy) = xdy + ydx$, and

$d(a) = 0$ for $a \in k$.

It is easy to see that for $p(X) \in k[X]$, $d(p(x)) = \frac{\partial p}{\partial X}(x)dx$.

The space of differential forms Ω satisfies a universal mapping property given by the following lemma.

Lemma 6.5. If $D : K \to K$ is a k-derivation (ie. $k \subseteq C_K$), then there is a K-linear $\xi : \Omega \to K$ such that $D = \xi \circ d$.

Proof.

Let $\xi(dx) = D(x)$. This is well defined since:
$\xi(d(x+y)) = D(x+y) = D(x) + D(y) = \xi(dx) + \xi(dy)$,
$\xi(d(xy)) = D(xy) = xD(y) + yD(x) = x\xi(dx) + y\xi(dx)$, and
$\xi(da) = D(a) = 0 = \xi(0)$, for $a \in k$.

We next show that the dimension of Ω as a K-vector space is equal to the transcendence degree of K/k. The proof uses two facts about extensions of derivations which we summarize in the next lemma (for proofs see Lang's *Algebra*).

Lemma 6.6. Let K be a field and let $D : K \to K$ be a derivation.

a) Let a be any element of $K(X)$, then D extends to a derivation $D^* : K(X) \to K(X)$, with $D^*(X) = a$.

b) If L/K is separable algebraic, then D extends to a derivation on L.

Lemma 6.7. $\dim_K \Omega = td(K/k)$.

Proof.

Suppose $t_1, \ldots, t_n \in K$ and $p(X_1, \ldots, X_n) \in k[\overline{X}]$ is of minimal degree such that $p(\overline{t}) = 0$. Then

$$dp(\overline{t}) = \sum_{i=1}^{n} \frac{\partial p}{\partial X_i}(\overline{t}) dt_i = 0.$$

Since the degree of p is minimal, for some i, $\frac{\partial p}{\partial X_i}(\overline{t}) \neq 0$. Thus $dt_1, \ldots, dt_n$, are linearly dependent over K. Thus $\dim_K(\Omega) \leq td(K/k)$.

Suppose $t_1, \ldots, t_n$ are algebraically independent over k. By 6.6, we can find derivations $D_i : K \to K$ such that

$$D(t_i) = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{otherwise.} \end{cases}$$

Let $\xi_i : \Omega \to K$ such that $D_i = \xi_i \circ d$.

Suppose $a_1, \ldots, a_n \in K$ and

$$\sum_{j=1}^{n} a_j dt_j = 0.$$

Then

$$\begin{aligned} 0 &= \xi_i(\sum_{j=1}^{n} a_j dt_j) \\ &= \sum_{j=1}^{n} a_j D_i(t_j) \\ &= a_i. \end{aligned}$$

Thus $dt_1, \ldots, dt_n$ are linearly independent, so $\dim_K \Omega \geq td(K/k)$.

Corollary 6.8. If $t \in K$, then t is algebraic over k if and only if $dt = 0$.

Suppose $D : K \to K$ is a derivation. Let $D' : \Omega \to \Omega$, be defined by

$$D'\Big(\sum x_i dy_i\Big) = \sum \Big(D(x_i)dy_i + x_i d(D(y_i)\Big).$$

The following properties are easy to verify for $x \in K$, $\omega, \eta \in \Omega$:

$$\begin{aligned} D'(\omega + \eta) &= D'(\omega) + D'(\eta) \\ D'(x\omega) &= D(x)\omega + xD'(\omega) \\ D'(dx) &= d(D(x)). \end{aligned}$$

Lemma 6.9. Let $D : K \to K$, be a derivation such that $D|k$ is a derivation on k. If x, y in K are algebraically dependent over C_k, then $D(y)dx = D(x)dy$ and $D'(xdy) = d(xDy)$.

Proof. Let $p(X,Y) \in C_k[X,Y]$, be such that $p(x,y) = 0$.

Since $p(x,y) = 0$, $d(p(x,y)) = 0$. But

$$d(p(x,y)) = \frac{\partial p}{\partial X}(x,y)dx + \frac{\partial p}{\partial Y}(x,y)dy.$$

So

$$\frac{dy}{dx} = -\frac{\frac{\partial p}{\partial X}}{\frac{\partial p}{\partial Y}}(x,y).$$

Also, since the coefficients of p are constant, $D(p(x,y)) = \frac{\partial p}{\partial X}D(x) + \frac{\partial p}{\partial Y}D(y)$ (see lemma 5.10). Thus

$$\frac{D(y)}{D(x)} = -\frac{\frac{\partial p}{\partial X}}{\frac{\partial p}{\partial Y}}(x,y).$$

So $D(x)dy = D(y)dx$.

Finally

$$\begin{aligned} D'(xdy) &= D(x)dy + xd(D(y)) \\ &= D(y)dx + xd(D(y)) \\ &= d(xD(y)). \end{aligned}$$

Lemma 6.10. Suppose $u_1, \ldots, u_n, v \in K$ and all the u_i are nonzero. Suppose $c_1, \ldots, c_n \in k$ are linearly independent over $\mathbf{Q}$. Let

$$\omega = dv + \sum_{i=1}^{n} c_i \frac{du_i}{u_i}.$$

Then $\omega = 0$ if and only $du_1 = \ldots = du_n = dv = 0$ (ie. all of the u_i and v are algebraic over k).

Proof.

<u>case 1</u>. $u_1, \ldots, u_n$ are algebraic over k.

Then all of the $du_i = 0$. Thus $\omega = 0$ if and only if $dv = 0$ if and only if v is algebraic over k.

Thus we may assume that some u_i is transcendental over k. Without loss of generality assume u_1 is transcendental over k. We will show this leads to a contradiction.

<u>case 2</u>. u_1 is transcendental over k and $u_2, \ldots, u_n, v \in k(u_1)$.

We can give formal Laurent series expansions for u_j and v in terms of u_1. Say

$$u_j = \sum_{i=m_j}^{\infty} \alpha_{j,i} u_1^i, \quad \text{and}$$

$$v = \sum_{i=l}^{\infty} \beta_i u_1^i.$$

Then

$$du_j = \sum_{i=m_j-1}^{\infty} (i+1)\alpha_{j,i+1} u_1^i du_1, \quad \text{and}$$

$$dv = \sum_{i=l-1}^{\infty} (i+1)\beta_{i+1} u_1^i du_1.$$

In particular in this expansion $dv = f(u_1)du_1$, where $f(u_1)$ is a Laurent series where the coefficient of u_1^{-1} is zero.

Thus

$$\frac{du_j}{u_j} = du_1(m_j u_1^{-1} + \text{higher degree terms})$$

If $\omega = 0$, then comparing the u_1^{-1} coefficients we see that

$$c_1 + \sum_{j=2}^{n} m_j c_j = 0.$$

This is a contradiction, since $c_1, \ldots, c_n$ are linearly independent over $\mathbf{Q}$.

Finally we show that we can reduce to case 2. Suppose u_1 is transcendental over k. Let $u_1, t_1 \ldots t_m$ be a transcendence base for $u_1, \ldots, u_n, v$ over k. Consider the natural homomorphism $\phi : \Omega_{K/k} \to \Omega_{K/k(t_1 \ldots t_n)}$. If $\omega = 0$, then $\phi(\omega) = 0$. We replace k by $k(t_1 \ldots t_n)$. Thus we assume that u_1 is transcendental over k and $u_2 \ldots u_n, v$ are algebraic over $k(u_1)$.

We also replace K by a finite algebraic extension of $k(u_1, \ldots, u_n, v)$ so that $K/k(u_1)$ is Galois.

Let $G = Gal(K/k(u_1))$. For $\sigma \in G$, let

$$\omega^\sigma = \sum c_i \frac{d\sigma u_i}{\sigma u_i} + d\sigma v$$

.

Each $\omega^\sigma = 0$. Let $\eta = \sum_{\sigma \in G} \omega^\sigma$.

For $j = 2, \ldots, n$, let

$$u_j^{\#} = \prod_{\sigma \in G} \sigma u_j.$$

Then $u_j^{\#} \in k(u_1)$ and

$$du_j^{\#} = \sum_{\sigma \in G} (\prod_{\tau \neq \sigma} \tau u_j) d\sigma u_j.$$

Let

$$v^{\#} = \sum_{\sigma \in G} \sigma v$$

$$dv^{\#} = \sum_{\sigma \in G} d\sigma v.$$

Thus

$$\eta = [K : k(u_1)]c_1 \frac{du_1}{u_1} + \sum_{i=2}^{n} c_i \frac{du_i^{\#}}{u_i^{\#}} + dv^{\#}.$$

Replacing u_j by $u_j^{\#}$ for $j > 2$, v by $v^{\#}$, and c_1 by $[K : k(u_1)]c_1$, we have reduced to case 2.

Remark. The fact that the constants $c_1, \ldots, c_n$ are linearly independent over $\mathbf{Q}$ is a red-herring. Note that:

i) $\frac{d(xy)}{xy} = \frac{dx}{x} + \frac{dy}{y}$

ii) $\frac{da^n}{a^n} = n\frac{da}{a}$ for $n \in \mathbf{N}$.

Using these two facts it is easy to see that for any $\sum c_i \frac{du_i}{u_i}$ can be rewritten as $\sum b_i \frac{dw_i}{w_i}$ where the b_i are linearly independent over $\mathbf{Q}$.

We are now ready to prove theorem 6.2 which we repeat for convenience.

Theorem 6.2 (Rosenlicht). Let $k \subset K$ be differential fields such that the C_K is algebraic over C_k. Let C denote C_k. Suppose $f \in C(X)$, $c_1, \ldots, c_n \in C, u_1, \ldots, u_n, v \in C(X)$ and

$$\frac{1}{f(X)} = \sum_{i=1}^{n} c_i \frac{\frac{\partial u_i}{\partial X}}{u_i} + \frac{\partial v}{\partial X}.$$

Suppose $x_1, x_2 \in K$ are solutions to $X_i' = a_i f(X_i)$, where $a_1, a_2 \in k$. If x_1 and x_2 are algebraically dependent over k, then each x_i is algebraic over k or $a_2 v(X_1)' = a_1 v(X_2)'$.

proof of 6.2.

We may assume that $K = k(x_1, x_2)$. Suppose x_1 and x_2 are algebraically dependent over k, but neither is algebraic over k. Thus $td(K/k) = 1$. By lemma 6.7, $dim_K \Omega = 1$. In particular, $\frac{dx_i}{f(x_i)}$ generates Ω as a K-vector space. Thus there is a nonzero $c \in K$ such that

$$\frac{dx_2}{f(x_2)} = c\frac{dx_1}{f(x_1)} \tag{1}$$

.

We claim that c is a constant.

By lemma 6.9 (with $x = \frac{1}{f(x_i)}, y = x_i$).

$$D'\Big(\frac{dx_i}{f(x_i)}\Big) = d\Big(\frac{x_i'}{f(x_i)}\Big) = d(a_i) = 0$$

since $a_i \in k$.

Thus

$$\begin{aligned}
0 &= D'(\frac{dx_2}{f(x_2)}) \\
&= D'(c\frac{dx_1}{f(x_1)}) \\
&= D(c)\frac{dx_1}{f(x_1)} + cD'(\frac{dx_1}{f(x_1)}) \\
&= D(c)\frac{dx_1}{f(x_1)}.
\end{aligned}$$

But then $D(c) = 0$ so c is constant and hence algebraic over k.

We now use our expression for f and the fact that $d(w(x)) = \frac{\partial w}{\partial X}dx$ for $w(X) \in C_k(X)$.

$$\begin{aligned}
\frac{dx_i}{f(x_i)} &= \sum_{j=1}^{n} c_j \frac{\frac{\partial u_j}{\partial X}}{u_j}(x_i)dx_i + \frac{\partial v}{\partial X}(x_i)dx_i \\
&= \sum_{j=1}^{n} c_j \frac{d(u_j(x_i))}{u_j(x_i)} + d(v(x_i)).
\end{aligned}$$

So by (1)

$$\sum_{j=1}^{n} c_j \frac{d(u_j(x_2))}{u_j(x_2)} + d(v(x_2)) = c\Bigg(\sum_{j=1}^{n} c_j \frac{d(u_j(x_1))}{u_j(x_1)} + d(v(x_1))\Bigg). \tag{2}$$

Since $c \in C_K$, c is algebraic over C_k. Thus by corollary 6.8 $dc = 0$. Thus we can rewrite (2) as

$$\sum_{j=1}^{n} c_j \Bigg(\frac{d(u_j(x_2))}{u_j(x_2)} - \frac{d(cu_j(x_1))}{u_j(x_1)}\Bigg) + d(v(x_2) - cv(x_1)\Bigg) = 0. \tag{3}$$

We now apply lemma 6.10 (and the remark following it) to (3). Thus

$$d(v(x_2) - cv(x_1)) = 0 \qquad (4).$$

Finally,

$$\begin{aligned}
a_1 v(x_2)' &= a_1 \frac{\partial v}{\partial X}(x_2)x_2' \\
&= a_1 a_2 \frac{\partial v}{\partial X}(x_2) f(x_2) \\
&= a_1 a_2 \frac{d(v(x_2))}{\frac{dx_2}{f(x_2)}}.
\end{aligned}$$

Similarly

$$a_2 v(x_1)' = a_1 a_2 \frac{d(v(x_1))}{\frac{dx_1}{f(x_1)}}.$$

By (1) and (4)

$$\frac{d(v(x_2))}{\frac{dx_2}{f(x_2)}} = \frac{cd(v(x_1))}{c\frac{dx_1}{f(x_1)}}.$$

Thus

$$a_1 v(x_2)' = a_2 v(x_1)',$$

as desired.

We conclude this section with a proof that in Rosenlicht's extensions we do not add new constants. This will be useful in the next section.

Definition. We say that E/F is a *function field* if there is $t \in E$ transcendental over F and E is a finite algebraic extension of $F(t)$.

If F is algebraically closed, then function fields correspond to isomorphism classes of smooth projective curves over F. If E/F is a function field, then the *genus* of E is the genus of the corresponding curve.

Lemma 6.11. Let K/k be differential fields such that K/k is a function field and C_k is algebraically closed. If $C_K \neq C_k$, then C_K/C_k is a function field and the genus of C_K/C_k is at most the genus of K/k.

Proof.

Suppose $C_K \neq C_k$ and $t \in C_K - C_k$. Then t is transcendental over C_k. The arguments from the proof of 2.13 show t is transcendental over k.

claim. $C_{k(t)} = C_k(t)$.

Suppose $D(p(t)) = 0$, where $p(X) = \sum a_i X^i \in k[X]$. Then

$$D(p(t)) = D(t)\sum i a_i t^{i-1} + \sum D(a_i)t^i = \sum D(a_i)t^i.$$

Since t is transcendental over k, we must have all $D(a_i) = 0$, so $a_i \in C_k$. Thus $p(t) \in C_k(t)$.

Suppose $p(X)$ and $q(X)$ are in $k[X]$ and $D(\frac{p(t)}{q(t)}) = 0$. We may assume that q is monic and that for any q_0 of lower degree there is no p_0 such that $\frac{p_0(t)}{q_0(t)} = \frac{p(t)}{q(t)}$. Since $D(\frac{p(t)}{q(t)}) = 0$, $q(t)D(p(t)) - p(t)D(q(t)) = 0$. But then $\frac{D(p(t))}{D(q(t))} = \frac{p(t)}{q(t)}$. But if $q(X) = X^n + \sum_{i=0}^{n-1} b_i X^i$, then $D(q(t)) = \sum_{i=0}^{n-1} D(b_i)t^i$, contradicting the minimality of q.

claim. C_K/C_k is a function field.

