CHARACTERISTIC SETS

MARCUS TRESSL

Abstract. We give a detailed and self-contained introduction to Kolchin's approach, mostly in characteristic 0 (cf. [Kol]), including a full proof of the Rosenfeld lemma.

Contents

Date: April 24, 2020.
2000 *Mathematics Subject Classification.* Primary: XXXXX, Secondary: XXXXX.
Thanks to...

1. Auto reduced sets

1.1. **Definition.** Let
$$\mathscr{D} := \{\partial_1^{i_1}...\partial_K^{i_K} \mid i_1,...,i_K \in \mathbb{N}_0\}$$
be the free abelian monoid generated by $\Delta := \{\partial_1,...,\partial_K\}$, written multiplicatively. Here $\mathbb{N}_0 = \{0,1,2,3\ldots\}$, whereas $\mathbb{N} = \{1,2,3,\ldots\}$. Let $R = (R,\Delta_1,...,\Delta_K)$ be a unitary, commutative, differential ring in K commuting derivations. Let $N \in \mathbb{N}$. For $n \in \{1,...,N\}$ and $\theta \in \mathscr{D}$ let θY_n be an indeterminate over R. Then the differential polynomial ring of R in the indeterminates $Y_1,...,Y_N$ is defined as
$$A := R\{Y_1,...,Y_N\} := R[\theta Y_n \mid \theta \in \mathscr{D},\ n \in \{1,...,N\}]$$
(where $\theta Y_N = Y_N$ if $\theta = \partial_1^0...\partial_K^0$ by definition), together with the unique derivations $\Delta_i : A \longrightarrow A$ satisfying $\Delta_i(r\theta Y_n) := \Delta_i(r)\theta Y_n + r(\partial_i\theta)Y_n$ for every $r \in R$, $n \in \{1,...,N\}$ and $\theta \in \mathscr{D}$. So A is a differential ring extension of R and A is the free object generated by N elements over R in the category of differential rings with K commuting derivatives.

From now on we also write $\partial_1,...,\partial_K$ for the derivations $\Delta_1,....,\Delta_K$ given on R. This will not lead to confusion and increases readability.

1.2. *Notation.* Let $f \in R\{Y\}$. We say that a **monomial** M **occurs in** f or **appears** in f, if there are $l \geq 0$, $a_i \in R$, monomials $U_i \neq M$ $(1 \leq i \leq l)$ and some $a \in R$, $a \neq 0$ such that $f = aM + \sum_{i=1}^{l} a_iU_i$. In particular no monomial occurs in the zero polynomial.

We say that a **variable** θY_n **occurs in** f or **appears** in f, if θY_n divides a monomial occurring in f.[1]

By convention, if we say θY_n occurs or appears in f we mean θY_n occurs in f as a variable.

1.3**. The rank on variables** Throughout we work with one specific rank on monomials. Notice that in [Kol] an axiomatic approach of the notion of “rank" is given.

The rank on $\mathscr{D}$ is the map $\mathrm{rk} : \mathscr{D} \longrightarrow \mathbb{N}_0 \times \mathbb{N}_0^K$ defined by
$$\boxed{\mathrm{rk}(\partial_1^{i_1}...\partial_K^{i_K}) := (i_1+...+i_K, i_K,...,i_1),}$$
where the monoid $\mathbb{N}_0 \times \mathbb{N}_0^K$ is ordered lexicographically.

Let $\mathscr{D}Y$ be the set $\{\theta Y_n \mid \theta \in \mathscr{D},\ n \in \{1,...,N\}\}$ of indeterminates (also called “variables"). The rank on $\mathscr{D}Y$ is the map $\mathrm{rk} : \mathscr{D}Y \longrightarrow \mathbb{N}_0 \times \{1,...,N\} \times \mathbb{N}_0^K$ defined by
$$\boxed{\mathrm{rk}(\partial_1^{i_1}...\partial_K^{i_K}Y_n) := (i_1+...+i_K, n, i_K,...,i_1),}$$
where the set $\mathbb{N}_0 \times \{1,...,N\} \times \mathbb{N}_0^K$ is ordered lexicographically. Observe that $\mathrm{rk} : \mathscr{D}Y \longrightarrow \mathbb{N}_0 \times \{1,...,N\} \times \mathbb{N}_0^K$ is a monoid embedding and the image of rk in $\mathbb{N}_0 \times \{1,...,N\} \times \mathbb{N}_0^K$ has the order type of $\mathbb{N}$ (since every element in that image has only finitely many predecessors in that image).

Let $\mathscr{D}Y^*$ be the set $\{(\theta Y_n)^p \mid \theta \in \mathscr{D},\ n \in \{1,...,N\}, p \in \mathbb{N}\} \subseteq A$. The rank on $\mathscr{D}Y^*$ is the map $\mathrm{rk} : \mathscr{D}Y^* \longrightarrow \mathbb{N}_0 \times \{1,...,N\} \times \mathbb{N}_0^K \times \mathbb{N}$ defined by

[1] Observe that by definition, the monomial Y_1 does **not** occur in the polynomial Y_1^2. However, the variable Y_1 does occur in the polynomial Y_1^2.

$$\boxed{\mathrm{rk}((\theta Y_n)^p) := (\mathrm{rk}\,\theta Y_n, p),}$$

where the set

$$\boxed{W := \mathbb{N}_0 \times \{1, ..., N\} \times \mathbb{N}_0^K \times \mathbb{N}}$$

is ordered lexicographically. Hence W is well ordered and

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

Observe that the rank on $\mathscr{D}Y^*$ is again injective, but its image is not longer of order type ω.

