DIFFERENTIAL GALOIS THEORY
BANACH CENTER PUBLICATIONS, VOLUME 58
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 2002

A STRUCTURE THEOREM FOR DIFFERENTIAL ALGEBRAS

MARCUS TRESSL

NWF-I Mathematik, Universität Regensburg, 93040 Regensburg, Germany
E-mail: marcus.tressl@mathematik.uni-regensburg.de

The theorem mentioned in the title is

THEOREM 1. *Let $S = (S, \partial_1, \ldots, \partial_K)$ be a differential domain in K commuting derivatives, containing $\mathbb{Z}$ and let $R = (R, \partial_1, \ldots, \partial_K) \subseteq (S, \partial_1, \ldots, \partial_K)$ be a differential subring such that S is differentially finitely generated over R. Then there are R-subalgebras B and P of S and an element $h \in B$, $h \neq 0$ such that:*

(a) B is a finitely generated R-algebra and B_h is a finitely presented R-algebra.
(b) $S_h = (B \cdot P)_h$ is a differentially finitely presented R-algebra.
(c) The homomorphism $B \otimes_R P \to B \cdot P$ induced by multiplication is an isomorphism of R-algebras.
(d) P has the following structure. For each subset Δ of $\{\partial_1, \ldots, \partial_K\}$ there is an R-subalgebra P_Δ of P such that P_Δ together with the derivatives from Δ is a differential polynomial ring in these derivatives and finitely many variables (the case $P_\Delta = R$ is not excluded). The homomorphism

$$\bigotimes_{\Delta \subseteq \{\partial_1, \ldots, \partial_K\}} P_\Delta \to P$$

induced by multiplication is an isomorphism of R-algebras.

If R is a differential ring as in the theorem, then a differential R-algebra S is a quotient of a differential polynomial ring $R\{Y\}$ over R modulo a differential ideal $\mathfrak{a}$. One of the fundamental tools of differential algebra is a reduction process of polynomials $F \in R\{Y\}$ with respect to such ideals as explained in Kolchin's book [2]; provided $\mathbb{Z} \subseteq R \subseteq S$ and S is a domain. We translate the result of this reduction in terms of the differential algebra S. In the case where $R = \mathbb{R}$ is the field of real numbers and the number of derivatives K is 1, our structure theorem can be used to reduce the solvability of an ordinary system of differential equations to an algebraic question on the system. This is done in [1].

2000 *Mathematics Subject Classification*: Primary 12H05; Secondary 13N.
The paper is in final form and no version of it will be published elsewhere.

In section 1 we recall the definition of a characteristic set (in characteristic 0) from [2]. In section 2 we recall the result of the reduction process with respect to characteristic sets and how differential prime ideals can be recovered from their characteristic sets. In section 3 we translate these facts into the proof of Theorem 1.

1. Definition of characteristic sets. Let R be a differential ring in K pairwise commuting derivatives $\partial_1, \dots, \partial_K$. Let $Y := (Y_1, \dots, Y_N)$ be a tuple of N indeterminates over R and let $\mathcal{D} := \{\partial_1^{i_1} \dots \partial_K^{i_K} \mid i_1, \dots, i_K \in \mathbb{N}_0\}$ be the free abelian monoid generated by $\{\partial_1, \dots, \partial_K\}$, which we denote multiplicatively. For each $D \in \mathcal{D}$ and $n \in \{1, \dots, N\}$ let DY_n be an indeterminate, where $DY_n = Y_n$ if $D = \partial_1^0 \dots \partial_K^0$ by definition. Moreover let

$$\mathcal{D}Y := \{DY_n \mid D \in \mathcal{D}, 1 \leq n \leq N\}.$$

The differential polynomial ring over R in K derivatives and N indeterminates is the polynomial ring $R\{Y\} := R[y \mid y \in \mathcal{D}Y]$ together with the uniquely determined derivations ∂_i such that $\partial_i(r \cdot DY_n) = (\partial_i r) \cdot DY_n + r \cdot (\partial_i D) Y_n$ $(1 \leq i \leq K,\ 1 \leq n \leq N,\ r \in R)$. So $R\{Y\}$ is a differential ring extension of R and $R\{Y\}$ is the free object generated by N elements over R in the category of differential rings with K commuting derivatives. The set of all powers of variables from $\mathcal{D}Y$ is denoted by

$$\mathcal{D}Y^* := \{y^p \mid y \in \mathcal{D}Y, p \in \mathbb{N}\}.$$

Definition 1. The *rank* on $\mathcal{D}Y^*$ is the map $\mathrm{rk} : \mathcal{D}Y^* \to \mathbb{N}_0 \times \{1, \dots, N\} \times \mathbb{N}_0^K \times \mathbb{N}$ defined by

$$\mathrm{rk}(\partial_1^{i_1} \dots \partial_K^{i_K} Y_n)^p := (i_1 + \dots + i_K, n, i_K, \dots, i_1, p).$$

The set $\mathcal{O} := \mathbb{N}_0 \times \{1, \dots, N\} \times \mathbb{N}_0^K \times \mathbb{N}$ equipped with the lexicographic order (hence the first component is the dominating one) is well ordered. Note that the order type of the image of rk in $\mathcal{O}$ is the order type of $\mathbb{N}$.