We know that t is a transcendence base for K over k. Assume that $K/k(t)$ is an algebraic extension of degree N. Let $x \in C_K - C_{k(t)}$. Let $f(X) \in k(t)[X]$, be the minimal polynomial of x over K. The degree of f is at most N. Let $f(X) = X^m + \sum b_i X^i$. $0 = D(f(x)) = \sum_{i=0}^{n-1} D(b_i)x^i$. Since this polynomial has lower degree, we must have all of the $D(b_i) = 0$. So $f(X) \in C_{k(t)}[X]$. Thus $[C_K : C_{k(t)}] \leq N$. So C_K/C_k is a function field.

Let α be a generator for $C_K/C_{k(t)}$. Let $f(X,Y) \in C_k[X,Y]$ such that $f(t,Y)$ is the minimal polynomial of α over $C_{k(t)}$. By the above arguments $f(t,Y)$ is also the minimal polynomial of α over $k(t)$. Thus $k(t,\alpha)$ is a function field of the same genus as C_K/C_k. Since $k(t,\alpha) \subseteq K$, the genus of K/k is at least the genus of $k(t,\alpha)/k$ (there can be no maps from a curve of genus g to a curve of genus $g_1 > g$ [by Hurwitz formula]).

Theorem 6.12. Let k be a differential field such that $C = C_k$ is algebraically closed. Let $f(X) \in C_k(X)$ and let x be a solution of the differential equation $D(X) = f(X)$, where x is transcendental over k. Suppose that $\frac{1}{f(X)}$ is not of the form $c\frac{\partial u}{\partial X}/u$ or $c\frac{\partial v}{\partial X}$ for any u or $v \in C(X), c \in C$. Then $C_{k(x)} = C$.

Proof.

Suppose $C_{k(x)} \neq C$. By 6.11, $C_{k(x)}$ is a genus 0 function field over C. Thus there is $t \in C_{k(x)}$ such that $C_{k(x)} = C(t)$.

Consider the non-zero differentials dt and $\frac{dx}{f(x)}$ in $\Omega_{k(x)/k}$. By 6.7 there is $g \in k(x)$ such that $\frac{dx}{f(x)} = gdt$.

$D'(gdt) = D(g)dt + gD'(dt) = D(g)dt + gd(D(t)) = D(g)dt$. While by 6.9
$D'(\frac{dx}{f(x)}) = d\big(\frac{D(x)}{f(x)}\big) = d(1) = 0$.
Thus $D(g) = 0$, so $g \in C(t)$.

Using the partial fraction decomposition of $\frac{1}{f(x)} \in C(x)$, we can write

$$\frac{dx}{f(x)} = \sum_{i=1}^{n} c_i \frac{du_i}{u_i} + dv$$

where $c_i \in C$, $u_i, v \in C(x)$. Using the remarks after the proof of 6.10 we can choose this decomposition so that $c_1, \ldots, c_n$ are linearly independent over $\mathbf{Q}$.

Since $g \in C(t)$, we can use the partial fraction decomposition of g to write

$$gdt = \sum_{i=1}^{m} b_i \frac{dw_i}{w_i} + dy$$

where $b_i \in C$ and $w_i, y \in C(t)$.

Let $c_1, \ldots, c_n, c_{n+1}, \ldots, c_N$ be a basis for the span of $c_1, \ldots, c_n, b_1, \ldots, b_m$ over $\mathbf{Q}$. Using the remarks after 6.10, letting $u_j = 1$ for $j = n+1, \ldots, N$ and suitably defining the w_i, we can may assume:

$$\frac{dx}{f(x)} = \sum_{i=1}^{N} c_i \frac{du_i}{u_i} + dv$$

$$gdt = \sum_{i=1}^{N} b_i \frac{dw_i}{w_i} + dy$$

where $b_i = \frac{c_i}{M}$ for some $M \in \mathbf{Z}$.

Note that

$$Mc_i\frac{du_i}{u_i} - c_i\frac{dw_i}{w_i} = c_i\Big(\frac{d(u_i^M/w_i)}{u_i^M/w_i}\Big).$$

Thus we may use the fact that $gdt = \frac{dx}{f(x)}$ to conclude that

$$\sum_{i=1}^{N} c_i \frac{d(u_i^M/w_i)}{u_i^M/w_i} + d(Mv - y) = 0.$$

By 6.10, $d(u_i^M/w_i) = 0$ for each i and $d(Mv - y) = 0$. Since $k(x)$ is a purely transcendental extension of k, by 6.8 each $u_i^M/w_i \in k$ and $Mv - y \in k$.

For each i, $D(\frac{u_i^M}{w_i}) = \frac{M}{w_i}u_i^{M-1}D(u_i)$, since $w_i \in C(t) = C_{k(x)}$. Thus $\frac{D(u_i)}{u_i} \in k$. We also have $D(v) \in k$. But $u_1, \ldots, u_n, v \in C(x)$. Thus $\frac{D(u_i)}{u_i}$ and $D(v) \in k \cap C(x) = C$.

For any $h \in C(x)$, $D(h) = \frac{\partial h}{\partial X}D(x) = \frac{\partial h}{\partial X}f(x)$. At least one of $u_1, \ldots, u_N, v$ is not in k, for otherwise $dx = 0$. Thus at least one of $\frac{\frac{\partial u_i}{\partial x}}{u_i}f$ or $\frac{\partial v}{\partial x}f$ is a nonzero element of C. Thus $\frac{1}{f(x)}$ is of one of the forms stated in the theorem.

References

The nonminimality of differential closures was proved in [Kolchin 3], [Rosenlicht 1] and [Shelah]. Shelah's and Rosenlicht's arguments are discussed in [Gramain 1] and [Gramain 2].

[Rosenlicht 2] contains some of the theory of differential forms that we use. This work is an extension of earlier work of Ax.

[Brestovski] contains several extensions of Rosenlicht's ideas.

§7. The number of non-isomorphic models

In this section we will prove that if κ is uncountable, then there are 2^κ non-isomorphic differentially closed fields of cardinality κ, while also analyzing orthogonality and strongly regular types. The number of countable models was only recently shown to be $2^{\aleph_0}$ by Hrushovski and Sokolović. Pillay's paper in this volume contains a proof of this result. [Through out this section we assume a reasonable knowledge of stability theory. References [L] are to Lascar's *Stability in Model Theory*, while [B] is Baldwin's *Fundamentals of Stability Theory*.]

We say that $\overline{a}$ and $\overline{b}$ are *independent* over k if the $t(\overline{a}/k\langle\overline{b}\rangle)$ does not fork over k. We write $\overline{a}\mathop{\smile\!\!\!\!\!\mid}_k\overline{b}$. Recall that the $a\mathop{\smile\!\!\!\!\!\mid}_k\overline{b}$ if and only if $RD(a/k) = RD(a/k\langle\overline{b}\rangle)$. We say that a type is *stationary* if over any extension of the domain there is there is a unique non-forking extension. For $p \in S_1(k)$, p is stationary if and only if the minimal polynomial of p is absolutely irreducible.

Lemma 7.1. Suppose $K \models DCF$ and F is the differential closure of $K\langle\overline{b}\rangle$. If $a \in F - K$ then $a \not\mathop{\smile\!\!\!\!\!\mid}_K \overline{b}$.

Proof.
Let $\psi(v,\overline{b})$ isolate $t(a/K\langle\overline{b}\rangle)$. For all $m \in K$, $\psi(v,\overline{b}) \to v \neq m$.
Suppose $a\mathop{\smile\!\!\!\!\!\mid}_K\overline{b}$. By symmetry $\overline{b}\mathop{\smile\!\!\!\!\!\mid}_K a$ (see [L] 3.5). Thus $t(\overline{b}/K\langle a\rangle)$ is the heir of $t(\overline{b}/K)$. Since $t(\overline{b}/K\langle a\rangle)$ represents $\psi(v,\overline{w})$, there is $a_0 \in K$ such that $\psi(a_0,\overline{b})$. But then $\psi(a_0,\overline{b}) \to a_0 \neq a_0$, a contradiction.

Note that the above argument works for any stable theory with prime models.

Definition. Let $K \models DCF$ and $p, q \in S_1(K)$. We say that p and q are *orthogonal* if and only if for any a realizing p and b realizing q, $a\mathop{\smile\!\!\!\!\!\mid}_K b$. We write $p \perp q$.

The above notion is usually called *almost orthogonality*. For types over models of an ω-stable theory these notions are equivalent (see [L] 8.23). If $p \in S(k)$ and $q \in S(l)$, we say that $p \perp q$ if and only if for any differentially closed $K \supset k \cup l$, if p' and q' are non-forking extensions of p and q to K, then $p' \perp q'$. In general if $p \perp q$ and p' and q' are nonforking extensions of p and q respectively, then $p' \perp q'$.

Lemma 7.2. If $K \models DCF$, $p, q \in S_1(K)$, $p \perp q$, a realizes p and F is the differential closure of $K\langle a\rangle$, then q is not realized in F.

Proof. Clear from 7.1.

Lemma 7.3. Suppose $F \supset K$ are differentially closed, $\phi(v)$ is a formula with parameters from K and every element of F that satisfies $\phi(x)$ is already in K. Let $a \in F - K$, let $p = t(a/K)$ and let $q \in S_1(K)$ be a type containing $\phi(v)$. Then $p \perp q$.

Proof. Let b realize q. Let $r(X) \in K\{X\}$ be the minimal polynomial of q. If $b \not\mathop{\smile\!\!\!\!\!\mid}_K a$, there are $g(X), h(X) \in K\langle a\rangle\{X\}$, such that $g(b) = 0$, the order of g is less than the order of r, the order of $h(X)$ is less than the order of $g(X)$ and

$$g(x) = 0 \wedge h(x) \neq 0 \rightarrow \phi(x).$$

Since $\phi(v)$ has no new solutions in F,

$$\{x \in F : F \models g(x) = 0 \wedge h(x) \neq 0\} = \{x \in K : F \models g(x) = 0 \wedge h(x) \neq 0\}.$$

By definability of types and model completeness, there is a formula $\psi(v)$ with parameters from K such that

$$\{x \in K : F \models g(x) = 0 \wedge h(x) \neq 0\} = \{x \in K : K \models \psi(x)\} = \{x \in F : F \models \psi(x)\}.$$

Note that $\psi(b)$ holds. But $F \models$ "there are polynomials g and h such that g has order less than r and h has order less than g such that $(g(x) = 0 \wedge h(x) \neq 0)$ if and only if $\psi(x)$. Thus by model completeness there are $g_0, h_0 \in K\{X\}$ such that $g_0(x) = 0 \wedge h_0(x) \neq 0$ is equivalent to $\psi(x)$. In particular $g_0(b) = 0$ contradicting the fact that r is the minimal polynomial of $t(b/K)$.

As an application of 7.3 suppose $p \in S_1(K)$ is the type of a differential transcendental. Let K_p be the prime model over a realization of p. We first note that every element of $K_p \setminus K$ is differentially transcendental over K. Suppose not. Let $b \in K_p - K$, and suppose $f(b) = 0$ for some $f(X) \in K\{X\}$. Then $RD(b/K) \leq ord(f)$, but by 7.1 $a \not\downarrow_K b$. Thus $RD(a/K\langle b\rangle) < \omega$. But RD is transcendence degree. Thus if $td(K\langle a, b\rangle/K\langle b\rangle) < \omega$ and $td(K\langle b\rangle/K) < \omega$, then $td(K\langle a\rangle/K) < \omega$ contradicting the fact that a is a differential transcendental.

In particular if $f \in K\{X\}$, $f(X) = 0$ has no solutions in $K_p - K$. Thus by 7.3 if $q \in S_1(K)$ and $q \neq p$, $q \perp p$.

Definition. Let $K, F \models DCF$. Let $p \in S(F)$. We say $p \perp K$ if and only if for all $q \in S(K)$, if q' is a non-forking extension of q to F then $p \perp q'$.

We use the following fact (see [B] VI 2.23).

Lemma 7.4. If $M \subset N \models T$ and f is an elementary map with domain N such that $N \downarrow_M f(N)$, then $p \perp M$ if and only if $p \perp f(p)$.

Definition. T has the *dimension order property* (DOP) if and only if there are M_0, M_1, M_2, M_3 models of T such that:

1) $M_0 \subseteq M_1 \cap M_2$
2) $M_1 \downarrow_{M_0} M_2$
3) M_3 is prime over $M_1 \cup M_2$.
4) There is p such that $p \perp M_1$, $p \perp M_2$, and $p \not\perp M_3$.

The interest of the dimension order property is the following theorem of Shelah (see [B] XVI).

Theorem 7.5 If T is ω-stable with DOP, then for any uncountable κ there are 2^κ non-isomorphic models of T of power κ.

Theorem 7.6 Differentially closed fields have DOP.

Proof.

Let $K \models DCF$. Let b_1, b_2 be independent differential transcendental over K. Let K_i, $i = 1, 2$ be the differential closure of $K\langle b_i \rangle$. Let K_3 be the differential closure of $K\langle b_1, b_2 \rangle$.

Let $p \in S_1(K_3)$ be the type of a generic solution of $X' = b_1 b_2 f(X)$, where $f(X) = X^3 - X^2$ (or $f(X) = \frac{X}{X+1}$). Clearly $p \not\perp K_3$.

We claim that $p \perp K_1$. By 7.4 it suffices to show that if b_3 is differentially transcendental over K, $b_3 \mathop{\smile\!\!\!\!\!\!|}_{K_1} b_2$, and q is the type of a generic solution of $X' = b_1 b_3 f(X)$, then $p \perp q$.

Let F be the differential closure of $K\langle b_1, b_2, b_3 \rangle$ and identify p and q with their non-forking extensions to F. Let x_1 and x_2 be realizations of p and q over F. We claim that $x_1 \mathop{\smile\!\!\!\!\!\!|}_F x_2$. Let $L = F\langle x_1, x_2 \rangle$. Since $x_i' \in F(x_i)$, it is easy to see that $F(x_i) = F\langle x_i \rangle$ and $L = F(x_1, x_2)$. Since $RD(p) = RD(q) = 1$, these are types of $RU(p) = RU(q) = 1$. If $t(x_2/F\langle x_1 \rangle)$ forks over F, then x_2 is algebraic over $F(x_1)$.

We will apply Rosenlicht's theorem with $k = F$ and $K = L$. We need to show that C_L is algebraic over C_F. By theorem 6.12, $C_F = C_{F(x_1)}$. In general if K/k is algebraic then C_K/C_k is algebraic. [Let $c \in C_K$, let $\sum a_i X^i$ be the minimal polynomial of c over k, where the leading $a_i = 1$. Then $0 = D(\sum a_i c^i) = \sum D(a_i) c^i + D(c) \sum i a_i c^{i-1}$. So $\sum D(a_i) X^i$ vanishes at c but this has lower degree unless all of the a_i are constants.] Thus C_L is algebraic over C_F.

By Rosenlicht's theorem, $b_1 b_2 v(x_2)' = b_1 b_3 v(x_1)'$. As we saw in 6.3, this implies $x_1 = x_2$, but this is impossible since $b_1 b_2 \neq b_1 b_3$.

Similarly $p \perp K_2$, so p witnesses DOP.

Corollary 7.7 For $\kappa \geq \aleph_1$, there are 2^κ non-isomorphic differentially closed field of power κ.

The idea of the proof is the following. Fix M a differentially closed field of power κ containing $(a_\alpha, b_\alpha : \alpha < \kappa)$ independent differential transcendentals.

Let R be a binary relation on κ. We can find M_R differentially closed of power κ. Such that $R(\alpha, \beta)$ if and only if $X' = a_\alpha b_\beta f(X)$ has $\aleph_1$ solutions and $\neg R(\alpha, \beta)$ if and only if $X' = a_\alpha b_\beta f(X)$ has $\aleph_0$ solutions. This idea can be used to build 2^κ non-isomorphic models. (For example this shows that if Q is the quantifier "there exists uncountably many" DCF is unstable in $L(Q)$.)

We conclude this section with some remarks on strongly regular types and orthogonality.

Notation: If $K \models DCF$ and $p \in S_1(K)$ we let K_p denote the prime model over a realization of p and we let f_p denote the minimal polynomial of p.