1.4. **Order of a variable** We define

$$\mathrm{ord}((\partial_1^{i_1} ... \partial_K^{i_K} Y_n)^p) := \mathrm{ord}(\partial_1^{i_1} ... \partial_K^{i_K}) := i_1 + ... + i_K$$

and

$$\mathrm{ord}_k((\partial_1^{i_1} ... \partial_K^{i_K} Y_n)^p) := \mathrm{ord}_k(\partial_1^{i_1} ... \partial_K^{i_K}) := i_k.$$

1.5. **Leader, leading degree and rank of a differential polynomial** If $f \in A \setminus R$ we define the **leader** (or **conductor**) u_f of f to be the variable $\theta Y_n \in \mathscr{D}Y$ of highest rank that appears in f. Moreover we define

$$\boxed{u_f^* := u_f^{\deg_{u_f} f}}$$

The natural number $\deg_{u_f} f$ is called the **leading degree** of f and is denoted by

$$Ldeg(f) := \deg_{u_f} f.$$

We expand the rank from $\mathscr{D}Y^*$ to polynomials $f \in A \setminus R$ by

$$\boxed{rk(f) := \mathrm{rk}(u_f^*).}$$

So rk is a map $A \setminus R \longrightarrow W$.

1.6. **Definition.** If $f, g \in A \setminus R$, then f is called **weakly reduced** with respect to g if no *proper* derivative of u_g appears in f. Furthermore, f is called **reduced** with respect to g if f is weakly reduced with respect to g and if $\deg_{u_g} f < \deg_{u_g} g$. So by definition f is reduced with respect to g if and only if f is reduced with respect to u_g^*, i.e. the relation 'f is reduced with respect to g' only depends on $\mathrm{rk}\, g$ for given f. An element $f \in R$ is reduced and weakly reduced with respect to every $g \in A \setminus R$ by definition.

Note that if $f \in A \setminus R$ is reduced with respect to $g \in A \setminus R$, then the rank of f need not be less than the rank of g. Take $f = y_1''$ and $g = y_2'$.

1.7. **Lemma.** *Let $f \in A$ and $g \in A \setminus R$. Then*

(i) If $f \notin R$ is reduced with respect to g, then $\mathrm{rk}\, f \neq \mathrm{rk}\, g$.
(ii) Let $f \in R$ or $\mathrm{rk}\, f < \mathrm{rk}\, g$. Then
   (a) f is reduced with respect to g.
   (b) If u_g appears in f, then $u_f = u_g$.
   (c) If g is reduced with respect to f then u_g does not appear in f.

Proof. Certainly (i) holds.

(ii). We may assume that $f \notin R$. Suppose $\operatorname{rk} f < \operatorname{rk} g$, hence $\operatorname{rk} u_f^* < \operatorname{rk} u_g^*$ and $\operatorname{rk} u_f \leq \operatorname{rk} u_g$.

f is weakly reduced with respect to g, since every proper derivative of u_g has a rank bigger than $\operatorname{rk} u_g^* = \operatorname{rk} g$. So if u_g does not appear in f, then f is reduced with respect to g. If u_g appears in f, then $\operatorname{rk} u_f \leq \operatorname{rk} u_g$ implies $u_f = u_g$ and $\operatorname{rk} u_f^* < \operatorname{rk} u_g^*$ implies $\deg_{u_g} f < \deg_{u_g} g$. Hence f is reduced with respect to g and g is not reduced with respect to f. □

1.8**. Definition of (auto)-reduced sets** An element $f \in A$ is called **reduced** with respect to a set $G \subseteq A \setminus R$, if f is reduced with respect to g for each $g \in G$. A subset $G \subseteq A \setminus R$ is called **reduced** or **autoreduced** if for all $f, g \in G$ with $f \neq g$ we have that f is reduced with respect to g. If G has a single element, then G is called reduced as well.

1.9. **Lemma.** *If $\theta_1, \theta_2, ... \in \mathscr{D}$ and $\operatorname{ord} \theta_1 < \operatorname{ord} \theta_2 < ...$, then there is a subsequence $\theta_{k_1}, \theta_{k_2}, ...$ of $\theta_1, \theta_2, ...$ such that $\theta_{k_{i+1}}$ is a proper derivative of θ_{k_i} for every $i \in \mathbb{N}$.*

Proof. The claim certainly holds if $K = 1$. Assume we know (i) in the case of $K - 1$ partial derivatives. Let $\theta_i = \partial_1^{\mu_1^i} .... \partial_K^{\mu_K^i}$. Suppose first that there is some $k \in \{1, ..., K\}$ such that the sequence $(\mu_k^i)_i$ is bounded. Then we also may assume that it is constant by taking a subsequence of (θ_i) if necessary. But then we can apply the inductive hypothesis to the sequence $(\partial_1^{\mu_1^i} .... \partial_{k-1}^{\mu_{k-1}^i} \partial_{k+1}^{\mu_{k+1}^i} ... \partial_K^{\mu_K^i})_i$, which in turn gives the assertion for the original sequence $(\theta_i)_i$.

So we may assume that $(\mu_k^i)_i$ is unbounded for every $k \in \{1, ..., K\}$, i.e. - by taking a subsequence of (θ_i) if necessary - we may assume that $(\mu_k^i)_i$ is strictly increasing for every $k \in \{1, ..., K\}$.