Definition 2. We say a variable $y \in \mathcal{D}Y$ *appears* in $f \in R\{Y\}$ if y appears in f considered as an ordinary polynomial (hence Y_1 does not appear in $\partial_1 Y_1$). The *leader* u_f of $f \in R\{Y\} \setminus R$ is the variable $y \in \mathcal{D}Y$ of highest rank which appears in f. Moreover $u_f^* := u_f^{\deg_{u_f} f} \in \mathcal{D}Y^*$ denotes the highest power of u_f in f. We extend the rank to polynomials $f \in R\{Y\}$ by

$$\mathrm{rk}(f) := \mathrm{rk}(u_f^*) \in \mathcal{O}.$$

Definition 3. If $g, f \in R\{Y\}$, $g \notin R$ are polynomials, then f is called *weakly reduced* with respect to g if no proper derivative of u_g appears in f. f is called *reduced* with respect to g if f is weakly reduced with respect to g and if $\deg_{u_g} f < \deg_{u_g} g$.

The polynomial f is called (weakly) reduced with respect to a nonempty set $G \subseteq R\{Y\} \setminus R$ if f is (weakly) reduced with respect to every $g \in G$.

A nonempty subset $G \subseteq R\{Y\} \setminus R$ is called *autoreduced* if every $f \in G$ is reduced with respect to all $g \in G$, $g \neq f$. If G consists of a single element then G is called autoreduced as well.

It is easy to see that $u_f \neq u_g$ (hence $\mathrm{rk}\, f \neq \mathrm{rk}\, g$) if f, g are different polynomials from an autoreduced set. Moreover, by [2], Chap. O, Section 17, Lemma 15 (a) we have

Proposition 2. *Every autoreduced set is finite.* ∎

Let ∞ be an element bigger than every element in $\mathcal{O}$ and let $(\mathcal{O}\cup\{\infty\})^{\mathbb{N}}$ be equipped with the lexicographic order. We define the rank of an autoreduced set G to be an element of $(\mathcal{O}\cup\{\infty\})^{\mathbb{N}}$ as follows. Let $G=\{g_1,\ldots,g_l\}$ with $\operatorname{rk} g_1<\ldots<\operatorname{rk} g_l$. Then

$$\operatorname{rk} G := (\operatorname{rk} g_1,\ldots,\operatorname{rk} g_l,\infty,\infty,\ldots).$$

Proposition 3. *There is no infinite sequence* $G_1, G_2, \cdots$ *of autoreduced sets with the property* $\operatorname{rk} G_1 > \operatorname{rk} G_2 > \cdots$.

Proof. [2], Chap. I, Section 10, Proposition 3. ∎

Definition 4. If $M\subseteq R\{Y\}$ is a set not contained in R, then by Proposition 3 the set $\{\operatorname{rk} G \mid G\subseteq M \text{ is autoreduced }\}$ has a minimum. Every autoreduced subset G of M with this rank is called a *characteristic* set of M.

Proposition 4. *If G is a characteristic set of $M\subseteq R\{Y\}$ and $f\in M\setminus R$, then f is not reduced with respect to G.*

Proof. If $f\in M\setminus R$ is reduced with respect to G, then the set $\{g\in G \mid \operatorname{rk} g < \operatorname{rk} f\}\cup\{f\}$ is an autoreduced subset of M of rank strictly lower than the rank of G, which is impossible. ∎

2. Fundamental properties of characteristic sets. From now on we assume that R is a differential domain in K derivatives containing $\mathbb{Z}$.