Definition. Let $K \models DCF$. A nonalgebraic type $p \in S_1(K)$ is *strongly regular* if and only if for any $a \in K_p - K$, if $f_p(a) = 0$, then $p = t(a/K)$.

If $p \in S_1(k)$ is stationary, p is strongly regular if and only if for any differentially closed $K \supset k$, the non-forking extension of p to K is strongly regular.

If $K, F \models DCF$, $K \subset F$, $p \in S_1(K)$, $q \in S_i(F)$, q is a non-forking extension of p and p is strongly regular, then q is strongly regular. (See [L] 8.9).

Two important types are easily seen to be strongly regular. Let $t_c \in S_1(K)$ be the type of a new constant and let $t_g \in S_1(K)$ be the type of a differential transcendental. Clearly every constant in $K_{t_c} - K$ realizes t_c and every new element of $K_{t_g} - K$ realizes t_g (see the argument following 7.3). Note that in the case of t_g the minimal polynomial is 0.

The next lemma shows that strongly regular types are abundant.

Lemma 7.8 If $F, K \models DCF$ and $K \subset F$ then there is $a \in F - K$ such that $t(a/K)$ is strongly regular.

Proof. Choose $a \in F - K$ such that $RD(a/K)$ is minimal. If $RD(a/K) = \omega$, then a is differentially transcendental over K, and $t(a/K)$ is strongly regular. Otherwise, let f be the minimal polynomial of $t(a/K)$. If $b \in F - K$ and $f(b) = 0$, then $RD(b/K)$ is at most the order of f. By the minimality of $RD(a/K)$, $RD(b/K)$ is equal to the order of f. Thus f is the minimal polynomial of $t(b/K)$, and $t(b/K) = t(a/K)$. Hence $t(a/K)$ is strongly regular.

Lemma 7.9. If $K \models DCF$ and $p \in S_1(K)$ has $RU(p) = 1$, then p is strongly regular.

Proof.

Let a realize p and let K_p be prime over $K\langle a \rangle$. Suppose $b \in K_p - K$ and $f_p(b) = 0$. By 7.1 $a \not\downarrow_K b$. Thus $RU(a/K\langle b \rangle) = 0$ and a is algebraic over $K\langle b \rangle$. Let $g(X)$ be the minimal polynomial of $t(b/K)$. Since $f(b) = 0$, the order of g is at most the order of f. The order of f is equal to the transcendence degree of $K\langle a \rangle/K$,while the order of g is equal to the transcendence degree of $K\langle b \rangle/K$. Since a is algebraic over $K\langle b \rangle$, f and g must have the same order. But then since $f \in I(g)$, f and g are multiples of each other by an element of K. So $t(b/K) = p$.

Lemma 7.10. Suppose $p \in S_1(K)$ is strongly regular and $f(X)$ is the minimal polynomial of p. Let $q \in S_1(K)$ be such that "$f(v) = 0$" $\in q$ and $RD(q) < RD(p)$. Then $q \perp p$.

Proof.

Let g be the minimal polynomial of q. Then $K_p \setminus K$ contains no elements satisfying $f(x) = g(x) = 0$. Thus, by lemma 7.3, $p \perp q$.

Lemma 7.11. Suppose $p \in S_1(K)$ is strongly regular, and $K \subseteq K' \subseteq K_p$, and $K \neq K'$, then $K_p \cong K'$.

Proof.

Let a realize p and let K_p be prime over $K\langle a \rangle$. Suppose $b \in K' - K$. First, suppose $K' - K$ contains no solutions to $f_p(X) = 0$, then $t(b/K) \perp p$. But since $b \in K_p$, $a \not\downarrow_K b$, a contradiction. Thus $K' - K$ contains a solution d to $f_p(X) = 0$. Since p is strongly regular

$t(d/K) = p$. Thus K' contains a realization of p, and hence is prime over a realization of p. By uniqueness of prime models $K' \cong K_p$.

Definition. We define the *Rudin-Keisler order* on $S_1(K)$ as follows. Let $p, q \in S_1(K)$. We say $p \geq_{RK} q$ if and only if q is realized in K_p. We say $p \sim_{RK} q$ if $p \geq_{RK} q$ and $q \geq_{RK} p$.

Corollary 7.12. If $p \in S_1(K)$ be strongly regular, $q \in S_1(K)$ is non-algebraic and $p \geq_{RK} q$, then $p \sim_{RK} q$.

Proof.

We can embed $K_q \subset K_p$ such that $K_q \neq K$. By 7.10, K_q contains a realization of p.

Lemma 7.13. Let $p, q, r \in S_1(K)$. Suppose $r \geq_{RK} p$ and $r \perp q$, then $p \perp q$.

Proof. Let a, b realize p, q. Since $r \geq_{RK} p$, we can find d realizing r such that a is in the differential closure of $K\langle d\rangle$. Since $q \perp r$, $b \mathop{\smile\!\!\!\!\!\!\mid}_K d$. In particular we can find a differentially closed field $F \supset K\langle d\rangle$ such that $t(b/F)$ is the heir of the q. Since $K\langle a\rangle \subset F$, $b \mathop{\smile\!\!\!\!\!\!\mid}_K a$. Thus $p \perp q$.

Corollary 7.14. Let $p, q \in S_1(K)$ be strongly regular. The following are equivalent:

i) $K_p \cong K_q$

ii) $p \geq_{RK} q$

iii) $p \sim_{RK} q$

iv) $p \not\perp q$.

Proof.

i) $\Rightarrow$ ii) $\Rightarrow$ iii) $\Rightarrow$ i) is clear from 7.11,7.12.

ii) $\Rightarrow$ iv). Is clear from 7.2.

iv) $\Rightarrow$ ii). Suppose $p \not\geq_{RK} q$. If $K_p \setminus K$ contains no elements satisfying $f_q(x) = 0$, then by 7.3 $p \perp q$. Suppose $a \in K_p \setminus K$ and $f_q(a) = 0$. By 7.10 $q \perp t(a/K)$. By 7.12 $t(a/K) \geq_{RK} p$, thus by 7.13 $p \perp q$, as desired.

Strongly regular types are important because they can be assigned dimensions. (The reader is referred to [B] chapter XII for details.)

Let $k \subset K$. We say that $A \subset K$ is *k-free* if and only if for all $a \in A$ $a \mathop{\smile\!\!\!\!\!\!\mid}_k A - \{a\}$.

If $p \in S_1(k)$, we say that $B \subset K$ is a *p-base* for K if it is a maximal k-free set of realizations of p. If p is strongly regular, then $\not\!\mathop{\smile\!\!\!\!\!\!\mid}$ is transitive on the realizations of p. Thus any two p-bases have the same cardinality. We call this cardinality the p-dimension of K/k. We denote this as $dim(p; K)$. If k_0, k_1 are finitely generated, $p_i \in S_1(k_i)$ is strongly regular, and $K \supset k_0 \cup k_1$, then $dim(p_0; K)$ differs from $dim(p_1; K)$ by at most a finite amount.

Two dimensions are clearly important invariants of a differentially closed field. Let $t_c \in S_1(\mathbf{Q})$ be the type of a new constant and let $t_q \in S_1(\mathbf{Q})$ be the type of a new transcendental. For any differentially closed field K, let $I_c(K) = dim(t_c; K)$ and $I_g(K) = dim(t_g; K)$. It is easy to see that for pair of cardinals κ, λ, there is a differentially closed field K with $I_c(K) = \kappa$ and $I_g(K) = \lambda$. Until the work of Hrushovski and Sokolović the only types known that were nonorthogonal to t_c and t_g were trivial types like those arising from Rosenlicht's examples. This lead Lascar to conjecture that perhaps any strongly type which is orthogonal to t_c and t_g is $\aleph_0$-categorical. Lascar's conjecture would have implied that the number of countable models is $\aleph_0$. Indeed a countable model would be determined up to isomorphism by $I_g(K)$ and $I_c(K)$. The work of Hrushovski and Sokolović shows that this is far from true. There are many locally modular strongly regular types which are not $\aleph_0$-categorical. These matters are discussed extensively in Pillay's article in this volume.

References

Shelah ([Shelah 1]) proved that in uncountable cardinals DCF has the maximal possible number of models.

The analysis of orthogonality and strongly regular types is from [Lascar 1].

§8. **Differential Galois Theory**

Let K/k be differential fields. We define $G(K/k)$ the *Differential Galois Group* of K over k, to be the group of differential automorphisms of K which fix k pointwise.

We begin by looking at some important examples.

Examples:

1) Adjoining an integral:

Let $a \in k$. Consider the equation $X' = a$. Let u be a generic solution of $X' = a$ over k and let $K = k\langle u \rangle$. Since $u' = a \in k$, $K = k(u)$. If $\sigma \in G(K/k)$, then $\sigma(u)' = a$, thus for some $c \in C_K$, $\sigma(u) = u + c$. If $c \in C_k$, then $u \mapsto u + c$ determined a differential automorphsim of K fixing k.

We will assume that C_k is algebraically closed. Then by theorem 4.5 K/k is Picard-Vessiot (the equation $X'' - \frac{a'}{a}X' = 0$ has linear independent solutions 1 and u). Indeed if $X' = a$ has no solution in k, then K/k is Picard-Vessiot (see [Kaplansky]). Since $C_K = C_k$, the above argument shows that $G(K/k)$ is isomorphic to the additive group of C_k.

2) Exponentials

Let $a \in k$. Let u be a generic solution of $X' = aX$ over k. Let $K = k\langle u \rangle = k(u)$. Suppose $C_K = C_k$ (for example, suppose C_k is algebraically closed), then K/k is Picard-Vessiot. If $\sigma \in G(K/k)$, then $\sigma(u) = cu$, for some $c \in C_k$. Moreover if $c \in C_k$, then $u \mapsto cu$ determines an automorphism of K. Thus $G(K/k)$ is isomorphic to the multiplicative group of C_k.

3) We next exhibit a Picard-Vessiot extension where the differential Galois group is $GL_n(C)$.

Let k_0 be any differential field and let $K = k_0\langle X_1, \ldots, X_n \rangle$. Let $C = C_{k_0} = C_K$. Suppose $A = (a_{i,j})$ is a non-singular $n \times n$ matrix over C. Then A determines an automorphism of K by $\sigma_A(X_i^{(m)}) = \sum a_{i,j} X_j^{(m)}$. Thus $GL_n(C)$ is a subgroup of $G(K/k_0)$. Let k be the fixed field of $GL_n(C)$. One sees that $G(K/k) = GL_n(C)$.

Let

$$L(Y) = \frac{W(Y, X_1, \ldots, X_n)}{W(X_1, \ldots, X_n)}.$$

We claim that $L(Y)$ is a linear differential equation over k. To see this note that if $A \in GL_n(C)$ and X is the matrix such that $W(X_1, \ldots, X_n) = |X|$, then

$$W(\sigma_A(X_1), \ldots, \sigma_A(X_n)) = |XA^T| = W(X_1, \ldots, X_n)|A^T|,$$

while

$$\begin{aligned} W(Y, \sigma_A(X_1), \ldots, \sigma_A(X_n)) &= W(Y, X_1, \ldots, X_n) \cdot \begin{vmatrix} 1 & 0 \\ 0 & A^T \end{vmatrix} \\ &= W(Y, X_1, \ldots, X_n)|A^T|. \end{aligned}$$

Thus $L(Y)$ is invariant under σ_A, so $L(Y) \in k\{Y\}$. The elements $X_1, \ldots, X_n$ are linearly independent solutions to $L(Y) = 0$, thus K/k is Picard-Vessiot.

In all of these examples the differential Galois group of the Picard-Vessiot extension is a linear algebraic group over the constant field. We next show that this is always the case.

For the following arguments we fix $\mathbf{K}$ a very saturated differentially closed field. $\mathbf{K}$ will serve as a universal domain (ie. monster model) for all of our work.

Let k be a differential field and let K/k be a Picard-Vessiot extension. Say $K = k\langle u_1, \ldots, u_n\rangle$ and $L(Y) = 0$ is the homogeneous linear equation determining the extension. Recall that since K/k is Picard-Vessiot, $C_K = C_k$. We denote the common constant field C.

Suppose $k \subseteq F$ and $\sigma : K \to F$ is an embedding fixing k. Then $\sigma(u_i)$ is a solution of $L(Y) = 0$ for each i. Thus there are constants $c_{i,j} \in C_F$ such that $\sigma(u_i) = \sum c_{i,j} u_j$. We call $(c_{i,j})$ the matrix associated with σ.

Theorem 8.1. There is Σ a system of equations in $C[X_{i,j}.1 \leq i, j \leq n]$ such that:

i) If $\sigma : K \to F$ is an embedding fixing k, then the coefficients of the matrix associated with σ satisfy Σ.

ii) If $F \supseteq K$ and $\overline{c} \in C_F$ satisfies Σ, then $u_i \mapsto \sum c_{i,j} u_j$ determines an embedding of K into F fixing k.

This immediately yields:

Corollary 8.2. If K/k is a Picard-Vessiot extension of order n, then $G(K/k)$ is isomorphic to an algebraic subgroup of $GL_n(C)$ (ie. $G(K/k)$ is a linear algebraic group over the constant field).

proof of 8.1.

Let p be the type of $\overline{u}$ over k. Consider the map

$$\phi : k\langle Y_1, \ldots, Y_n\rangle \to K[Z_{i,j} : 1 \leq i, j \leq n]$$

determined by $Y_i \mapsto \sum_{j=1}^{n} Z_{i,j} u_i$ and let Δ be the image of I_p under ϕ.

In other words, Δ is the ideal of polynomials in $K[\overline{Z}]$ such that if $\overline{d}$ is in the variety given by Δ and σ is the map $u_i \mapsto \sum d_{i,j} u_j$. Then $\sigma(u_1), \ldots, \sigma(u_n)$ is in the variety given by I_p.

Let W be a vector space basis for K over C. For each $f \in \Delta$, write

$$f = \sum_{w \in W} f_w(\overline{Z}) w$$

where $f_w \in C[\overline{Z}]$.

Let Σ be the ideal generated by the $\{f_w : f \in \Delta, w \in W\}$.

Let L be the differential closure of K. Then C_L is the algebraic closure of C. Since the elements of W are independent over C, and K and C_L are linearly disjoint over C (as C is algebraically closed in K), $L \models$ " for all constants $\overline{c}$, if $p(\overline{c}) = 0$, then for all $w \in W$, $p_w(\overline{c}) = 0$". By model completeness this is also true in $\mathbf{K}$.

Suppose $\sigma : K \to \mathbf{K}$ is an embedding fixing k and determined by $u_i \mapsto \sum c_{i,j} u_j$, for some constants $\overline{c} \in \mathbf{K}$. Then for every polynomial $p(\overline{Z}) \in \Delta$, $p(\overline{c}) = 0$. By the above remarks, for all $w \in W$, $p_w(\overline{c}) = 0$. Thus all of the polynomials in Σ vanish at $\overline{c}$.

Let $F \supset K$ and let $A = (c_{i,j})$ be a nonsingular matrix in C_F such that $\overline{c}$ satisfies Σ. Let $\sigma : K \to F$ fix k and send $u_i \mapsto \sum c_{i,j} u_j$. We claim that σ is an embedding. We chose Σ to insure that σ is a homomorphism. It suffices to show that σ is one to one.

Suppose not. Then $td(K/k) > td(k\langle \sigma(\overline{u})\rangle/k)$ (if σ has a nontrivial kernel, then the Krull dimension of $k\langle \overline{u}\rangle$ is greater than the Krull dimension of $k\langle \sigma(\overline{u})\rangle$). Thus $td(k\langle \overline{u}, \sigma(\overline{u})\rangle/k\langle \overline{u}\rangle) < td(k\langle \overline{u}, \sigma(\overline{u})\rangle/k\langle \sigma(\overline{u})\rangle)$.