But in this case, for every $i \in \mathbb{N}$ there is some $\theta \in \mathscr{D}$ with $\theta_{i+1} = \theta\theta_i$. □

1.10. **Proposition.** *Every reduced set is finite.*

Proof. If there is an infinite reduced set, then by 1.7(i) there is a chain $\operatorname{rk} g_1 < \operatorname{rk} g_2 < ...$ and g_i is reduced with respect to g_j for all $i \neq j$. Then $u_{g_i} \neq u_{g_j}$ for all $i \neq j$. It follows that u_{g_i} is reduced with respect to u_{g_j} for all $i \neq j$ and we may assume that $g_i = u_{g_i}$.

As g_i is not a derivative of g_j for all $i \neq j$ may assume that $g_i = \theta_i Y_1$ for some $\theta_i \in \mathscr{D}$ and all $i \in \mathbb{N}$. Since $(\operatorname{rk} \theta_i Y_1)$ is strictly increasing, it follows that after taking a subsequence, the sequence $(\operatorname{ord} \theta_i Y_1)_i$ is strictly increasing, too. But this contradicts 1.9, since $\{\theta_j Y_1 \mid j \in \mathbb{N}\}$ is (weakly) reduced by assumption. □

1.11**. Definition of the rank of a reduced set** Let ∞ be an element, which is bigger than W. We consider $(W \cup \{\infty\})^{\mathbb{N}}$ as an ordered set, equipped with the lexicographic order. If $G \subseteq A \setminus R$ is reduced, then G is finite by 1.10 and by 1.7(i), there is a unique enumeration $(g_1, ..., g_l)$ of G, such that $\operatorname{rk} g_1 < ... < \operatorname{rk} g_l$ and $l \in \mathbb{N}$ (Note that $l \leq N$ if $K = 1$). We define $\operatorname{rk} G \in (W \cup \{\infty\})^{\mathbb{N}}$ by

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

If $f \in A \setminus R$, then we want to write $\operatorname{rk} f = \operatorname{rk}\{f\}$, thus we identify $W \cup \{\infty\}$ with $(W \cup \{\infty\}) \times \prod_{i>1} \{\infty\} \subseteq (W \cup \{\infty\})^{\mathbb{N}}$ if necessary.

1.12. **Theorem.** *There is no infinite sequence $G_1, G_2, ...$ of reduced sets with the property $\operatorname{rk} G_1 > \operatorname{rk} G_2 > ....$*

Proof. Otherwise let $G_i := \{g_{i1}, ..., g_{ik_i}\}$ with $\operatorname{rk} g_{i1} < ... < g_{ik_i}$. As $\operatorname{rk} G_1 > \operatorname{rk} G_2 > ...$ we must have $\operatorname{rk} g_{11} \geq \operatorname{rk} g_{21} \geq ...$ and the sequence $(\operatorname{rk} g_{i1})_i$ is eventually constant. Let $M_1 \in \mathbb{N}$ be an index such that $\operatorname{rk} g_{i1} = \operatorname{rk} g_{M_1 1}$ for all $i \geq M_1 - 1$.

As $\operatorname{rk} G_1 > \operatorname{rk} G_2 > ...$ we must have $k_i > 1$ for all $i \geq M_1$. Consequently $\infty > \operatorname{rk} g_{M_1 2} \geq \operatorname{rk} g_{(M_1+1)2} \geq ...$ and the sequence $(\operatorname{rk} g_{(M_1+i)2})_i$ is eventually constant. Let $M_2 > M_1$ be an index such that $\operatorname{rk} g_{i2} = \operatorname{rk} g_{M_2 2}$ for all $i \geq M_2 - 1$. Then $k_i > 2$ for all $i \geq M_2$.

Proceeding in this way we get a new sequence $(G_{M_i})_i$ which we denote by $(G_i)_i$ again. $(G_i)_i$ has the following property: $k_i \geq i$ and $\operatorname{rk} g_{ii} = \operatorname{rk} g_{ji}$ for all $j \geq i$. If $j > i$, then g_{jj} is reduced with respect to g_{ji}, since G_j is a reduced set. As $\operatorname{rk} g_{ji} = \operatorname{rk} g_{ii}$ it follows that g_{jj} is reduced with respect to g_{ii}. Conversely since $\operatorname{rk} g_{ii} = \operatorname{rk} g_{ji} < \operatorname{rk} g_{jj}$, it follows that g_{ii} is reduced with respect to g_{jj}. Hence $\{g_{ii}, g_{jj}\}$ is a reduced set for all $i < j$ and the set of diagonal entries $\{g_{ii} \mid i \in \mathbb{N}\}$ is an infinite reduced set. This contradicts 1.10. □

2. Characteristic sets

By 1.12 we may define:

2.1. **Definition.** For each subset M of A, $M \not\subseteq R$ we define

$$\operatorname{rk} M := \min\{\operatorname{rk} G \mid G \subseteq M \setminus R,\ G \text{ reduced}\} \in (W \cup \{\infty\})^{\mathbb{N}}.$$

A **characteristic set** of M is a reduced subset S of M with $\operatorname{rk} M = \operatorname{rk} S$.