Definition 5. Let $f\in R\{Y\}\setminus R$, $f=f_d u_f^d+\ldots+f_1u_f+f_0$ with polynomials $f_d,\ldots,f_0\in R[y\in\mathcal{D}\mid y\neq u_f]$ and $f_d\neq 0$. The *initial* $I(f)$ of f is defined as

$$I(f):=f_d.$$

The *separant* $S(f)$ of f is defined as

$$S(f):=\frac{d}{du_f}f=d\cdot f_d u_f^{d-1}+\ldots+f_1.$$

Moreover, for every autoreduced subset $G=\{g_1,\ldots,g_l\}$ of $R\{Y\}$ we define

$$H(G):=\prod_{i=1}^{l} I(g_i)\cdot S(g_i) \text{ and } H_G:=\Big\{\prod_{i=1}^{l} I(g_i)^{n_i}S(g_i)^{m_i} \mid n_i,m_i\in\mathbb{N}_0\Big\}.$$

Since R is a domain and $\mathbb{Z}\subseteq R$ the set H_G does not contain 0. Moreover, $S(g)$ and $I(g)$ are reduced with respect to G ($g\in G$).

Theorem 5. *Let $G\subseteq R\{Y\}$ be an autoreduced set and let $f\in R\{Y\}$. Let $[G]$ denote the differential ideal generated by G in $R\{Y\}$ and let (G) denote the ideal generated by G in $R\{Y\}$. Then there is some $\tilde f\in R\{Y\}$ which is reduced with respect to G and some $H\in H_G$ such that $H\cdot f\equiv \tilde f \operatorname{mod}[G]$. If f is weakly reduced with respect to G, then we can take H such that $H\cdot f\equiv\tilde f\operatorname{mod}(G)$.*

Proof. [2], Chap. I, Section 9, Proposition 1. ∎

Corollary 6. *If G is a characteristic set of a differential prime ideal $\mathfrak{p}$ of $R\{Y\}$ with $\mathfrak{p} \cap R = 0$ then*

$$\mathfrak{p} = \{f \in R\{Y\} \mid H(G)^n \cdot f \in [G] \text{ for some } n \in \mathbb{N}_0\}.$$

Moreover if $f \in \mathfrak{p}$ is weakly reduced with respect to G, then $H(G)^n \cdot f \in (G)$ for some $n \in \mathbb{N}_0$.

Proof. From Theorem 5 and Proposition 4, since $H_G \cap \mathfrak{p} = \emptyset$. ■

3. Proof of Theorem 1. Since S is a differentially finitely generated R-algebra, there is some $N \in \mathbb{N}$ and a surjective differential homomorphism $\varphi : R\{Y_1, \ldots, Y_N\} \to S$. Let $Y := (Y_1, \ldots, Y_N)$ and let $\mathfrak{p}$ be the kernel of φ. Since $R \subseteq S$ and S is a differential domain, the ideal $\mathfrak{p}$ is a differential prime ideal of $R\{Y\}$ with $\mathfrak{p} \cap R = 0$. Let G be a characteristic set of $\mathfrak{p}$ (c.f. Definition 4). First we define B, P and h. We take $h := \varphi(H(G))$ ($H(G)$ is defined in Definition 5),

$$V := \{y \in \mathcal{D}Y \mid y \text{ is not a proper derivative of any } u_g\},$$

$$V_B := \{y \in V \mid y \text{ appears in some } g \in G\},$$

$$B := \varphi(R[V_B]) \quad \text{and} \quad P := \varphi(R[V \setminus V_B]).$$

Since G is an autoreduced set, a polynomial $f \in R\{Y\}$ is weakly reduced with respect to G if and only if $f \in R[V]$.

Claim 1. *The restriction of φ to the subring $R[V \setminus V_B]$ of $R\{Y\}$ is injective.*

Proof. Let $f \in R[V \setminus V_B] \cap \mathfrak{p}$. Since f is weakly reduced with respect to G and all leaders of elements $g \in G$ are in V_B we have that f is reduced with respect to G. Since G is a characteristic set of $\mathfrak{p}$ we get $f = 0$ from Proposition 4 and $\mathfrak{p} \cap R = 0$. This proves the claim.

Claim 2. *$h \neq 0$ and $S_h = (B \cdot P)_h$.*

Proof. Since every $S(g), I(g)$ with $g \in G$ is reduced with respect to G we have $H(G) \notin \mathfrak{p}$. As $H(G) \in R[V_B]$ it follows $B \ni h = \varphi(H(G)) \neq 0$.

Let $f \in R\{Y\}$. By Theorem 5 there is some $\tilde{f} \in R\{Y\}$ which is reduced with respect to G and some $H \in H_G$ such that $H \cdot f \equiv \tilde{f} \bmod [G]$. Since $\tilde{f} \in R[V]$ and every $I(g), S(g)$ is invertible in $(B \cdot P)_h$ we get $\varphi(f) \in (B \cdot P)_h$. This shows that $S_h = (B \cdot P)_h$.