Also $td(k\langle \overline{u}, \sigma(\overline{u})\rangle)/k\langle \overline{u}\rangle = td(k\langle \overline{u}, \overline{c}\rangle/k\langle \overline{u}\rangle)$.

But if constants $\overline{c}$ are algebraically dependent over a differential field L they are dependent over the constants of L. Thus $td(k\langle \overline{u}, \overline{c}\rangle/k\langle \overline{u}\rangle) = td(C(\overline{c})/C)$.

But C is also the field of constants of $k\langle \sigma(\overline{u})\rangle$. Thus

$$td(k\langle \sigma(\overline{u}), \overline{c}\rangle/k\langle \sigma(\overline{u})\rangle) = td(C(\overline{c})/C),$$

a contradiction.

There is a beautiful Galois theory for Picard-Vessiot extensions. We state the main theorem here and refer the reader to the books by Kaplansky and Magid.

Definition. Let K/k be differential fields and let $G(K/k)$ be the differential Galois group. If $H \subseteq G(K/k)$, let $Fix(H) = \{x \in K : \forall \sigma \in H\ \sigma(x) = x\}$.

We say that K/k is *normal* if for any $x \in K \setminus k$ there is $\sigma \in G(K/k)$ such that $\sigma(x) \neq x$.

Theorem 8.3. Let k be a differential field with C_k algebraically closed. If K/k is Picard-Vessiot, then K/k is normal, $G(K/k)$ is a linear algebraic group over C_k and $L \mapsto G(K/L)$ gives a one to one correspondence between the intermediate differential subfields of K/k and the algebraic subgroups of $G(K/k)$. An algebraic subgroup H is normal if and only if $Fix(H)/k$ is a normal. In this case $G(Fix(H)/k)$ is $G(K/k)/H$. Moreover if k is algebraically closed, then $G(K/k)$ is connected

Much as ordinary Galois theory can be used to prove that the general quintic can not be solved by adjunction radicals, differential Galois theory can be used to prove the unsolvability of differential equations by simple means.

Let $f(X) \in k\langle X\rangle$. We say that K is a *Liouville extension* of k if there are extensions $k = K_0 \subseteq K_1 \subset \cdots \subseteq K_n = K$, where each K_{i+1} is obtained from K_i by adjoining an integral, adjoining the exponential of an integral or making an algebraic extension. We say that $f(X) = 0$ is *solvable by quadratures* if it is solvable in a Liouvile extension.

Theorem 8.4. Let k be a differential field of characteristic zero with C_k algebraically closed. Suppose that K/k is Liouville. If $K \supseteq L \supseteq k$ is Liouville, then the connected component of $G(L/k)$ is solvable.

For example this method can be used to show that $y' = y^2 - x$ is not solvable by quadratures over $\mathbf{C}(\mathbf{x})$

References

The algebraic Galois theory of Picard-Vessiot extensions is due to Kolchin ([Kolchin 4]). Kaplansky's *Differential Algebra* and Magid's *Lectures on Differential Galois Theory* provide extensive treatments of this subject. We refer the reader to these books for the proofs of theorems 8.3 and 8.4.

§9. **Strongly Normal Extensions**.

In this section we will examine Kolchin's strongly normal extensions. This class of extensions contains the Picard-Vessiot extensions and also has an interesting Galois theory. Again we work inside a very saturated universal domain $\mathbf{K}$.

Definition. L/K is *strongly normal* if and only if
i) $C_L = C_K$ is algebraically closed
ii) L/K is finitely generated
iii) if $\sigma : \mathbf{K} \to \mathbf{K}$ is an automorphism fixing K, then $\langle L, C_{\mathbf{K}} \rangle = \langle \sigma(L), C_{\mathbf{K}} \rangle$.

For example, if C_K is algebraically closed and L/K is Picard-Vessiot, we show that L/K is strongly normal. Suppose $L = K\langle \overline{a} \rangle$, where $\overline{a}$ is a fundamental system of solutions to a linear equation over K. For any K-automorphism σ, $\sigma(\overline{a}) \in \langle L, C_{\mathbf{K}} \rangle$, thus $\langle L, C_{\mathbf{K}} \rangle \supseteq \langle \sigma(L), C_{\mathbf{K}} \rangle$. Similarly, L is contained in $\langle \sigma(L), C_{\mathbf{K}} \rangle$. So equality holds.

We will show that for strongly normal extensions $G(L/K)$ is an algebraic group over C_K.

Lemma 9.1. Suppose L/K is strongly normal and $L = K\langle \overline{a} \rangle$. Then L is contained in the differential closure of K.

Proof. Suppose not. Let F be the differential closure of L. Note that $C_F = C_L = C_K$. Let p be the type of $\overline{a}$ over the differential closure of K and let q be a non-forking extension of p to F. Since F contains no new constants, p is orthogonal to the the type of a new constant. Thus q is orthogonal to the type of a new constant. Let $\overline{b}$ realize q and let F_1 be the differential closure of $F\langle \overline{b} \rangle$. Since q is orthogonal to the constants, $C_{F_1} = C_K$.

Since $\overline{a}$ and $\overline{b}$ realize the same type over K, there is an automorphism of $\mathbf{K}$ fixing K and sending $\overline{a}$ to $\overline{b}$. Thus since L is strongly normal, $\overline{b} \in \langle L, C_{\mathbf{K}} \rangle$. In particular, there is a K-definable function f such that

$$\mathbf{K} \models \exists \overline{c} \ (\bigwedge c_i' = 0 \wedge f(\overline{a}, \overline{c}) = \overline{b}).$$

By model completeness

$$F_1 \models \exists \overline{c} \ (\bigwedge c_i' = 0 \wedge f(\overline{a}, \overline{c}) = \overline{b}).$$

Thus $\overline{b} \in \langle L, C_{F_1} \rangle = L$. Thus $\overline{a}$ must be in the differential closure of K.

Suppose $L = K\langle \overline{a} \rangle$ and L/K is strongly normal. Since $\overline{a}$ is in the differential closure of K, there is a formula $\psi(\overline{v})$ over K, which isolates the $tp(\overline{a}/K)$.

Lemma 9.2. $\psi(\overline{v})$ isolates $tp(\overline{a}/\langle K, C_{\mathbf{K}} \rangle)$.

Suppose $\overline{b} \in K, \overline{c} \in C_{\mathbf{K}}$ and $\phi(\overline{v}, \overline{b}, \overline{c})$ and $\neg\phi(\overline{v}, \overline{b}, \overline{c})$ split $\psi(\overline{v})$. Then

$$\mathbf{K} \models \exists \overline{c} \ (\bigwedge c_i' = 0 \wedge \exists \overline{v} \exists \overline{w} \ (\psi(\overline{v}) \wedge \psi(\overline{w}) \wedge \phi(\overline{v}, \overline{b}, \overline{c}) \wedge \ \neg\phi(\overline{w}, \overline{b}, \overline{c}))).$$

By model completeness this is also true in the differential closure of K. But the differential closure of K has the same constants as K. Thus ψ is not an atom over K, a contradiction.

Before proving the general result we examine an important special case.

Example. Weierstrass Equations:

Fix $g_2, g_3 \in C_K$ with $27g_3^2 - g_2^3 \neq 0$. For $a \in K$ let $G_a(Y)$ be the differential polynomial $(Y')^2 - a^2(4Y^3 - g_2Y - g_3)$.

We say that $\alpha \in \mathbf{K}$ is *Weierstrassian* over K if it is non-constant and satisfies the equation $G_a(\alpha) = 0$ for some $a \in K$.

If K is the field of complex meromorphic functions , then the Weierstrass p-function $\wp$ is Weierstrassian over K.

We assume that C_K is algebraically closed. Consider the projective curve W given by the equation $ZY^2 = 4X^3 - g_2XZ^2 - g_3Z^3$. Since $27g_3^2 - g_2^3 \neq 0$, W is non-singular and hence an elliptic curve defined over C_K. Hence there is an abelian group law on W. We write the group multiplicatively. W has a unique point at infinity $(0, 1, 0)$ and this point is the zero of the group. In general $(a, b, 1)^{-1} = (a, -b, 1)$. [Note: Henceforth when we consider affine points of W we will use the standard affine coordinates.]

If $G_a(\alpha) = 0$, then $(\alpha, \frac{\alpha'}{a}) \in W$.

We use the following lemma from [Kolchin 2].

Lemma 9.3. Suppose $G_a(\alpha) = 0$ and $G_b(\beta) = 0$, where α and β are non-constant. Suppose that $(\alpha, \frac{\alpha'}{a})(\beta, \frac{\beta'}{b}) = (\gamma, \delta)$. Then $\gamma' = (a + b)\delta$. In particular either γ is constant or γ is Weierstrassian over K with $(\gamma')^2 = (a + b)^2(4\delta^3 - g_2\delta - g_3)$.

Suppose α is Weierstrassian with $G_a(\alpha) = 0$. Let $L = K\langle\alpha\rangle$ and suppose that $C_L = C_K$. Let $\sigma : L \to \mathbf{K}$ be a K-embedding.

Consider $P_\sigma = (\sigma(\alpha), \frac{\sigma(\alpha)'}{a})(\alpha, \frac{\alpha'}{a})^{-1} = (\sigma(\alpha), \frac{\sigma(\alpha)'}{a})(\alpha, -\frac{\alpha'}{a})$. $P_\sigma \in W$ and $P_\sigma = (0, 1, 0)$ if and only if σ is the identity.

Suppose σ is nontrivial. Let $P_\sigma = (c_1, c_2)$. By the previous lemma $c_1' = (a - a)c_2$. Thus c_1 is constant. It follows that c_2 is also constant. Thus for every embedding σ there is $P_\sigma \in W(\mathbf{C_K})$ such that $(\sigma(\alpha), \frac{\sigma(\alpha)'}{a}) = P_\sigma(\alpha, \frac{\alpha'}{a})$.

Thus $\sigma(\alpha) \in \langle L, C_{\mathbf{K}}\rangle$ so L/K is strongly normal. Suppose σ and $\tau \in G(L/K)$. Then P_σ and P_τ are in L. But the differential closure of L has the same constants as K, so these points are in $W(C_K)$. Then

$$(\sigma\tau(\alpha), \frac{\sigma\tau(\alpha)'}{a}) = P_\sigma(\tau(\alpha), \frac{\tau(\alpha)'}{a}) = P_\sigma P_\tau(\alpha, \frac{\alpha'}{a}).$$

Thus $P_{\sigma\tau} = P_\sigma P_\tau$. Thus $\sigma \mapsto P_\sigma$ is an embedding from $G(L/K)$ into $W(C_K)$.

Let ψ isolate the type of α over K. The set $\{(c_1, c_2) \in W(C_K) : \psi$ holds of the first coordinate of $(c_1, c_2)(\alpha, \frac{\alpha'}{a}))\}$ is definable. Thus $G(L/K)$ is isomorphic to a definable subgroup of $W(C_K)$. As $W(C_K)$ is an irreducible variety (and hence a connected group), the only proper definable subgroups of $W(C_K)$ are finite.

Suppose $G(L/K)$ is finite. Suppose β is in F the differential closure of L and $\psi(\beta)$ holds. Thus there is an automorphism σ of $\mathbf{K}$ such sending α to β. This automorphism corresponds to an action of the group $W(C_K)$. But then β is already in L. Thus in F there are only finitely many solutions of ψ, so α is algebraic over K.

Thus we have shown that if $C_K = C_{K\langle\alpha\rangle}$ and α is Weierstrassian over K it is either algebraic over K or $G(K\langle\alpha\rangle, K)$ is the group law of an elliptic curve over C_K.

We will next show that the Galois group of a strongly normal extension is always an algebraic group over the constants.

Let L/K be strongly normal and suppose $L = K\langle\overline{a}\rangle$. Let $\psi(\overline{v})$ isolate $t(\overline{a}/K)$.

If $\psi(\overline{b})$, then there is $\sigma \in G(\mathbf{K}/K)$ such that $\sigma(\overline{a}) = \overline{b}$. Since L/K is strongly normal, $\overline{b} \in \langle L, C_{\mathbf{K}}\rangle$. In particular there is a K-definable function $g_{\overline{b}}$ and $\overline{c} \in C_{\mathbf{K}}$ such that $g_{\overline{b}}(\overline{a}, \overline{c}) = \overline{b}$. By compactness and the usual coding tricks we can find a single K-definable function g such that for all $\overline{b} \in \psi^{\mathbf{K}}$ there is $\overline{c} \in C_{\mathbf{K}}$ such that $\overline{b} = g(\overline{a}, \overline{c})$.

Let F be the differential closure of L (and K). If $\overline{b} \in F$, then any automorphism of L sending $\overline{a}$ to $\overline{b}$ lifts to an automorphism of $\mathbf{K}$. Thus there is $\overline{c} \in C_{\mathbf{K}}$ such that $\overline{b} = g(\overline{a}, \overline{c})$. By model completeness, there is $\overline{c} \in C_F$ such that $\overline{b} = g(\overline{a}, \overline{c})$. But $C_F = C_K$ so there are constants in L such that $\overline{b} = g(\overline{a}, \overline{c})$.

It is easy to see that $\sigma \in G(L/K)$ is determined by its action on $\overline{a}$. Clearly $\psi(\sigma(\overline{a}))$ and if $\psi(\overline{b})$, then there is $\sigma \in G(L/K)$ with $\sigma(\overline{a}) = \overline{b}$.

Consider the relation $R(\overline{b}, \overline{d}, \overline{e})$, which asserts that if $\sigma(\overline{a}) = \overline{b}$ and $\tau(\overline{a}) = \overline{d}$, then $\sigma \circ \tau(\overline{a}) = \overline{e}$. Then $R(\overline{b}, \overline{d}, \overline{e})$ holds if and only if $\sigma(\overline{d}) = \overline{e}$. But there are constants $\overline{c} \in C_K$ such that $\overline{d} = g(\overline{a}, \overline{c})$. But then $\sigma(\overline{d}) = g(\overline{b}, \overline{c})$. So

$$R(\overline{b}, \overline{d}, \overline{e}) \Leftrightarrow \psi(b) \wedge \psi(d) \wedge \psi(e) \wedge \exists \overline{c} \bigwedge c_i' = 0 \wedge \overline{d} = g(\overline{a}, \overline{c}) \wedge \overline{e} = g(\overline{b}, \overline{c}).$$

Let X be the set ψ^L and define $\cdot$ on X by $\overline{b} \cdot \overline{d} = \overline{e}$ if and only if $R(\overline{b}, \overline{d}, \overline{e})$. We have shown that $(X, \cdot)$ is isomorphic to $G(L/K)$.

We can do even better. Let $Y = \{\overline{c} \in C_F : \psi(g(\overline{a}, \overline{c}))\}$. We define an equivalence relation E on Y by $\overline{c}_0 E \overline{c}_1$ if and only if $g(\overline{a}, \overline{c}_0) = g(\overline{a}, \overline{c}_1)$. We also define a ternary relation R^* on Y by $R^*(\overline{c}_0, \overline{c}_1, \overline{c}_2)$ if and only if $R(g(\overline{a}, \overline{c}_0), g(\overline{a}, \overline{c}_1), g(\overline{a}, \overline{c}_2))$. Clearly R^* is E invariant.

Since C_F is a pure algebraically closed field, Y, E and R^* are definable in the pure language of fields. By elimination of imaginaries we can find a field definable function $f : Y \to C_F^n$ such that $\overline{c} E \overline{c}_0$ if and only if $f(\overline{c}) = f(\overline{c}_0)$. Let G be the image of Y under f. Define $\cdot$ on G by $x_0 \cdot x_1 = x_2$ if and only if there are $\overline{c}_0$, $\overline{c}_1$ and $\overline{c}_2 \in Y$ such that $f(\overline{c}_i) = x_i$ and $R^*(\overline{c}_0, \overline{c}_1, \overline{c}_2)$. Then $(G, \cdot)$ is isomorphic to $G(L/K)$ and $(G, \cdot)$ is definable in the pure field structure of C_F. (Also $C_F = C_L = C_K$.)