2.2. **Lemma.** *If $G \subseteq A \setminus R$ is a reduced set and $f \in A \setminus R$ is reduced with respect to G, then $\tilde{G} := \{g \in G \mid \operatorname{rk} g < \operatorname{rk} f\} \cup \{f\}$ is a reduced set and $\operatorname{rk} \tilde{G} < \operatorname{rk} G$.*

Proof. By 1.7(ii), the set $\tilde{G}$ is reduced. Since f is reduced with respect to G, 1.7(i) implies that $\operatorname{rk} f \neq \operatorname{rk} g$ for all $g \in G$, thus $\operatorname{rk} \tilde{G} < \operatorname{rk} G$. □

2.3. **Corollary.** *If S is a characteristic set of $M \subseteq A$ and $f \in M \setminus R$, then f is not reduced with respect to S*

Proof. Immediately from 2.2. □

2.4. **Definition.** The leading coefficient of $f \in A \setminus R$ is defined as follows:
Let $u_f = \theta Y_n$, let $B := R[\tilde{\theta} Y_m \mid \tilde{\theta} Y_m \neq \theta Y_n]$ and let $f = f_d \cdot u_f^d + ... + f_1 \cdot u_f + f_0$, with $f_d, ..., f_0 \in B$, $f_d \neq 0$. Then f_d is called the **leading coefficient** $L(f)$ of f.

Observe that $\operatorname{rk} L(f) < \operatorname{rk} u_f$. Moreover if f is (weakly) reduced with respect to g then $L(f)$ is (weakly) reduced with respect to g. But in general $L(f)^m$ is not reduced with respect to g if f is reduced with respect to g.

2.5. **Lemma.** *Let R be a domain. Let $G \subseteq A \setminus R$ be a reduced set, $G = \{g_1, ..., g_l\}$ with $\operatorname{rk} g_1 < ... < \operatorname{rk} g_l$. Let $h \in A$ be weakly reduced with respect to G and suppose there is given some $i \in \{1, ..., l\}$ such that h is reduced with respect to $\{g_{i+1}, ..., g_l\}$. Then there are $q, r \in A$ and some $k \in \mathbb{N}_0$ such that*

(a) $L(g_i)^k \cdot h = q \cdot g_i + r$ *and*
(b) *r is weakly reduced with respect to G and reduced with respect to $\{g_i, ..., g_l\}$.*
(c) $\operatorname{rk} u_r \leq \max\{\operatorname{rk} u_h, \operatorname{rk} u_{g_i}\}$ *and* $k = \deg_{u_{g_i}} h - \deg u_{g_i} g_i + 1$ *if h is not reduced with respect to g_i.*

Proof. We may assume that h is not reduced with respect to g_i. Let

$$A_0 := R[\theta Y_n \mid \theta Y_n \textit{ appears in } h \textit{ or in } g_i,\ \theta Y_n \neq u_{g_i}].$$

Then $h, g_i \in A_0[u_{g_i}]$ and we can apply the division theorem for the ring $A_0[u_{g_i}]$. Hence, there are $q, r \in A_0[u_{g_i}]$ with $L(g_i)^k \cdot h = q \cdot g_i + r$, $k = \deg_{u_{g_i}} h - \deg u_{g_i} g_i + 1$ such that $\deg_{u_{g_i}} r < \deg_{u_{g_i}} g_i$. Furthermore the uniqueness statement of the division theorem applied to A instead of $A_0[u_{g_i}]$ says: if $q^*, r^* \in A$ with $L(g_i)^k \cdot h = q^* \cdot g_i + r^*$ and $\deg_{u_{g_i}} r^* < \deg_{u_{g_i}} g_i$, then $q = q^*$ and $r = r^*$.

Since $r \in A_0[u_{g_i}]$ we know that $\operatorname{rk} u_r \leq \operatorname{rk} h$ or $\operatorname{rk} u_r \leq \operatorname{rk} u_{g_i}$ and since h and g_i are weakly reduced with respect to G we have that r is weakly reduced with respect to G as well. By the choice of r we know that r is reduced with respect to g_i and it remains to show that r is reduced with respect to g_j for each $j \in \{i+1, ..., l\}$.

Let z be the conductor of g_j and let $d := \deg_z g_j$. Since r is weakly reduced with respect to g_j it is enough to prove $\deg_z r < d$.

Since g_j is reduced with respect to g_i and $\operatorname{rk} g_i < \operatorname{rk} g_j$ the variable z does not appear in g_i (1.7(ii)(c)). Consequently z does not appear in $L(g_i)$. Let

$$\tilde{A} := R[\theta Y_n \mid \theta Y_n \in \mathscr{D}Y, \theta Y_n \neq z].$$

Since h is reduced with respect to g_j, there are $h_0, ..., h_{d-1} \in \tilde{A}$, such that $h = h_{d-1} z^{d-1} + ... + h_1 z + h_0$. Let $q_\beta, r_\beta \in \tilde{A}$ $(\beta \geq 0)$ such that $q = q_0 + q_1 z + q_2 z^2 + ...$ and $r = r_0 + r_1 z + r_2 z^2 + ...$ Now we have the polynomial equality

$$L(g_i)^k h_{d-1} \cdot z^{d-1} + ... + L(g_i)^k h_1 \cdot z + L(g_i)^k h_0 =$$

$$= (g_i q_0 + r_0) + (g_i q_1 + r_1) \cdot z + (g_i q_2 + r_2) z^2 + ...$$

in the variable z, where all coefficients are in $\tilde{A}$. Consequently $g_i q_\beta + r_\beta = 0$ for $\beta \geq d$. With $q^* := q_0 + q_1 z + ... + q_{d-1} z^{d-1}$ and $r^* := r_0 + r_1 z + ... + r_{d-1} z^{d-1}$ we found a decomposition $L(g_i)^k \cdot h = q^* \cdot g_i + r^*$ such that $\deg_{u_{g_i}} r^* < \deg_{u_{g_i}} g_i$ and $\deg_z r^* < d$. From the uniqueness statement of the division theorem we get $r = r^*$, thus $\deg_z r < d$. □

2.6. *Remark.* In the situation of 2.5 the polynomial $L(g_i)^m \cdot r$ is weakly reduced with respect to G and reduced with respect to $\{g_i, ..., g_l\}$ for all $m \in \mathbb{N}_0$. Hence we may increase the power k if we want.