Claim 3. *S_h is a differentially finitely presented R-algebra and B_h is a finitely presented R-algebra.*

Proof. First we prove that S_h is differentially finitely presented over R. The differential homomorphism $R\{Y\} \to S \hookrightarrow S_h$ maps $H(G)$ onto a unit in S_h, hence φ can be extended to a surjective differential homomorphism $\psi : R\{Y\}[H(G)^{-1}] \to S_h$ mapping $H(G)^{-1}$ to h^{-1}. Since $R\{Y\}[H(G)^{-1}]$ is a differentially finitely generated R-algebra (with generators $Y_1, \ldots, Y_N, H(G)^{-1}$) it is enough to prove that $\operatorname{Ker} \psi$ is generated by G as a differential ideal. As ψ extends φ we have $G \subseteq \operatorname{Ker} \psi$. Conversely if $f \in R\{Y\}$ and $d \in \mathbb{N}$ with $\psi(f/H(G)^d) = 0$ we get $f \in \mathfrak{p}$ from $h \neq 0$, hence $H(G)^n \cdot f \in [G]$ for some $n \in \mathbb{N}$ by Corollary 6. This shows that $f/H(G)^d$ is in the differential ideal generated by G in $R\{Y\}[H(G)^{-1}]$.

Now we show that B_h is a finitely presented R-algebra. Similar as above we get a surjective R-algebra homomorphism $\psi : R[V_B]_{H(G)} \to B_h$ extending $\varphi|_{R[V_B]}$ with $\psi H(G)^{-1} = h^{-1}$ and it is enough to show that the ideal $\operatorname{Ker}\psi$ is generated by G. If $f \in R[V_B]$ and $d \in \mathbb{N}$ with $\psi(f/H(G)^d) = 0$ we get $f \in \mathfrak{p}$. Since f is weakly reduced with respect to G we get $H(G)^n \cdot f \in (G)$ for some $n \in \mathbb{N}$ from Corollary 6. Since G, f and $H(G)$ are in $R[V_B]$, f is in the ideal generated by G in $R[V_B]_{H(G)}$. This finishes the proof of claim 3.

Claims 2 and 3 prove assertions (a) and (b) of Theorem 1.

Claim 4. *If $b_1, \ldots, b_m \in B$ are linearly dependent over P, then they are linearly dependent over R.*

Proof. Take $f_i \in R[V_B]$ with $\varphi f_i = b_i$ and $p_i \in R[V \setminus V_B]$, not all contained in $\mathfrak{p}$ with $q := p_1 f_1 + \ldots + p_m f_m \in \mathfrak{p}$. We may assume that $p_1 \notin \mathfrak{p}$. Since $q \in R[V]$, q is weakly reduced with respect to G. By Corollary 6 there is some $n \in \mathbb{N}$ and polynomials $h_g \in R\{Y\}$ $(g \in G)$ such that $H(G)^n \cdot q = \sum_{g \in G} h_g \cdot g$. Since $H(G), q \in R[V]$ and $G \subseteq R[V]$ we may assume that each $h_g \in R[V]$ as well. Since $p_1 \neq 0$ there is an R-algebra homomorphism $\psi : R[V \setminus V_B] \to R$ with $\psi(p_1) \neq 0$. Clearly ψ can be extended to an $R[V_B]$-algebra homomorphism $\psi : R[V] \to R[V_B]$. Since all p_i are in $R[V]$ we may apply ψ to the equation $H(G)^n \cdot (p_1 f_1 + \ldots + p_m f_m) = \sum_{g \in G} h_g \cdot g$. Since $H(G), f_i \in R[V_B]$ and $G \subseteq R[V_B]$ we get $H(G)^n \cdot (\psi(p_1) f_1 + \ldots + \psi(p_m) f_m) \in \sum_{g \in G} R[V_B] \cdot g$. Applying φ to this equation yields $h^n \cdot (\varphi(\psi(p_1)) b_1 + \ldots + \varphi(\psi(p_m)) b_m) = 0$. Since $h \neq 0$ and $\varphi(\psi(p_1)) = \psi(p_1) \neq 0$ the latter equation shows that $b_1, \ldots, b_m$ are linearly dependent over R and claim 4 is proved.