In other words $G(L/K)$ is isomorphic to a group definable in the pure algebraically closed field C_K. The following theorem of van den Dries says that any such group is definably isomorphic to an algebraic group.

Theorem 9.4. Let K be an algebraically closed field and let $(G, \cdot)$ be a group definable in K. Then G is definably isomorphic to an algebraic group over K.

Thus we have proved the following theorem of Kolchin.

Theorem 9.5. Suppose L/K is strongly normal and K is algebraically closed. Then $G(L/K)$ is isomorphic to an algebraic group defined over C_K.

Once we know that $G(L/K)$ is an algebraic group over C_K. We can develop a Galois correspondence between algebraic subgroups and intermediate fields. Much of the Galois theory of theorem 8.3 generalizes

For strongly normal extensions L/K, we will also study the group $G(\langle L, C_{\mathbf{K}}\rangle/\langle K, C_{\mathbf{K}}\rangle)$. We will call this group the *full differential Galois group* and denote it $Gal(L/K)$. The above arguments show that if L/K is strongly normal then $Gal(L/K)$ is an algebraic group over $C_{\mathbf{K}}$. In particular, there is an algebraic group G defined over C_K such that $G(L/K) \cong G(C_K)$ and $Gal(L/K) \cong G(C_{\mathbf{K}})$, (where for $F \supseteq C_K$, $G(F)$ denotes the F-rational points of G).

We will identify $Gal(L/K)$ with $G(C_{\mathbf{K}})$. The above arguments show that there is a map $\gamma : Gal(L/K) \to G(C_{\mathbf{K}})$ such that $\sigma(\overline{a}) \in K\langle \overline{a}, \gamma(\sigma)\rangle$ and $\gamma(\sigma) \in K\langle \overline{a}, \sigma(\overline{a})\rangle$ for all $\sigma \in Gal(L/K)$,.

We next make a careful choice of the generator of L/K which will prove useful later.

Definition. Let L/K be strongly normal and let F be the differential closure of K. We say that $\alpha \in L$ is *G-primitive* if and only if $\alpha \in G(L)$, $L = K\langle\alpha\rangle$ and for all $\sigma \in G(F/K)$ $\alpha{-}1\sigma(\alpha) \in G(C_K)$.

Lemma 9.6. Let K be algebraically closed. Every strongly normal extension L/K is of the form $L = K\langle\alpha\rangle$, where α is G-primitive.

Proof.

Since L is contained in the differential closure of K and L/K is finitely generated, L/K has finite transcendence degree. Thus we can find $\overline{a} \in L$ such that $L = K(\overline{a})$. For any $\sigma \in Gal(L/K)$, $\sigma(\overline{a}) \in K\langle \overline{a}, \gamma(\sigma)\rangle = K(\overline{a}, \gamma(\sigma))$ and $\gamma(\sigma) \in K\langle \overline{a}, \sigma(\overline{a})\rangle = K(\overline{a}, \sigma(\overline{a}))$.

Let $\overline{b}, \overline{c}$ realize $t(\overline{a}/K)$ such that $\overline{b}, \overline{c}$ are independent over L. Let $\tau(\overline{a}) = \overline{b}$. By the above remarks there is a rational function F over K such that $F(\overline{a}, \overline{b}) = \gamma(\tau)$. This F will work for independent realizations of the $t(\overline{a}/K)$. In particular $F(\overline{c}, \overline{b}) \cdot F(\overline{a}, \overline{c}) = F(\overline{a}, \overline{b})$. Let V be the K-variety such that $\overline{a}$ is the generic point of V. Then $\overline{b}$ is also a generic point of V over the field $L(\overline{c})$. Thus the equation $F(\overline{c}, \overline{x}) \cdot F(\overline{a}, \overline{c}) = F(\overline{a}, \overline{x})$, must hold on a Zariski open subset of V. In particular we can find $\overline{d} \in K$ such that $F(\overline{c}, \overline{d}) \cdot F(\overline{a}, \overline{c}) = F(\overline{a}, \overline{d})$ and $F(\overline{a}, \overline{d}) \in G(L)$ (Here we use the fact that if K is algebraically closed, $L \supset K$ and V is a variety defined over K, then the K-rational point of V are Zariski dense in the L-rational points). We let $\alpha = F(\overline{a}, \overline{d})$.

Let $\sigma \in Gal(L/K)$. We may as well assume that the $\overline{c}$ chosen above was independent of $\overline{\sigma}(\overline{a})$ over K. Thus $t(\overline{a}, \overline{c}/K) = t(\overline{c}, \sigma(\overline{a})/K)$. Hence $F(\sigma(\overline{a}), \overline{d}) \cdot F(\overline{c}, \sigma(\overline{a})) = F(\overline{c}, \overline{d})$. So $F(\sigma(\overline{a}), \overline{d}) \cdot F(\overline{c}, \sigma(\overline{a})) \cdot F(\overline{a}, \overline{c}) = \alpha$. But $F(\overline{c}, \sigma(\overline{a})) \cdot F(\overline{a}, \overline{c}) = \gamma(\sigma)$ and $F(\sigma(\overline{a}), \overline{d}) = \sigma(\alpha)$. Thus $\sigma(\alpha) = \alpha \cdot \gamma(\sigma)^{-1}$, as desired.

Finally we note that $L = K\langle\alpha\rangle$. If $\overline{a} \notin K\langle\alpha\rangle$, there is $\tau \in Aut(\mathbf{K}/K)$ such that $\tau(\alpha) = \alpha$ but $\tau(\overline{a}) \neq \overline{a}$. Thus $\sigma = \tau|L \in Gal(L/K)$ and $\sigma \neq 1$. But since $\sigma(\alpha) = \alpha$,

$\alpha = \alpha \cdot \gamma(\sigma)^{-1}$, so $\gamma(\sigma) = 1$ and σ is the identity.

The converse to 9.5 is also true.

Lemma 9.7. Suppose K is a differential field with C_K algebraically closed. Let G be an algebraic group defined over C_K. Let F be the differential closure of K. Suppose there is $\alpha \in G(F)$ such that for all $\sigma \in G(F/K)$ there is $g_\sigma \in G(C_K)$ such that $\sigma(\alpha) = \alpha \cdot g_\sigma$. Let $L = K\langle \alpha^{-1} \rangle$. Then L/K is strongly normal.

Proof.

Let $\sigma \in G(F/K)$, then $\sigma(\alpha^{-1}) = g_{\sigma^{-1}} \cdot \alpha^{-1}$. Let ψ isolate $t(\alpha^{-1}/K)$. Then

$$F \models \forall \gamma \ (\psi(\gamma) \to \exists g \in G(C) \ \gamma = g \cdot \alpha^{-1}).$$

This sentence is still true in $\mathbf{K}$. Thus for any automorphism σ, $\langle L, C_{\mathbf{K}} \rangle = \langle \sigma(L), C_{\mathbf{K}} \rangle$. So L/K is strongly normal.

Let $\Gamma(\mathbf{K})$ be the coset space $G(\mathbf{K})/G(C_{\mathbf{K}})$. By elimination of imaginaries in $\mathbf{K}$, we may assume that $\Gamma(\mathbf{K})$ is a quantifier free C_K-definable subset of $\mathbf{K}^m$. For any field $L \supseteq C_K$ let $\Gamma(L)$ denote the L-rational points of $\Gamma(\mathbf{K})$. Let $\rho : G(\mathbf{K}) \to \Gamma(\mathbf{K})$ be the quotient map. If F is the differential closure of K, then $\Gamma(F) = G(F)/G(C_K)$.

Lemma 9.8. Let $\alpha \in G(F)$. Then α is G-primitive if and only if $\rho(\alpha) \in \Gamma(K)$.

Proof.

Clearly $\rho(\alpha) \in \Gamma(K)$ if and only if $\rho(\alpha)$ is fixed by all elements of $G(\mathbf{K}/K)$ if and only if $\alpha^{-1} \cdot \sigma(\alpha) \in G(C_K)$ for all $\sigma \in G(\mathbf{K}/K)$. By the last lemma this is if and only if α is G-primitive.

Our next goal is to show that if G is a connected n-dimensional group, then $\Gamma(K)$ is essentially K^n. This will require some background work.

Let F/K be fields and let $D(F/K)$ be the space of derivations of F which annihilate K. Let $x_1, \ldots, x_n$ be a transcendence base for F/K. Then $\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}$ is a basis for $D(F/K)$ as an F-vector space.

First note that if $a_1, \ldots, a_n \in F$ and $D = \sum a_i \frac{\partial}{\partial x_i}$, and $D = 0$, then for each i, $D(x_i) = a_i = 0$. Thus $\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_i}$ are linearly independent.

Next we consider the case $F = K(x_1, \ldots, x_n)$. If $D \in D(F/K)$ then for $p(x_1, \ldots, x_n)$, $D(p(\overline{x})) = \sum D(x_i) \frac{\partial p}{\partial x_i}$. Thus $D = \sum D(x_i) \frac{\partial}{\partial x_i}$.

In general if y is algebraic over $K(\overline{x})$ with minimal polynomial $p(\overline{x}, y)$, then

$$0 = D(p(\overline{x}, y)) = \sum D(x_i) \frac{\partial p}{\partial x_i} + D(y) \frac{\partial p}{\partial y}.$$

So

$$D(y) = \frac{-\sum D(x_i) \frac{\partial p}{\partial x_i}}{\frac{\partial p}{\partial y}}.$$

Thus there is a unique way to extend a derivation on $K(\overline{x})$ to F. Thus $D(F/K)$ is an n-dimensional F vector space.

Let $V \subseteq K^m$ be an n-dimensional variety over K. Let $K(V)$ denote the field of rational functions on V, $K(V) = K[\overline{X}]/I(V)$. For $p \in V$, let O_p denote the local ring at p, ie. O_p is the ring of rational functions defined at p. We choose affine coordinates at p so that $x_1, \ldots, x_m \in O_p$.

We say that $\delta : O_p \to K$, is a local derivation at p, if δ is an additive homomorphism and $\delta(f_1 f_2) = f_1(p)\delta(f_2) + f_2(p)\delta(f_1)$. For example if $D \in D(K(V)/K)$ and $D : O_p \to O_p$ we define a local derivation D_p by $D_p(f) = D(f)(p)$. We let $\mathcal{T}_p(V)$ equal the set of all local derivations at p.

Let $f_1, \ldots, f_n$ be generators for I(V). If δ is a local derivation at p, then $0 = D(f_i) = \sum \frac{\partial f_i}{\partial x_i}(p)\delta(x_i)$.

Thus $\delta(x_1), \ldots, \delta(x_m)$ are a solution to the system of equations

$$(y_1, \ldots, y_m) \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(p) & \ldots & \frac{\partial f_1}{\partial x_m}(p) \\ \vdots & & \vdots \\ \frac{\partial f_N}{\partial x_1}(p) & \ldots & \frac{\partial f_N}{\partial x_m}(p) \end{pmatrix} = 0.$$

Thus $\mathcal{T}_p(V)$ can be viewed as the tangent space at p. In particular if p is a simple point on V, then $\mathcal{T}_p(V)$ is an n-dimensional vector space over K.

Clearly each $\frac{\partial}{\partial x_i} : O_p \to O_p$. Let $x_1, \ldots, x_n$ is a transcendence base for $K(V)/K$, then, by the above argument, the $\frac{\partial}{\partial x_1}_p, \ldots, \frac{\partial}{\partial x_n}_p$ are linearly independent over K, and hence a basis for $\mathcal{T}_p(V)$.

We next examine the case where G is a connected n-dimensional algebraic group.

For $a \in G$ we let $T_a : G \to G$ be the map $x \mapsto ax$. For $a, p \in G$, T_a induces $T_a^* : O_{ap} \to O_p$, by $T_a^* f = f \circ T_{ap}^*$. If D is a derivation of $K(G)/K$, then let $T_a D_p$ be the local derivation at ap given by $T_a D_p(f) = D_p(T_a^* f)$. We say that D is *invariant* (actually left-invariant) if for all $a, p \in G$, $T_a D_p = D_{ap}$. We let $\mathcal{L}(G)$ be the K-vector space of invariant derivations. We call $\mathcal{L}(G)$ the Lie-algebra of G.

Let 1 be the identity of G. We claim that $\mathcal{L}(G)$ is isomorphic to $\mathcal{T}_1(G)$ via the map $D \mapsto D_1$. We need only show that this map is surjective.

Suppose $\delta \in \mathcal{T}_1(G)$. We define D as follows. For $f \in K(G)$ we define f' by $f'(x) = \delta(T_x^* f)$. Let $D(f) = f'$. We claim that D is a left invariant derivation.

If $f, g \in K(G)$,

$$\begin{aligned} D(f+g)(x) &= \delta(T_x^*(f+g)) \\ &= \delta(T_x^* f + T_x^* g) \\ &= f'(x) + g'(x). \end{aligned}$$

$$\begin{aligned} D(fg)(x) &= \delta(T_x^*(fg)) \\ &= \delta(T_x^* f T_x^* g) \\ &= \delta(T_x^* f) T_x^* g + \delta(T_x^* g) T_x^* f \\ &= f'(x)g(x) + g'(x)f(x) \end{aligned}$$

So D is a derivation.

Finally,

$$\begin{aligned}(T_a D_x)f &= D_x(T_a^* f)\\ &= (D(T_a^* f))(x)\\ &= \delta(T_x^* T_a^* f)\\ &= \delta(T_{ax}^* f)\\ &= D_{ax}(f)\end{aligned}$$

since $T_x^* T_a^* = T_{ax}^*$. So D is left invariant.

Thus $\mathcal{L}(G)$ is isomorphic to $\mathcal{T}_1(G)$, the tangent space of G at 1.

Let F/K be of transcendence degree n. Say $x_1, \ldots, x_n$ is a transcendence base. We let $\Omega_{F/K}$ be the F-vector space of differentials on F over K as introduced in §6. Then $\Omega_{F/K}$ is an n-dimensional K vector space and $dx_1, \ldots, dx_n$ is a basis. In fact, $\Omega_{F/K}$ is the dual space of $D(F/K)$, ie. $\Omega_{F/K}$ is the space of F-linear maps from $D(F/K) \to F$. Each dx can be thought of as the map $dx(D) = D(x)$. If $\Phi : D(F/K) \to F$, let $\mathbf{K}_i = \Phi(\frac{\partial}{\partial x_i})$. Let $\omega = \sum \mathbf{K}_i dx_i$, then ω is induced by the map Φ.

If V is a variety and $p \in V$ we consider the space of *local differentials* at p. This is the dual space of the tangent space $\mathcal{T}_p(V)$. Let ω be a differential of $K(V)/K$, say $\omega = \sum g_i df_i$. We say that ω is *finite* at $p \in V$ if all of the g_i, f_i are defined at p. In this case ω has a *local component* ω_p defined by $\omega_p(\delta) = \sum g_i(p)\delta(f_i)$.

If G is a connected algebraic group, we say that ω is an *invariant differential* if and only if it is in the dual space of $\mathcal{L}(G)$. The space of invariant differentials is isomorphic to the space of local differentials at 1. Moreover if $D^1, \ldots, D^n$ are a basis for $\mathcal{L}(G)$, then $\omega^1, \ldots, \omega^n$ is a basis for the dual space where

$$\omega^i(D^j) = \begin{cases} 1 & \text{if } i = j; \\ 0 & \quad i \neq j. \end{cases}.$$

Suppose $k \subseteq K$ and V is defined over k. We may choose the transcendence base $x_1, \ldots, x_n$ such that $x_i \in k(V)$. In this way we may assume that all of our bases are defined over k. If $\delta \in D(K/k)$ and $p \in V$, then δ determines an element δ_p of the tangent space of V at p by $\delta_p(f) = \delta(f(p))$. If ω is a differential on V defined over k and well defined at p, then $\omega_p(\delta_p)$ is defined and in K. Then map $\delta \mapsto \omega_p(\delta_p)$ is a differential of K/k which we will call $\omega(p)$ the *induced differential* of ω at p. More specifically, if $\omega = \sum g_i f_i$ where g_i and $f_i \in O_p \cap k(V)$, then $\omega(p)(\delta) = \sum g_i(p)\delta(f_i(p))$.