2.7. **Definition.** If G is a finite subset of $A \setminus R$ we define $L_G := \{\prod_{g \in G} L(g)^{i_g} \mid i_g \in \mathbb{N}_0 \text{ for } g \in G\}$ and $L(G) := \prod_{g \in G} L(g)$.

If G is a reduced set then every $L \in L_G$ is weakly reduced with respect to every $g \in G$ but L need not be reduced with respect to G. For example if $G = \{Y_1^3, Y_1^2 Y_2, Y_1^2 Y_3\}$.

2.8. **Definition.** If $G \subseteq A$ and $y \in \mathscr{D}Y$ we define

$$G_{\leq y} = \{\theta g \mid g \in G,\ \theta \in \mathscr{D} \text{ and } \operatorname{rk}(\theta u_g) \leq \operatorname{rk}(y)\}$$
$$G_{<y} = \{\theta g \mid g \in G,\ \theta \in \mathscr{D} \text{ and } \operatorname{rk}(\theta u_g) < \operatorname{rk}(y)\}$$

Note that in general G is not a subset of $G_{\leq y}$, even if y is a proper derivative of some u_g, $g \in G$. Clearly $G_{<y} = \bigcup \{G_{\leq z} \mid \operatorname{rk} z < \operatorname{rk} y\}$.

At the moment we only work with the set $G \cap G_{\leq y} = \{g \in G \mid \operatorname{rk} u_g \leq \operatorname{rk} y\}$.

2.9. **Proposition.** *Let R be a domain. Let $G \subseteq A \setminus R$ be a reduced set. If $f \in A$ is weakly reduced with respect to G, then there is some $\tilde{f} \in A$, which is reduced with respect to G and some $L \in L_G$, such that $L \cdot f \equiv \tilde{f} \bmod (G \cap G_{\leq u_f})$. In particular $\tilde{f} \in (G \cap G_{\leq u_f}) + f \cdot A$.*

Proof. Let $G = \{g_1, ..., g_l, g_{l+1}, ..., g_m\}$ with $\operatorname{rk} g_1 < ... < \operatorname{rk} g_m$ and $\operatorname{rk} u_{g_l} \leq \operatorname{rk} u_f < \operatorname{rk} u_{g_{l+1}}$ (note that $l = m$ is not excluded; also, in the case $\operatorname{rk} u_f < \operatorname{rk} u_{g_1}$ there is nothing to do). We construct $f_l, ..., f_1, f_0 \in A$ taking $f_l := f$ with the following properties:

(1) If $i \in \{1, ..., l\}$, then g_i divides $L(g_i)^{k_i} f_i - f_{i-1}$ for some $k_i \in \mathbb{N}$.
(2) f_i is weakly reduced with respect to G for $i \in \{0, ..., l\}$.
(3) f_i is reduced with respect to $\{g_{i+1}, ..., g_m\}$ for $i \in \{0, ..., l-1\}$.

Firstly $f_l = f$ is weakly reduced with respect to G by assumption and reduced with respect to $\{g_{l+1}, ..., g_m\}$ as $\operatorname{rk} u_f < \operatorname{rk} u_{g_{l+1}}$. Thus (2) and (3) hold for f_l. Suppose we have already constructed the f_j, $i \leq j \leq l$, with $i \in \{1, ..., l\}$, such that (2) and (3) holds for $j \geq i$ and (1) holds for $j > i$. We apply 2.5 with $h = f_i$ (note that $f_i \in R$ is allowed here). We get some $k_i \in \mathbb{N}_0$ and f_{i-1} (the remainder polynomial r from 2.5) such that g_i divides $L(g_i)^{k_i} f_i - f_{i-1}$, such that f_{i-1} is weakly reduced with respect to G and reduced with respect to $\{g_i, ..., g_l\}$. Hence property (1) holds for i and properties (2),(3) hold for $i-1$. This gives the construction. Note that in the case $f_i = 0$ we have $f_j = 0$ for each $j \leq i$.

If we take $\tilde{f} := f_0$, then condition (1) implies that $L \cdot f \equiv \tilde{f} \bmod (\{g_1, ..., g_l\})$ for some $L \in L_G$. By condition (3) we have that $\tilde{f} = f_0$ is reduced with respect to G. □

2.10. **Definition.** If Z is a subset of A and $1 \in H \subseteq A$ is multiplicatively closed we define

$$Sat_H(Z) := \{f \in A \mid h \cdot f \in Z \text{ for some } h \in H\}.$$

If $h \in A$ then

$$Sat_h(Z) := Sat_{\{1, h, h^2, ...\}}(Z).$$

2.11. **Corollary.** *Let R be a domain. Let $0 \neq \mathfrak{a} \subseteq A$ be an ideal and let $G \subseteq \mathfrak{a} \setminus R$ be a characteristic set of $\mathfrak{a}$. If $f \in \mathfrak{a}$ is weakly reduced with respect to G, then*

$$f \in Sat_{L_G}(\mathfrak{a} \cap R + (G \cap G_{\leq u_f})).$$

If $\mathfrak{a} \cap R = 0$ then

$$f \in Sat_{L(G)}((G \cap G_{\leq u_f})) = Sat_{L_G}((G \cap G_{\leq u_f})).$$

Proof. Take $\tilde{f}$ as in 2.9. Since $f \in \mathfrak{a}$ we get $\tilde{f} \in \mathfrak{a}$ from $\tilde{f} \in (G) + f \cdot A$. Since $\tilde{f}$ is reduced with respect to G this is only possible if $\tilde{f} \in R$ (by 2.3). □