Claim 4 implies item (c) of Theorem 1 as follows. Suppose $B \otimes_R P \to B \cdot P$ is not injective. Take a minimal $m \in \mathbb{N}$ such that there are $b_1, \ldots, b_m \in B$ and $p_1, \ldots, p_m \in P$ with $p_1 b_1 + \ldots + p_m b_m = 0$ and $x := p_1 \otimes b_1 + \ldots + p_m \otimes b_m \neq 0$. Then $b_1, \ldots, b_m$ are linearly dependent over P. So by claim 4 there are $r_1, \ldots, r_m \in R$ not all zero with $r_1 b_1 + \ldots + r_m b_m = 0$. Say $r_1 \neq 0$. Then $m > 1$ and $r_1 \cdot x = (r_1 p_2 - r_2 p_1) \otimes b_2 + \ldots + (r_1 p_m - r_m p_1) \otimes b_m$. From the minimal choice of m we get $r_1 \cdot x = 0$. Let F be the quotient field of R. Then $1 \otimes x = \frac{1}{r_1} \otimes r_1 x = 0$ in $F \otimes_R (B \otimes_R P)$. By claim 1, P is a polynomial ring over R, hence a flat R-algebra. As $B \to F \otimes_R B$ is injective, it follows that $B \otimes_R P \to F \otimes_R B \otimes_R P$ is injective. So $1 \otimes x = 0$ in $F \otimes_R B \otimes_R P$ implies $x = 0$, a contradiction.

Finally we show that $P \cong R[V \setminus V_B]$ can be decomposed as claimed in (d). Let $\rho \in \mathbb{N}$ be strictly bigger than every $\operatorname{ord}_i u_g$ $(1 \leq i \leq K, g \in G)$. Here $\operatorname{ord}_i(\partial_1^{k_1} \ldots \partial_K^{k_K} Y_j) := k_i$. Let $V_\emptyset := \{y \in V \setminus V_B \mid \operatorname{ord}_i y < \rho \ (1 \leq i \leq K)\}$ and let

$$\begin{aligned} W := \{y \in V \mid\ & \operatorname{ord}_i y \leq \rho \ (1 \leq i \leq K) \text{ and} \\ & \operatorname{ord}_i y = \rho \text{ for at least one } i \in \{1, \ldots, K\}\}. \end{aligned}$$

For every nonempty subset Δ of $\{\partial_1, \ldots, \partial_K\}$ let

$$W_\Delta := \{w \in W \mid \operatorname{ord}_i w = \rho \iff \partial_i \in \Delta \ (1 \leq i \leq K)\} \text{ and}$$
$$V_\Delta := \{\partial_1^{k_1} \ldots \partial_K^{k_K} w \mid w \in W_\Delta \text{ and } k_i = 0 \text{ for all } i \in \{1, \ldots, K\} \text{ with } \partial_i \notin \Delta\}$$

So, if $W_\Delta = \emptyset$ then $V_\Delta = \emptyset$. Also, $y \in V_\Delta$ if and only if $y = Dw$ for a higher derivative D in the derivatives from Δ.

CLAIM 5. *We have*

(i) If $y \in V_\Delta$ and $\partial_i \in \Delta$, then $\partial_i y \in V_\Delta$. It follows that $R[V_\Delta]$ together with the derivatives from Δ is the differential polynomial ring in these derivatives, in the variables from W_Δ.

(ii) $V \setminus V_B$ is the disjoint union of the V_Δ ($\Delta \subseteq \{1, \dots, K\}$).

Proof. (i). We have to show $\partial_i y \in V$ whenever $y \in V_\Delta$ and $\partial_i \in \Delta$. Since $y = Dw$ for some $w \in W_\Delta \subseteq V$ and only derivatives from Δ appear in D, y cannot be a derivative of any u_g.

(ii). Clearly $V_\Delta \cap V_{\tilde{\Delta}} = \emptyset$, whenever $\Delta \neq \tilde{\Delta}$. Let $y \in V \setminus (V_B \cup V_\emptyset)$ be a derivative of Y_j, hence $\operatorname{ord}_i y \geq \rho$ for some $i \in \{1, \dots, K\}$. Let $\Delta := \{\partial_i \mid \operatorname{ord}_i y \geq \rho\}$ and let $k_i := \min\{\operatorname{ord}_i y, \rho\}$ $(1 \leq i \leq K)$. Then $w := \partial_1^{k_1} \dots \partial_K^{k_K} Y_j \in W_\Delta$ and $y \in V_\Delta$. This proves (ii).

We define $P_\Delta := \varphi(R[V_\Delta])$. By claim 1 and (c) we get (d) from (i) and (ii). ∎

References

[1] T. Grill, M. Knebusch and M. Tressl, *An existence theorem for systems of implicit differential equations*, this volume.

[2] E. R. Kolchin, *Differential Algebra and Algebraic Groups*, Pure Appl. Math. 54, Academic Press, 1973.