If G is a connected algebraic group and $\beta \in G(K)$ let $\tau(\beta) : G \to G$ by $\tau(\beta)(x) = \beta x \beta^{-1}$. In the manner we discussed above $\tau(\beta)$ induces automorphisms $\tau(\beta)^* : K(G) \to K(G)$ and $\tau(\beta) : \mathcal{L}(G) \to \mathcal{L}(G)$. In general a map $\phi : \mathcal{L}(G_0) \to \mathcal{L}(G_1)$ induces ϕ^* mapping the invariant differentials on G_1 to the invariant differentials on G_0. Thus we have $\tau(\beta)^*$ an automorphism of the invariant differentials on G.

The next result shows the compatibility of the group operations with forming induced differentials from invariant differentials. We postpone the proof to Appendix B.

Theorem 9.9. Let $\alpha, \beta \in G(K)$ and let ω be an invariant differential on G. Then $\omega(\alpha \cdot \beta) = (\tau(\beta)^*\omega)(\alpha) + \omega(\beta)$. In particular if G is abelian, then $\omega(\alpha \cdot \beta) = \omega(\alpha) + \omega(\beta)$.

We now return to the following setting. K is an algebraically closed differential field and G is a connected algebraic group defined over C_K. We let D be the derivation on K. C_K plays the role of k in the above discussion.

Lemma 9.10. Let $\alpha \in G(K)$. Then $\alpha \in G(C_K)$ if and only if for every invariant differential ω on G, $\omega(\alpha)(D) = 0$.

Proof.

First, if $\alpha \in G(C_K)$, then for any $f \in C_K(G) \cap O_\alpha$, $D(f(\alpha)) = 0$. Since, the space of invariant differentials has a basis of differentials defined over C_K, this implies that every invariant differential vanishes at D.

Conversely, if $\alpha \notin G(C_K)$, then there is a local coordinate x_i such that $x_i(\alpha) \notin C_K$. The local differential dx_i on G translates to a local differential at 1 and this extends to an invariant differential ω on G. But then $\omega(\alpha)(D) = D(x_i(\alpha)) \neq 0$.

Corollary 9.11. Let $\alpha, \beta \in G(K)$. Then $\alpha \cdot \beta^{-1} \in G(C_K)$ if and only if for every invariant differential ω on G, $\omega(\alpha)(D) = \omega(\beta)(D)$.

Proof. Let $\gamma = \alpha \cdot \beta^{-1}$. By 9.8,for all ω

$$\begin{aligned}\omega(\alpha)(D) &= \omega(\gamma\beta)(D)\\ &= \tau(\beta)^*\omega(\gamma)(D) + \omega(\beta)(D).\end{aligned}$$

By 9.9, $\tau(\beta)^*\omega(\gamma)(D) = 0$ for all ω if and only if $\gamma \in G(C_K)$ (since $\tau(\beta)^*$ is an automorphism of the invariant differentials).

If G is an algebraic group defined over C_K. Let $\omega_1, \ldots, \omega_n$ be a basis for the invariant differentials on G, such that each ω_i is defined over C_K. For $\alpha \in G$ let $h_i(\alpha) = \omega_i(\alpha)(D)$. If $\omega = \sum g_i df_i$ where the $g_i, f_i \in C_K(G)$, then $\omega(\alpha)(D) = \sum g_i(\alpha)D(f_i(\alpha))$. Thus f_i is definable in the differential field K. Let $F : G(K) \to K^n$ by $F(\alpha) = (h_1(\alpha) \ldots h_n(\alpha))$. By 9.10, $F(\alpha) = F(\beta)$ if and only if $\alpha\beta^{-1} \in G(C_K)$. Thus the image of F can be identified with the quotient $G(K)/G(C_K) = \Gamma(K)$.

In particular,

Corollary 9.12 $\Gamma(\mathbf{K}) = G(\mathbf{K})/G(C_{\mathbf{K}})$ can be embedded into $\mathbf{K}^n$.

<u>References</u>

All of the results in this section are due to Kolchin. They can be found in [Kolchin 2,5,6]. The proof of Theorem 9.5 that we give here is due to Poizat [Poizat 3]. Poizat's book *Groupes Stables* contains Hrushovski's elegant model theoretic proof of van den Dries theorem (9.4). The treatment we give here on G-primitives is taken from [Pillay-Sokolović].

The basic results on derivations and differentials on algebraic groups can be found in [Rosenlicht 3]). The commutative case of Theorem 9.8 was proved by Rosenlicht while the general case is from [Kolchin 6].

§10.**Superstable differential fields**:

We would like to prove the differential analogs of the following theorems about algebraically closed fields. We know that the theory of algebraically closed fields is quantifier eliminable and ω-stable. These results of Pillay and Sokolović give partial converses.

Theorem 10.1. i) (Macintyre-McKenna-van den Dries) If K is an infinite field and the theory of K admits quantifier elimination in the language of fields, then K is algebraically closed.

ii) (Cherlin-Shelah) If K is an infinite field (possible with extra structure) and the theory of K is superstable, then K is algebraically closed.

It would be natural to conjecture that any quantifier eliminable or superstable differential field is differentially closed. This question is open. We first note that the quantifier elimination question is subsumed by the superstability question.

Lemma 10.2. If T is a quantifier eliminable theory of differential fields (in the language of differential fields), then T is ω-stable.

Proof.

Let $K \models T$. By quantifier elimination any type over K is determined by the set of quantifier free formulas in the type. Thus an n-type is determined by the ideal of differential polynomials in $K\{X_1, \ldots, X_n\}$ that vanish at a realization. Thus the number of types is equal to the number of prime differential ideals over K. By the Ritt basis theorem, every prime differential ideal is finitely generated. Thus there are only $|K|$ types over K. Thus K is ω-stable.

In this section we will prove the following theorem from [Pillay-Sokolović].

Theorem 10.3. If K is a superstable differential field with a non-trivial derivation (we allow the possibility of extra structure), then K has no proper strongly normal extensions.

We begin by summarizing some of the Berline-Lascar [Berline-Lascar] theory of superstable groups which we will use in the proof.

Lemma 10.4. (Berline-Lascar) If K is a superstable field then for some ordinal α and some natural number m, $RU(K) = \omega^\alpha m$.

Definition. Suppose G be a superstable group and $A \subseteq G$ is ∞-definable. We say that A is α-indecomposable if A/H has only one class for any definable subgroup H with $RU(A/H) < \omega^\alpha$.

Theorem 10.5. (Berline-Lascar Indecomposability Theorem) If $RU(G) = \omega^\alpha n$ and $(A_i : i \in I)$ is a family of ∞-definable α-indecomposable sets each containing the identity of G, then the group H generated by the A_i is ∞-definable and H is of the form $A_{i_1}^{\pm 1} \ldots A_{i_n}^{\pm 1}$.

Finally we recall Lascar's U-rank inequality. Here $\oplus$ denotes the Cantor sum on the ordinals.

Theorem 10.6. (Lascar's Rank Inequality): $RU(a/Ab) + RU(b/A) \le RU(a, b/A) \le RU(a/Ab) \oplus RU(b/A)$.

Let K be a saturated superstable differential field with $RU(K) = \omega^\alpha m$. By Theorem 10.1 ii), K is an algebraically closed field. The Cherlin-Shelah analysis of superstable fields also shows that any superstable field has a unique type of maximal rank. We call this the *generic* of K.

Corollary 10.7. i) $RU(C_K) < \omega^\alpha$.
ii) $RU(x/x') < \omega^\alpha$.
iii) If $A \subseteq K$ and $a \in K$ is generic over A, then a' is generic over A.

Proof.
i) C_K is an algebraically closed field, so K is an infinite dimensional vector space over C_K. Thus for all n $RU(K) > RU(C_K^n) = RU(C_K)n$. Thus $RU(C_K) < \omega^\alpha$.

ii) Clear from i) since C_K is the kernel of the derivation.

iii) By the U-rank inequalities, $RU(x/A) \le RU(x, x'/A) \le RU(x/Ax') \oplus RU(x'/A)$. Since $RU(x/A) = \omega^\alpha m$, ii) implies that $RU(x'/A) = \omega^\alpha m$.

Lemma 10.8. Let $A \subset K$ and let $a \in K$ be generic over A. Then a is differentially transcendental over A.

Proof. Suppose not. Then we can find i and n such that $a^{(i)}$ is strongly algebraic over $A, a^{(i+1)}, \ldots, a^{(n)}$. Thus $a^{(i)}$ is algebraic over $Aa^{(i+1)}$. By 10.7 iii) $a^{(i)}$ is generic over A. Thus since a and $a^{(i)}$ realize the same type over A, a is algebraic over Aa'. But for any constant $c \in C_K$, $RU(a+c/A) \oplus RU(c/A) \ge RU(a+c, c/A) \ge RU(a/A)$. Since $RU(c/A) < \omega^\alpha$, $RU(a+c/A) = \omega^\alpha m$, so $a+c$ is generic over A. Thus $t(a+c, a'/A) = t(a, a'/A)$. Since C_K is infinite this contradicts the fact that a is algebraic over Aa'.

We can in fact prove something stronger.

Lemma 10.9. Let $A \subseteq K$ and let $a \in K$ be differentially algebraic over A, then $RU(a/A) < \omega^\alpha$.

Proof. We may without loss of generality assume that $A \models Th(K)$ and (by taking forking extensions) that $RU(a/A) = \omega^\alpha$. Let $p = t(a/A)$.

Let $\Phi_0 = \{x \in K : x \text{ realizes } p\}$. Fix $b \in \Phi_0$ and let $\Phi = \{x - b : x \in \Phi_0\}$. Since p is stationary, Φ is α-indecomposable with respect to additive subgroups of K. For each $x \in K$ let $\Phi_x = x\Phi$. The Φ_x are α-indecomposable and contain 0. By 10.5 the additive subgroup H generated by the Φ_x is ∞-definable and there are $x_1, \ldots, x_n \in K$ such that $H = \Phi_{x_1} + \Phi_{x_2} \ldots + \Phi_{x_n}$. Since $xH \subset H$ for all $x \in K$, H is an ideal. Thus $H = K$.

Let $y \in K$ be generic over $A\langle b, x_1, \ldots, x_n\rangle$. There are $y_1, \ldots, y_n$ realizing p such that

$y = \sum x_i(y_i - b)$. But then, since the y_i are differentially algebraic over A, y is differentially algebraic over $A\langle b, \overline{x}\rangle$ contradicting the genericity of y.

We will prove that K has no proper strongly normal extensions. Let Λ be a very saturated differentially closed field containing K. It suffices to show that for G an algebraic group defined over C_K if $\Gamma(\Lambda)$ is the quotient space $G(\Lambda)/G(C_\Lambda)$ and $\rho : G(\Lambda) \to \Gamma(\Lambda)$ is the quotient map, then ρ maps $G(K)$ onto $\Gamma(K)$.

Lemma 10.10. Let G be a connected n-dimensional algebraic group defined over C_K. Then $RU(G(K)) = \omega^\alpha mn$ and every orbit of $\Gamma(K)$ under the action of $G(K)$ has U-rank $\omega^\alpha mn$.

Proof.

The first remark is clear. More generally if V is an n-dimensional algebraic variety over a superstable field F, then $RU(V) = RU(F)n$.

Let $x \in \Gamma(K)$. Let $Stab(x) = \{g \in G(K) : gx = x\}$. Let F be the differential closure of K. There is $h \in G(F)$ such that $h/G(C_F) = x$. Since $C_F = C_K$, $g \in Stab(x)$ if and only if $h^{-1}gh \in G(C_K)$ if and only if $g \in hG(C_K)h^{-1}$. Since $RU(C_K) < \omega^\alpha$, $RU(Stab(x)) < \omega^\alpha$.

The orbit of $x \in \Gamma(K)$ under $G(K)$ is isomorphic to $G(K)/Stab(x)$. Using the U-rank inequality we see that each orbit has U-rank $\omega^\alpha mn$.

Since $RU(G(K)) = \omega^\alpha mn$ and $RU(G(C_K)) < \omega^\alpha$. By the U-rank inequality we must have $RU(\Gamma(K)) = \omega^\alpha mn$. Thus there are only finitely many orbits of $\Gamma(K)$ under $G(K)$. We will show that there is exactly one. In this case $\rho : G(K) \to \Gamma(K)$ is onto and we are done.

To prove this it suffices to show that $\Gamma(K)$ has a unique generic type. By 9.12, $\Gamma(\Lambda) \subset \Lambda^n$. Thus $\Gamma(K) \subset K^n$. But $\Gamma(K)$ has rank $\omega^\alpha mn = RU(K^n)$. Since K^n has a unique generic type, $\Gamma(K)$ has a unique generic type.

References

The material in this section is from [Pillay-Sokolović].

Theorem 10.3 generalizes a theorem of [Michaux] who proved that a quantifier eliminable differential field has no proper Picard-Vessiot extensions.

Poizat's book *Groupes Stables* contains treatments of the Berline-Lascar analysis of superstable groups and the Cherlin-Shelah results on superstable fields.

Appendix A: Seidenberg's Embedding Theorem

In [Seidenberg 1,2] Seidenberg proved that any countable differential field can be embedded into a field of germs of meromorphic functions. This follows from an embedding lemma for finitely generated differential fields.

Let $Mer(U)$ denote the field of meromorphic functions on U, for $U \subseteq \mathbf{C}$ open.

Lemma A.1. Let $K = \mathbf{Q}\langle u_1 \dots u_n\rangle$ and $K_1 = K\langle v\rangle$. Suppose U is an open ball in $\mathbf{C}$ and $\tau : K \to Mer(U)$ is a differential field embedding. Then there is an open ball $V \subseteq U$ and an extension of τ to an differential embedding of K_1 into $Mer(V)$.

Corollary A.2. Let K be a countable differential field. Then K is isomorphic to a subfield of the field of germs of meromorphic functions at the origin.

proof. By viewing K as a limit of finitely generated extensions and iterating A.1 we can find a point x such that K can be embedded into the germs of meromorphic functions at x. By changing coordinates we may assume $x = 0$.

The proof of lemma A.1, uses the following "primitive element theorem" from [Seidenberg 3]. Which we will prove shortly.

Theorem A.3. Suppose K is a differential field with a non-constant element. If u and v are differentially algebraic over K, then $K\langle u, v\rangle = K\langle u + \lambda v\rangle$ for some $\lambda \in K$.

Proof of A.1. Let $g_i = \tau(u_i)$. By shrinking U we may assume that each g_i is analytic on U. Let $\alpha \in U$ such that $f(\alpha) \neq 0$ for all $f \in \mathbf{Q}\langle g_1, \dots, g_m\rangle \setminus \{0\}$. Changing coordinates we may assume that $\alpha = 0$. Let $g_i(z) = \sum c_{i,j} \frac{z^j}{j!}$ for $z \in U$ (shrinking U if necessary). Note that $g_i^{(j)}(0) = c_{i,j}$. By choice of α, $f \mapsto f(0)$ is a field embedding of $\mathbf{Q}\langle g_1, \dots, g_n\rangle$ into $\mathbf{C}$ with $g_i^{(j)} \mapsto c_{i,j}$. As fields

$$\mathbf{Q}\langle g_1, \dots, g_n\rangle \cong \mathbf{Q}(c_{i,j} : i \leq n, j \in \omega).$$

case 1. v is differentially transcendental over K.