2.12. *Remark.* If $\mathfrak{a}$ is an ideal of A with $\mathfrak{a} \cap R = 0$ and G is a characteristic set of $\mathfrak{a}$, then $L(g) \neq 0$ is reduced with respect to G for every $g \in G$, hence $L(g) \notin \mathfrak{a}$ by 2.3. Thus if $\mathfrak{a}$ is prime in addition, then $Sat_{L_G}((G)) \subseteq \mathfrak{a}$.

2.13. *Example.* Without the assumption $\mathfrak{a} \cap R = 0$ we need not have $Sat_{L_G}((G)) \subseteq \mathfrak{a}$ - even if $\mathfrak{a}$ is prime. The reason is that $L(g)$ might be a member of $\mathfrak{a}$ - more precisely of $\mathfrak{a} \cap R$ for some $g \in G$.

To see an example let R_0 be a factorial $\mathbb{Q}$-algebra, let t be an ordinary indeterminate over R_0 and let $R := R_0[t]$ together with derivations $\partial_1, ..., \partial_K$, such that $\partial_i t \in t \cdot R$ (e.g. if all derivatives are trivial). Let Y be a single differential indeterminate, $A := R\{Y\}$ and let $\mathfrak{a} := t \cdot A$ be the ideal generated by t in A. Since $\partial_i t \in t \cdot R$ it follows that $\mathfrak{a}$ is a differential prime ideal. Moreover a set $G \subseteq A$ is a characteristic set of $\mathfrak{a}$ if and only if $G = \{t \cdot (h_1 \cdot Y + h_0)\}$ for some $h_1, h_0 \in R$, $h_1 \neq 0$. Now if we take $h_1 = 1$ and $h_0 = 0$ then $Y \in Sat_{L_G}((G))$, since $t \cdot Y \in (G)$ and $t = L(t \cdot Y)$. But $Y \notin \mathfrak{a}$.

Moreover this example shows that in general there is no characteristic set G of $\mathfrak{a}$ such that $Sat_{L_G}(\mathfrak{a} \cap R + (G)) \subseteq \mathfrak{a}$ - even if $\mathfrak{a}$ is prime. This is so, since for arbitrary $h_1, h_0 \in R, h_1 \neq 0$ we have $Sat_{L_G}(\mathfrak{a} \cap R + (G)) = A$, as $t \cdot h_1 \cdot 1 \in \mathfrak{a} \cap R$.

2.14. *Example.* Let R be an arbitrary differential domain in K derivations, $\mathbb{Z} \subseteq R$ and let $A := R\{Y\}$ be the differential polynomial ring over R in the single variable Y. If $\mathfrak{a} \subseteq A$ is an ideal and $r \in R \cap \mathfrak{a}$, $r \neq 0$, then $\{r \cdot Y\}$ is a characteristic subset of $\mathfrak{a}$. Hence every characteristic subset of $\mathfrak{a}$ is of the form $\{r_1 Y + r_0\}$ with some $r_1, r_0 \in R$, $r_1 \neq 0$.

2.15. **Proposition.** *Let R be a field and let G be a characteristic set of an ideal $\mathfrak{a} \subseteq A$ with $\mathfrak{a} \neq (0)$ and $\mathfrak{a} \cap R = (0)$.*

(i) If $\mathfrak{a}$ is a radical ideal then no $g \in G$ is a proper power of another polynomial from A.

(ii) If $\mathfrak{a}$ is a prime ideal, then for each $g \in G$ there is a unique irreducible factor g_0 of g with $g_0 \in \mathfrak{a}$. The set $\{g_0 \mid g \in G\}$ of all these factors is a characteristic set of $\mathfrak{p}$. Moreover if $h \in A$ with $g = g_0 \cdot h$, then $h \in R$ or h is reduced with respect to G and $\operatorname{rk} h < \operatorname{rk} u_g$.

Proof. (i). Suppose $h^d = g \in G$. Then $h \in \mathfrak{a}$, so h is not reduced with respect to G. Since h divides g, h is reduced with respect to every $\tilde{g} \in G \setminus \{g\}$ by 2.3. It follows that h is not reduced with respect to g, thus $h = g$.

(ii). Fix some $g \in G$. Let g_0 be an irreducible factor of g with $g_0 \in \mathfrak{a}$. Since G is reduced, g_0 is reduced with respect to each $\tilde{g} \in G \setminus \{g\}$. By 2.3 g_0 is not reduced with respect to g. Since g_0 divides g we must have $u^*_{g_0} = u^*_g$, hence $\operatorname{rk} g_0 = \operatorname{rk} g$. This proves that u_g must not appear in any other irreducible factor of g and $g = g_0 \cdot h$ implies $\operatorname{rk} h < \operatorname{rk} u_g$. Since h divides g, it is reduced with respect to every $\tilde{g} \in G \setminus \{g\}$.

Since $u^*_{g_0} = u^*_g$ and g_0 divides g ($g \in G$), the set $\{g_0 \mid g \in G\} \subseteq \mathfrak{a}$ is a reduced subset of $\mathfrak{a}$. As $\operatorname{rk} g_0 = \operatorname{rk} g$ ($g \in G$) this set is even a characteristic set of $\mathfrak{a}$. □

3. The Separant

From now on we assume that R has characteristic 0.

By convention every $f \in A$ is a derivative of itself (namely the 0th derivative). Again, we say that a variable $z \in \mathscr{D}Y$ appears in $f \in A$ if the degree of the polynomial f in the variable z is non zero. So z appears in a derivative of z but z does not appear in any proper derivative of z.

If $\mathrm{rk}\,\theta < \mathrm{rk}\,E$ with $\theta, E \in \mathscr{D}$ then E need not be a derivative of θ unless there is only one derivative. This is the main difficulty in the reduction process of the order. We begin with a fairly obvious but useful

3.1. **Observation.** *If $z_1, ..., z_l \in \mathscr{D}Y$ and $\theta \in \mathscr{D}$, then*

$$\theta(R[z_1, ..., z_l]) \subseteq R[Ez_1, ..., Ez_l \mid E \in \mathscr{D} \text{ and there is some } \tilde{E} \in \mathscr{D} \text{ with } \tilde{E}E = \theta]$$

Hence if $f \in A$, then by choosing the z_i as the list of all the variables in $\mathscr{D}Y$ that appear in f, we get the following:

If $z \in \mathscr{D}Y$ appears in θf (so z is one of the Ez_i), then there is a variable $y \in \mathscr{D}Y$ appearing in f (namely z_i) such that z is a derivative of y, and θy $(= \theta z_i = \tilde{E}Ez_i = \tilde{E}z)$ is a derivative of z.

Proof. This is a consequence of the Leibniz rule on the derivative of products. □

3.2. **Definition.** The separant of $f \in A \setminus R$ is defined as follows:
Let $u_f = \theta Y_n$, let $B := R[\tilde{\theta}Y_m \mid \tilde{\theta}Y_m \neq \theta Y_n]$ and let $f = f_d \cdot u_f^d + ... + f_1 \cdot u_f + f_0$, with $f_d, ..., f_0 \in B$, $f_d \neq 0$. The **separant** $S(f)$ is

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

Moreover if $\theta \in \mathscr{D}$ is of order > 0 we define

$$[\theta]f := \theta f - S(f)\theta u_f.$$

If $\theta = \partial_1^0 ... \partial_k^0$ we define $[\theta]f := f$. An alternative notation is $f^\theta = [\theta]f$.

3.3. **Lemma.** *Let $\theta \in \mathscr{D}$, $z \in \mathscr{D}Y$, $k \in \{1, ..., K\}$ and $f \in A \setminus R$.*

(i) If $f = f_d u_f^d + ... + f_1 u_f + f_0$, where u_f does not appear in any f_i, then

$$[\partial_k]f = (\partial_k f_d)u_f^d + ... + (\partial_k f_1)u_f + \partial_k f_0.$$

(ii) θu_f is the leader of θf and $S(f) = S(\theta f) \neq 0$.
(iii) If $\mathrm{ord}\,\theta > 0$ then $S(f) = L(\theta f)$ and $Ldeg(f) = 1$.
(iv) $[\partial_k \theta]f = [\partial_k]\theta f$.
(v) If $\mathrm{ord}\,\theta > 0$ and $[\theta]f \notin R$ then $\mathrm{rk}[\theta]f < \mathrm{rk}\,\theta u_f$.

Proof. (i) follows immediately from the product rule for the derivative.

For the remaining parts we use

Claim. If $[\partial_k]f \notin R$ then $\mathrm{rk}[\partial_k]f < \mathrm{rk}\,\partial_k u_f$.
Proof. Look at the representation of $[\partial_k]f$ from (i). It is enough to show that $\mathrm{rk}\,\partial_k f_i$ has rank $< \mathrm{rk}\,\partial_k u_f$. Let $z \in \mathscr{D}Y$ be a variable which appears in $\mathrm{rk}\,\partial_k f_i$. By 3.1, there is a variable $y \in \mathscr{D}Y$ which appears in f_i, such that z is a derivative of y and such that $\partial_k y$ is a derivative of z. Hence $z = y$ or $z = \partial_k y$. As y appears in f_i we have $\mathrm{rk}\,y < \mathrm{rk}\,u_f$, thus $\mathrm{rk}\,z < \mathrm{rk}\,\partial_k u_f$ and the claim is proved. ⋄

(ii) and (iii). Clearly every variable $y \in \mathscr{D}Y$ which appears in $S(f)$ has rank $< \operatorname{rk} \partial_k u_f$. So the claim implies that $\partial_k u_f$ is the conductor of $\partial_k f$, as well as $S(\partial_k f) = S(f) = L(\partial_k f)$. By a trivial induction we get (ii) and (iii).

(iv) holds if $\operatorname{ord} \theta = 0$. If $\operatorname{ord} \theta > 0$ then $[\partial_k]\theta f = \partial_k \theta f - S(\theta f)\partial_k u_{\theta f} = \partial_k \theta f - S(f)\partial_k \theta u_f$ by (ii) and (iii), so $[\partial_k]\theta f = [\partial_k \theta] f$.