Choose $d_0, d_1, d_2, \dots \in \mathbf{C}$ algebraically independent over $\mathbf{Q}(c_{i,j}.i \leq n, j \in \omega)$ and such that $h(z) = \sum d_j \frac{z^j}{j!}$ converges on a neighborhood of $V \subseteq U$ of 0. We claim that $h, h', \dots$ are algebraically independent over $\mathbf{Q}\langle g_1 \dots g_n\rangle$. Suppose p is a polynomial with coefficients in $\mathbf{Q}$ such that

$$p(g_1, g_1', \dots, g_1^{(l)}, \dots, g_n, g_n', \dots g_n^{(l)}, h, \dots, h^{(m)}) = 0.$$

Then

$$p(c_{1,0}, c_{1,1}, \dots, c_{1,l}, \dots, c_{n,0}, c_{n,1}, \dots c_{n,l}, d_0, \dots, d_m) = 0.$$

Since the d_i are algebraically independent $p(\overline{c}, Y_0, \ldots, Y_m)$ is identically zero. Thus by the isomorphism above

$$p(g_1, g_1', \ldots, g_1^{(l)}, \ldots, g_n, g_n', \ldots g_n^{(l)}, Y_0, \ldots, Y_m)$$

is identically zero. Thus h is differentially transcendental over $\mathbf{Q}\langle g_1, \ldots, g_n\rangle$ and $K_1 \cong \mathbf{Q}\langle g_1, \ldots, g_n, h\rangle$.

case 2. v is differentially algebraic over K.

Without loss of generality we may assume that K has differential transcendence degree at least one over $\mathbf{Q}$ (use case 1 to extend K if necessary). Let $u_1, \ldots, u_{n-1}$ be a differential transcendence base for K and let $K_0 = \mathbf{Q}\langle u_1, \ldots, u_{n-1}\rangle$. By the primitive element theorem there are u_n and v such that $K = K_0\langle u_n\rangle$ and $K_1 = K_0\langle v\rangle$. Let r be maximal such that $v, v', \ldots, v^{(r-1)}$ are algebraically independent over K_0. Let p be an irreducible polynomial with coefficients in $\mathbf{Q}$ such that

$$p(u_1, u_1', u_1^{(l)}, \ldots, u_{n-1}, u_{n-1}', u_{n-1}^{(l)}, v, \ldots, v^{(r-1)}, Y)$$

is the minimal polynomial of $v^{(r)}$ over $K_0(v, v', v^{(r-1)})$.

Let $d_0, \ldots, d_{r-1}$ be algebraically independent over $\mathbf{Q}(c_{i,j}.i < n, j \in \omega)$. Since the $c_{i,j}$ are algebraically independent,

$$p(c_1, c_1,', c_1^{(l)}, \ldots, c_{n-1}, c_{n-1}', \ldots c_{n-1}^{(l)}, d_0, \ldots, d_{r-1}, Y)$$

is irreducible. Let d_r be a zero of it. Then $\frac{\partial p}{\partial Y}(\overline{c}, d_0, \ldots, d_r) \neq 0$.

By the implicit function theorem there is W an open neighborhood of $(\overline{c}, d_0, \ldots, d_{r-1})$ and an analytic function $F : W \to \mathbf{C}$ such that $F(\overline{c}, d_0, \ldots, d_{r-1}) = d_r$ and $p(\overline{w}, f(\overline{w})) = 0$ for all $\overline{w} \in W$. Consider the differential equation:

$$y^{(r)} = F(g_1(z), g_1'(z), g_1^{(l)}(z), \ldots, g_{n-1(z)}, g_{n-1}'(z), \ldots, g_{n-1}^{(l)}(z), y, \ldots, y^{(r-1)}).$$

We can find a solution h which is analytic on a neighborhood of 0 such that for $h^{(i)}(0) = d_i$ for $i = 0, \ldots, r$. Sending v to h, gives τ^* an embedding of K_1 extending $\tau | K_0$. Unfortunately, we might have $\tau^*(u_n) = g_n^* \neq g_n$.

Let $d_j = h^{(j)}(0)$ for $j > r$. By shrinking (and shifting) U, we may assume that g_n^* is analytic on U and $g_n^* = \sum c_{n,j}^* \frac{z^j}{j!}$. Thus the map sending $u_i^{(j)}$ to $c_{i,j}$ for $i < n$, $u_n(j)$ to $c_{n,j}^*$ and $v^{(j)}$ to d_j is a field isomorphism from K_1 to

$$\mathbf{Q}(c_{1,0}, c_{1,1}, \ldots, c_{n-1,0}, c_{n-1,1}, \ldots, c_{n,0}^*, c_{n,1}^*, \ldots, d_0, d_1, \ldots).$$

Since

$$\mathbf{Q}(c_{1,0}, c_{1,1}, \ldots, c_{n-1,0}, c_{n-1,1}, \ldots, c^*_{n,0}, c^*_{n,1}, \ldots) \cong$$

$$\mathbf{Q}(c_{1,0}, c_{1,1}, \ldots, c_{n-1,0}, c_{n-1,1}, \ldots, c_{n,0}, c_{n,1}, \ldots),$$

we can find $d^*_0, d^*_1, \ldots$ such that

$$\mathbf{Q}(c_{1,0}, c_{1,1}, \ldots, c_{n-1,0}, c_{n-1,1}, \ldots, c^*_{n,0}, c^*_{n,1}, \ldots, d_0, d_1, \ldots) \cong$$

$$\mathbf{Q}(c_{1,0}, c_{1,1}, \ldots, c_{n-1,0}, c_{n-1,1}, \ldots, c_{n,0}, c_{n,1}, \ldots, d^*_0, d^*_1, \ldots).$$

Let $h_1(z) = \sum d^*_i \frac{z^i}{i!}$. Let F_1 be a function analytic near $(\overline{c}, d^*_0, \ldots, d_{r-1})$ giving a branch of $p = 0$ such that $F(\overline{c}, \overline{d}^*) = d^*_r$. Then h_1 is the unique formal solution to

$$y^{(r)} = F(g_1(z), g_1'(z), g_1^{(l)}(z), \ldots, g_{n-1(z)}, g_{n-1}'(z), \ldots, u_{n-1}(l)(z), y, \ldots, y^{(r-1)})$$

with $y(0) = d^*_0, \ldots, y^{(r)}(0) = d^*_r$. Since the initial value problem has a convergent solution near the origin, h_1 must converge on a neighborhood of 0.

It is easy to see that mapping v to h_1 extends τ to an embedding of K_1 into $Mer(V)$ for some open ball $V \subset \mathbf{C}$.

We now examine the primitive element theorem. First, note that some assumption on K is necessary. If K contains only constant elements and $L = K(u, v)$ where u and v are algebraically independent constants. Then clearly no $u + \lambda v$ generates L/K.

The proof uses the following lemma due to Ritt.

Lemma A.4. Let K be a differential field and let $\xi \in K$ with $\xi' \neq 0$. Let $G(X) \in K\{X\}$ be nontrivial of order n, then there are rational numbers $c_0, \ldots, c_n$ such that $G(\sum c_i \xi^i) \neq 0$.

Proof.

Suppose not. Let $H(X)$ be of minimal order r such that for all rationals $c_0, \ldots, c_n$ $H(\sum c_i \xi^i) = 0$. Let $h(Y_0, \ldots, Y_r) \in K[\overline{Y}]$ such that $H(X) = h(X, X', \ldots, X^{(r)})$. Let $U_j = \sum Z_i (\xi^i)^{(j)}$. Let $g(Z_0, \ldots, Z_n) = h(U_0, \ldots, U_r)$. Then $H(\sum c_i \xi^i) = g(c_0, \ldots, c_n)$.

Since g vanishes on $\mathbf{Q}^{n+1}$, g is identically zero (as $\mathbf{Q}^n$ is Zariski-dense in K^n). Thus $\frac{\partial g}{\partial Z_i} = 0$ for each j.

Thus for $j = 0, \ldots, r$

$$\sum_{i=0}^{r} \frac{\partial h}{\partial U_i} \frac{\partial U_i}{\partial Z_j} = 0.$$

For $j = 0$ we get

$$\frac{\partial h}{\partial U_0} = 0$$

and for $j > 0$

$$\sum_{i=0}^{r} \frac{\partial h}{\partial U_i} \xi^{j(i)} = 0.$$

From this we see that the vectors

$$(\xi, \xi', \ldots, \xi^{(r)}), \ldots, (\xi^r, (\xi^r)', \ldots, (\xi^r)^{(r)})$$

are linearly dependent. By lemma 4.1 they are linearly dependent over C_k. Thus $\sum b_i \xi^r = 0$ for some constants $b_0, \ldots, b_r$ where not all of the b_i are zero. Since ξ is algebraic over C_K (by 2.1), $\xi \in C_K$, a contradiction.

Proof of A.3.

Consider $K\langle u, v\rangle\langle X\rangle$. $u + vX$ is differentially algebraic over $K\langle X\rangle$. Let G be irreducible such that

$$G(X, X', \ldots, X^{(r)}, (u + vX), \ldots, (u + vX)^{(s)}) = 0 \tag{1}$$

and s is minimal.

Let $w = u + vX$. For $i < s$ $\frac{\partial w^{(i)}}{\partial X^{(s)}} = 0$. While for $i = s$ $\frac{\partial w^{(i)}}{\partial X^{(s)}} = v$.

Implicitly differentiating (1) with respect to $X^{(s)}$ we get

$$\frac{\partial G}{\partial X^{(s)}} + \frac{\partial G}{\partial w^{(s)}} v = 0. \tag{2}$$

Because of the minimality of G, $\frac{\partial G}{\partial w^{(s)}}$ is not identically zero. By lemma A.4, we can find $\lambda \in K$ such that $\frac{\partial G}{\partial w^{(s)}}(\lambda, u + v\lambda) \neq 0$. Using (2) we see that $u, v \in K\langle u + v\lambda\rangle$.

Appendix B: The proof of 9.8

In this section we will give Kolchin's proof of Theorem 9.8.

First suppose G and H are algebraic groups defined over an algebraically closed field K, $f : G \to H$ is rational and $x \in G$. As usual we have $f^* : K(H) \to K(G)$ by $f^*g = g \circ f$. This in-turn induces $f : \mathcal{T}_x(G) \to \mathcal{T}_{f(x)}(H)$, by $f\delta(g) = \delta(f^*g)$. Using the isomorphisms between the tangent spaces and the Lie-algebras we obtain $f_x^\# : \mathcal{L}(G) \to \mathcal{L}(H)$.

In particular if $\delta \in \mathcal{T}_x(G)$ and let $D \in \mathcal{L}(G)$ be such that $D_x = \delta$, then $f_x^* D$ is the element E of $\mathcal{L}(H)$, such that $E_{f(x)} = f\delta$.

Lemma B.1: Suppose $f : G \to H$ is a homomorphism, then $f_x^\#$ does not depend on x.

proof:

Let $\delta \in \mathcal{T}_x(G)$ and let $\widehat{D} \in \mathcal{L}(G)$ be such that $\widehat{D}_x = \delta$. Let $D = f_x^\# \widehat{D}$.

For $h \in O_1$.

$$\begin{aligned}
D_1(h) &= T_{f(x)^{-1}} D_{f(x)}(h) \\
&= D_{f(x)}(T^*_{f(x)^{-1}} h) \\
&= D_{f(x)}(t \mapsto h(f(x^{-1})t)) \\
&= f\overline{D}_x(t \mapsto h(f(x^{-1})t)) \\
&= \overline{D}_x(t \mapsto h(f(x^{-1})f(t))) \\
&= \overline{D}_x(t \mapsto h(f(x^{-1}t))).
\end{aligned}$$

Suppose $E = f_y^\# \overline{D}$. Then

$$\begin{aligned}
E_1(h) &= \overline{D}_x(t \mapsto h(f(y^{-1}t))) \\
&= T_{yx^{-1}} \overline{D}_x((t \mapsto h(f(y^{-1}t))) \\
&= \overline{D}_x((t \mapsto h(f(y^{-1}yx^{-1}t))) \\
&= \overline{D}_1(h).
\end{aligned}$$

Thus $D_1 = E_1$ so $D = E$.

If $f : G \to G_1$ and $g : G_1 \to G_2$, then $(g \circ f)_x^\# = g_{f(x)}^\# \circ f_x^\#$.

Lemma B.2: a) If $f : G \to H$ is constantly c, then $f_x^\# = 0$.

b) Let T_v be left multiplication by v, then $(T_v)_x^\#$ is the identity on $\mathcal{L}(G)$.

proof:

a) Let $\delta \in \mathcal{T}_x(G)$ and let $D \in \mathcal{L}(G)$ be such that $D_x = \delta$. Let $E = f_x^\# D$. Since $c \in K$, $E_{f(x)}(h) = f\delta(h) = \delta(h(c)) = 0$ for all $h \in O_{f(x)}$. Thus $E_{f(x)}$ is the trivial tangent vector. So E is the trivial derivation.

b) This is clear since $(T_v)_x^\# D_x = D_{vx}$ for $D \in \mathcal{L}(G)$.

We fix v a point on G. To simplify notation we will refer to the maps $f^{\#}$ as f. [If for a particular map (a non-homomorphism) it is important which tangent space we use to define the map we assume we use the base point v.]

We consider the following maps:
-$i_1, i_2 : G \to G \times G$ by $i_1(x) = (x, v)$, $i_2(x) = (v, x)$.
-$\Delta : G \to G \times G$ is the diagonal map $x \mapsto (x, x)$.
-$\pi_1, \pi_2 : G \times G \to G$ are the projections, $\pi_i(x_1, x_2) = x_i$.
-$i : G \to G$ is the identity.
-$\epsilon : G \to G$ is the zero map.
-$\lambda_v : G \to G$ is right multiplication $x \mapsto xv$.
-$\psi : G \times G \to G$ by $\psi(x, y) = xy^{-1}$.
-for $v \in G$ $\tau(v) : G \to G$ by conjugation, $x \mapsto v^{-1}xv$.

Lemma B.3: $\mathcal{L}(G \times G) = i_1\mathcal{L}(G) \oplus i_2\mathcal{L}(G)$.

proof:
Clearly i_j is injective.
Suppose $i_1D + i_2E = 0$. Then

$$\begin{aligned} D &= iD + \epsilon E \\ &= \pi_1 i_1 D + \pi_1 i_2 E, \text{ by B.2 a)} \\ &= \pi_1 i_1 D + i_2 E) \\ &= 0. \end{aligned}$$

Similarly $E = 0$.
Thus $i_1\mathcal{L}(G) \oplus i_2\mathcal{L}(G)$ has twice the dimension of $\mathcal{L}(G)$, and hence is equal to $\mathcal{L}(G \times G)$.

Lemma B.4: $\Delta = i_1 + i_2$.

proof:
Let $D \in \mathcal{L}(G)$. We will show that for all $g \in K(G)$, $(\Delta D - i_1 D - i_2 D)\pi_i^* g = 0$. Since $K(G \times G) = \pi_1^* K(G) \otimes \pi_2^* K(G)$, this implies $(\Delta D - i_1 D - i_2 D) = 0$.
First, suppose $f \in O_1$, then

$$\begin{aligned} (\Delta D - i_1 D - i_2 D)_{(1,1)} \pi_1^* f &= \pi + 1(\Delta D - i_1 D - i_2 D)_{(1,1)} f \\ &= (\pi_1 \Delta D - \pi_1 i_1 D - \pi_1 i_2 D)_{(1,1)} \\ &= (iD - iD - \epsilon D)_{(1,1)} f \\ &= 0. \end{aligned}$$

Now let $g \in O_s$.

$$\begin{aligned} (\Delta D - i_1 D - i_2 D)\pi_1^* g(s,t) &= (\Delta D - i_1 D - i_2 D)_{(s,t)} \pi_1^* g \\ &= (\Delta D - i_1 D - i_2 D)_{(1,1)} \pi_1^* T_s^* g \\ &= 0 \text{ (by the claim above).} \end{aligned}$$

Thus for all $g \in K(G)$, $(\Delta D - i_1 D - i_2 D)\pi_1 g = 0$. The same is true for π_2. Thus by the above remarks, for all D $\Delta D - i_1 D - i_2 D = 0$. So $\Delta = i_1 + i_2$.

Lemma B.5: $\lambda_v \circ \psi = \pi_1 - \pi_2$.

proof:

For any $x \in G$ $\lambda_v \circ \psi \circ i_1(x) = x$. Thus $\lambda_v \circ \psi \circ i_1$ is the identity map i.

On the other hand for any x, $\lambda_v \circ \psi \circ \Delta(x) = v$. Since this map is constant, the it induces the trivial endomorphism of the Lie-algebra.

By lemma B.4, $\lambda_v \circ \psi \circ i_2 = \lambda_v \circ \psi \circ (\Delta - i_1)$. By the above remarks, this is $-i$.

Thus $(\lambda_v \circ \psi + \pi_2 - \pi_1) \circ i_1 = i + 0 - i = 0$ and $(\lambda_v \circ \psi + \pi_2 - \pi_1) \circ i_2 = -1 + i - 0$.

Thus by lemma B.3, $\lambda_v \circ \psi = \pi_1 - \pi_2$.

Lemma B.6: $\lambda_v = \tau(v)$.

proof:

$\lambda_v = T_v \tau(v)$, but T_v acts on $\mathcal{L}(G)$ as the identity.

For $\delta \in \mathcal{D}(K/k)$, we define a tangent vector at v $l\delta(v)$, the *logarithmic derivative* by $l\delta(v)(g) = \delta(g(v))$. If f is any rational map, then, of course $f(l\delta(v)) = l\delta(f(v))$.

Lemma B.7: $l\delta(xv) = \tau(v)l\delta(x) + l\delta(v)$.

proof:

$$\begin{aligned}
\tau(v)l\delta(x) &= \lambda_v l\delta(\psi(xv, v)) \\
&= \lambda_v \circ \psi l\delta(xv, v) \\
&= \pi_1 - \pi_2 l\delta(xv, v) \\
&= l\delta(xv) - l\delta(v).
\end{aligned}$$

Finally, suppose ω is an invariant differential on G. If $x \in G$, ω_x is the local component of ω at x. We defined the *induced differential* $\omega(x)$ on $\mathcal{D}(K/k)$, by $\omega(x)(\delta) = \omega_x(l\delta(x))$.

In particular if $x, v \in G(K)$, $\omega(xv)(\delta)\omega_{xv}(l\delta(xv))$ By B.7 this is $\omega_{v^{-1}xv}(\tau(v)l\delta(x)) + \omega_v(l\delta(v)$, which is $\tau(v)^*\omega_x(l\delta(x)) + \omega_v(l\delta(v) = (\tau(v)^*\omega(x) + \omega(v))\delta$.

Thus we have proved:

Theorem 9.8: If $x, v \in G(K)$ and ω is an invariant differential on G, then $\omega(xv) = \tau(v)^*\omega(x) + \omega(v)$.

Appendix C: Kolchin's Irreducibility Theorem

This appendix is devoted to the following theorem of Kolchin.

Theorem C.1. Let K be an algebraically closed field with derivation D. Suppose $V \subset K^l$ is an irreducible algebraic variety defined over K. Then V is D-irreducible.

Suppose V is an irreducible variety. Suppose $(\overline{x}, \overline{y}) \in V$ is a generic point of V where we (without loss of generality) we may assume that $x_1, \ldots, x_n$ are algebraically independent and $y_1, \ldots, y_m$ is algebraic over $K(\overline{x})$. For $i = 1, \ldots, m$ let $p_i(\overline{x}, Y)$ be the minimal polynomial of y_i over $K(\overline{x})$. An easy induction shows that for all n,

$$y_i^{(j)} \frac{\partial p_i}{\partial Y}(\overline{x}, y) = r_{i,j}(\overline{x}, \overline{x}', \ldots, \overline{x}^{(j)}, y_i, y_i', \ldots, y_i^{(j-1)})$$

for some polynomial $r_{i,j}$ with coefficients in K.

If $(\overline{x}, \overline{y})$ is a D-generic point of V (ie. a point of maximal Morley rank in $\mathbf{K}$, then $\overline{x}, \overline{x}', \overline{x}^{(2)}, \ldots$ are algebraically independent and

$$K\langle \overline{x}, \overline{y} \rangle = K\langle \overline{x} \rangle(\overline{y}).$$

Thus there is a unique D-generic type.

Since an irreducible algebraic variety has a unique D-generic type this says that there is a unique D-irreducible component of maximal rank. We will need to do a bit more work to show that there is only one D-irreducible component.

Suppose $L \supseteq K$ are differential fields and $\overline{a}, \overline{b} \in L^n$. We say that $\overline{a} \mapsto \overline{b}$ is a *differential specialization* over K if $f(\overline{b}) = 0$, whenever $f \in K\{\overline{X}\}$ and $f(\overline{a}) = 0$.

We will use the following lemma on specializations.

Lemma C.2. Let K be an algebraically closed field with derivation D. Let $V \subseteq K^n$ be an irreducible variety defined over K, $p \notin I(V)$, and let $\alpha \in V$ be a K-rational point. There is a differential field extension $L \supseteq K$ and β an L-rational point of V such that $p(\beta) \neq 0$ and there is $\beta \mapsto \alpha$ is a differential specialization over K.

proof:

If dim $V \geq 2$, let H be a hyperplane through α not contained in $V(p)$. Let W be an irreducible component of $V \cap H$ through α. Then dim W = dim $V - 1$ and $p \notin I(W)$. Thus without loss of generality we may assume V is a curve.

If V is not smooth there is a smooth curve W and a polynomial map $\sigma : W \to V$. Let $\alpha^* \in W \cap \sigma^{-1}(\alpha)$. Suppose there is a differential field $L \supseteq K$ and β^* an L-rational point of W such that $p(\sigma(\beta)) \neq 0$ and $\beta^* \mapsto \alpha^*$ is a differential specialization over K. Let $\beta = \sigma(\beta^*)$. If C is any D-closed set defined over K and $\beta \in K$, then $\beta^* \in \sigma^{-1}C$. Hence $\alpha^* \in \sigma^{-1}C$ and $\alpha \in C$. Thus $\beta \mapsto \alpha$ is the desired specialization. Thus without loss of generality we may assume V is a smooth curve.

Let O_α be the local ring of regular functions at α and let M_α be the maximal ideal of functions vanishing at α. Since V is smooth M_α/M_α^2 is a one dimensional K-vector space. Let $t \in M_\alpha$ be a generator for M_α/M_α^2. Let $K(V)$ be the function field of V, there is a unique derivation $D : K(V) \to K(V)$ extending the derivation on K with $D(t) = 0$.

There is a natural embedding of $K(V)$ into the field of formal Laurent series $K((t))$ sending 0_α into $K[[t]]$ and M_α into $tK[[t]]$. Consider the derivation δ defined on $K((t))$ defined by

$$\delta\Big(\sum_{i=m}^{\infty} a_i t^i\Big) = \sum_{i=m}^{\infty} D(a_i).$$

Clearly $\delta(K[[t]]) \subseteq K[[t]]$ and $\delta(tK[[t]]) \subseteq tK[[t]]$. Since there is a unique derivation from $K(V)$ to $K((t))$ extending D and sending t to 0, we must have $D : O_\alpha \to O_\alpha$ and $D : M_\alpha \to M_\alpha$.

Let $\pi : O_\alpha \to K$ be the evaluation map $f \mapsto f(\alpha)$. If $f \in O_\alpha$, then for some $a \in K$, and $g \in M_\alpha$, $f = a + g$. Then

$$\begin{aligned}\pi(D(f)) &= \pi(D(a) + D(g)) \\ &= D(a) + \pi(D(g)) \\ &= D(a)\end{aligned}$$

since $D(g) \in M$. Since $D(a) = D(\pi f)$, π commutes with D, thus π is a differential specialization.

Let $L = K(V)$. Let $\beta = (x_1, \ldots, x_n) \in L$ be the coordinate functions. Clearly $\pi(\beta) = \alpha$. Since p is not identically 0 on V, $p(\beta) \neq 0$.

We now give the proof of C.2.

Let p_i and $r_{i,j}$ be the polynomials described above. If $(\overline{x}, \overline{y})$ is any point of V, then $p_i(\overline{u}, v_i) = 0$ and

$$y_i^{(j)} \frac{\partial p_i}{\partial Y}(\overline{x}, y) = r_{i,j}(\overline{x}, \overline{x}', \ldots, \overline{x}^{(j)}, y_i, y_i', \ldots, y_i^{(j-1)})$$

for all j.

Let

$$p(\overline{X}, \overline{Y}) = \prod_{i=1}^{m} p_i(\overline{X}, Y_i).$$

For any $f(\overline{X}, \overline{Y}) \in K\{\overline{X}, \overline{Y}\}$ there is a polynomial g with coefficients in K and natural numbers s and t such that if $p(\overline{x}, \overline{y}) \neq 0$, then

$$f(\overline{x}, \overline{y}) = \frac{g(\overline{x}, \overline{x}', \ldots, \overline{x}^{(s)}, \overline{y})}{p(\overline{x}, \overline{y})^t}.$$

Suppose $(\overline{u}, \overline{v}) \in V$ is D-generic and $f(\overline{u}, \overline{v}) = 0$. Then $g(\overline{u}, \overline{u}', \ldots, \overline{u}^{(s)}, y) = 0$. Since $\overline{u}, \overline{u}', \ldots, \overline{u}^{(s)}$ are algebraically independent, $g(\overline{X}, \overline{X}', \overline{X}^{(s)}, \overline{Y}) = h_0(\overline{X}, Y)h_1(\overline{X}, Y)$

where $h_0 \in K[\overline{X}, \ldots, \overline{X}^{(s)}, \overline{Y}]$ and $h_1 \in K[\overline{X}, \overline{Y}]$ and $h_1 \in K[\overline{X}, \overline{Y}]$ vanishes on all of V. It follows that if $f \in K\{\overline{X}, \overline{Y}\}$ vanishes at the D-generic of V, then f vanishes on $\{(\overline{x}, \overline{y}) \in V : p(\overline{x}, \overline{y}) \neq 0\}$.

Since for any $\alpha \in V$, we can find $L \subset K$ and an L-rational point β in $V \setminus V(p)$ with $\beta \mapsto \alpha$ a differential specialization, it follows that any $f(\overline{X}, \overline{Y})$ which vanishes on the D-generic of V vanishes on all of V. Thus if W is the D-irreducible component containing the D-generic, we must have $V = W$.

REFERENCES

Books

J. Baldwin, *Fundamentals of Stability Theory*, Springer Verlag, 1988.

M. Hirsh and S. Smale, *Differential Equations, Dynamical Systems and Linear Algebra*, Academic Press, 1974.

A. Buium, *Differential Algebra and Diophantine Geometry*, Hermann, 1994.

I. Kaplansky, *Differential Algebra*, Hermann, 1957.

E. Kolchin, *Differential Algerbra and Algebraic Groups*, Academic Press, 1973.

S. Lang, *Algebra*, Addison Wesley, 1971.

S. Lang, *Introduction to Algebraic Geometry*, Interscience, 1959 .

D. Lascar, *Stability in Model Theory*, Longman Scientific & Technical, 1987.

A. Magid, *Lectures on Differential Galois Theory*, American Mathematical Society, 1994.

B. Poizat, *Cours de Théorie des Modèles*, Nur al-Mantiq wal-Ma'rifah, 1987.

B. Poizat, *Groupes Stables*, Nur al-Mantiq wal-Ma'rifah, 1985.

J. Ritt, *Differential Algebra*, Dover, 1950.

G. Sacks, *Saturated Model Theory*, Benjamin,1972.

Papers

[Berline-Lascar] C, Berline and D. Lascar, "Superstable groups", Annals pure and applied logic, vol 30, 1986.

[Blum] "Differentially closed fields: a model theoretic tour", in *Contributions to Algebra*, ed. H. Bass, P. Cassidy and J. Kovacic, Academic Press 1977.

[Brestovski] M. Brestovski, " Algebraic independence of solutions of differential equations of the second order", Pacific J. Math. vol 140, 1989.

[Cherlin-Shelah] G. Cherlin and S. Shelah, "Superstable fields and groups", Annals Math. Logic vo1 18, 1980.

[Gramain 1] F. Gramain, "Non-minimalite de la clôture différentielle I: la preuve de S. Shelah", *Theories Stables*, Paris Seminar Notes 1980-83.

[Gramain 2] F. Gramain, "Non-minimalite de la clôture différentielle II: la preuve de M. Rosenlicht", *Theories Stables*, Paris Seminar Notes 1980-83.

[Hrushovski-Sokolović] E. Hrushovski and Ž. Sokolović, "Minimal subsets of differentially closed fields", Trans. AMS, to appear.

[Kolchin 1] E. Kolchin,"Existence theorems connected with the Picard-Vessiot theory of homogeneous linear ordinary differential equations", Bulletin AMS vol.54, 1948.

[Kolchin 2] E. Kolchin, "Galois Theory of Differential Fields", Amer. J. Math vol 75, 1953.

[Kolchin 3] E. Kolchin, "Constrained extensions of differential fields", Advances in Math. vol 12, 1974

[Kolchin 4] E. Kolchin, " Algebraic matrix groups and the Picard-Vessiot theory of homogeneous linear ordinary differential equations" Annals of Math vol 49, 1948.

[Kolchin 5] E. Kolchin, "On the Galois Theory of Differential Fields", Amer. J. Math vol 77,1955.

[Kolchin 6] E. Kolchin, "Abelian extensions of differential fields, Amer. J. Math, vol 82, 1960.

[Lascar 1] D. Lascar, "Les corps différentiellement clos dénomrables", *Theories Stables*, Paris Seminar Notes 1980-83.

[Lascar 2] D. Lascar, "Relation entre le rang U et le poids", Fundamenta Mat. vol 121 (1984).

[Macintrye-McKenna-van den Dries] A. Macintyre, K. McKenna and L. van den Dries, "Elimination of quantifiers in algebraic structures", Advances in Math vol 47, 1983.

[Marker] "Introduction to the model theory of fields", this volume.

[Michaux] C. Michaux," Sur l'élimination des quantificateurs dans les anneaux différentiels, Comptes Rendus 47, 1983.

[Pillay] A. Pillay, "Differential algebraic groups and the number of countable differentially closed fields", this volume.

[Pillay-Sokolović], A. Pillay and Ž. Sokolović, "Superstable differential fields", JSL 57, 1992.

[Poizat 1] B. Poizat, "Deux remarques à propos de la propriété de recouvrement fini", Journal of Symbolic Logic, vol 49, 1984.

[Poizat 2] B. Poizat, "Rangs des types dan les corps différentiels", *Theories Stables*, Paris Seminar Notes 1977/78.

[Poizat 3] B. Poizat, "Une théorie de Galois imaginaire", Journal of Symbolic Logic vol 48, 1983.

[Poizat 4] B. Poizat, "C'est beau et chaud", *Theories Stables*, Paris Seminar Notes 1980-83.

[Rosenlicht 1] M. Rosenlicht, "The non-minimality of differential closure", Pacific J. Math. vol 52, 1974.

[Rosenlicht 2] M. Rosenlicht, "On Lioulville's theory of elementary functions", Pacific J. Math, vol 65, 1976.

[Rosenlicht 3] M. Rosenlicht, "A note on derivations and differentials on algebraic groups", Portugal Math vol 16, 1957.

[Seidenberg 1] A. Seidenberg, "Abstract differential algebra and the analytic case", Proc. AMS vol. 9, 1958.

[Seidenberg 2] A. Seidenberg, "Abstract differential algebra and the analytic case II", Proc. AMS vol. 23, 1969.

[Seidenberg 3] A. Seidenberg, "Some basic theorems in differential algebra (characteristic p, arbitrary), Trans. AMS vol. 73, 1952.

[Shelah] S. Shelah, "Differentially closed fields", Israel J. Mathematics vol 16, 1973.

[Wood] C. Wood, "The model theory of differential fields revisited", Israel Journal of Mathematics, vol 25, 1976.