(v). As $\operatorname{ord} \theta > 0$ we may assume that $\theta = \partial_k E$ for some $E \in \mathscr{D}$. Hence $\operatorname{rk}[\theta]f = [\partial_k]Ef < \operatorname{rk} \partial_k u_{Ef}$ by (iv) and the claim. Hence (ii) implies $\operatorname{rk}[\theta]f < \operatorname{rk} \partial_k E u_f = \operatorname{rk} \theta u_f$. □

3.4. *Example.* Clearly $\theta u_f = u_{\theta f}$. However, neither is θu_f a derivative of the leader of $[\theta]f$ nor is the leader of $[\theta]f$ a derivative of u_f in general. For example if $f = \partial_1 Y \partial_2 Y$ and $\theta = \partial_3$. Then $u_f = \partial_2 Y$, $u_{\partial_3 f} = \partial_3 \partial_2 Y$ and $u_{[\partial_3]f} = \partial_3 \partial_1 Y$.

4. Reduction of the order

By 3.3(v) we have

$$\theta f = S(f)\theta u_f + [\theta]f \text{ and } \operatorname{rk}[\theta]f < \operatorname{rk} \theta u_f.$$

This is the core step for the reduction of the order if $\operatorname{ord} D > 0$. It means that $S(f)\theta u_f$ can be reduced to a polynomial (namely $-[\theta]f$) of smaller rank modulo the differential ideal $[f]$.

4.1. **Definition.** If $G \subseteq A \setminus R$ is finite then the **separant** of G is the polynomial

$$S(G) := \prod_{g \in G} S(g)$$

Moreover we define $S_G := \{\prod_{i=1}^n S(g_i) \mid n \in \mathbb{N}, g_i \in G\}$.

Observe that $S(G) \neq 0$, as $\operatorname{char} R = 0$ and R is a domain. Moreover if G is a reduced set, then $S(G)^d$ is weakly reduced with respect to G for all $d \in \mathbb{N}_0$. $S(G)$ need not be reduced with respect to G, for example $G = \{Y_1^2, Y_1 Y_2\}$ has separant $S(G) = 2Y_1^2$.

In what follows we fix a reduced set $G \subseteq A$. If $f \in A$ is not weakly reduced with respect to G we define

$$r_G(f) := \max\{rk(y) \mid y \in \mathscr{D}Y \text{ appears in } f \text{ and } y \text{ is a } \texttt{proper} \text{ derivative of some } u_g, g \in G\}$$

Observe for $g \in G$ such that u_g appears in f we need not have $\operatorname{rk}(u_g) \leq r_G(f)$. Therefore the next lemma is not true if we would define $r_G(f)$ as
$\max\{\operatorname{rk}(y) \mid y \in \mathscr{D}Y$ appears in f and y is a derivative of some $u_g, g \in G\}$

4.2. **Lemma.** *Let $f \in A \setminus R$ and let G be a reduced set. Let $y \in \mathscr{D}Y$ be a variable which appears in f and suppose for some $g \in G$, $\theta \in \mathscr{D}$, $\operatorname{ord} D > 0$ we have $y = \theta u_g$ (observe that g is not uniquely determined by this demand, even if $\operatorname{rk}(y) = r_G(f)$). Let $f = f_d y^d + f_{d-1} y^{d-1} + ... + f_0$, where y does not appear in f_j, $f_d \neq 0$. Furthermore let*

$$h = \sum_{\alpha=0}^{d} f_\alpha \cdot S(g)^{d-\alpha} \cdot (-[\theta]g)^\alpha.$$

Then

$$S(g)^d f \equiv h \bmod (\theta g)$$

and either h *is weakly reduced with respect to* G *or* $r_G(h) \leq r_G(f)$*. Moreover* $\mathrm{rk}(S(g)^\alpha \cdot h) \leq \mathrm{rk}(f)$ *for all* $\alpha \in \mathbb{N}_0$ *and if* $\mathrm{rk}(y) = r_G(f)$ *then* $r_G(h) < r_G(f)$*.*

Proof. The plan is to replace $y = \theta u_g$ in f by $\frac{1}{S(g)}(\theta g - [\theta]g)$. After multiplying the resulting expression with a suitable power of $S(g)$ we subtract a multiple of θg in A to get h.

Since $y = \theta u_g$, we have

$$S(g)^d f = f_d \cdot (S(g)\theta u_g)^d + f_{d-1} S(g)(S(g)\theta u_g)^{d-1} + ... + f_0 S(g)^d.$$

Since $S(g)\theta u_g = \theta g - [\theta]g$ we may replace $S(g)\theta u_g$ by $\theta g - [\theta]g$ in this equation and get

$$S(g)^d f = f_d \cdot (\theta g - [\theta]g)^d + f_{d-1} S(g)(\theta g - [\theta]g)^{d-1} + ... + f_0 S(g)^d,$$

which proves $S(g)^d f - h \in (\theta g)$.

Now suppose h is not weakly reduced with respect to G. Let $z \in \mathscr{D}Y$, suppose z appears in h and z is a proper derivative of $u_{\tilde{g}}$ for some $\tilde{g} \in G$. If z appears in $S(g)$, then $\mathrm{rk}\, z \leq \mathrm{rk}\, u_g < \mathrm{rk}\, \theta u_g = \mathrm{rk}\, y \leq r_G(f)$. If z appears in $[\theta]g$ then $\mathrm{rk}\, z \leq \mathrm{rk}[\theta]g < \mathrm{rk}\, \theta u_g = \mathrm{rk}\, y \leq r_G(f)$ by 3.3(v). If z appears in f_α for some $\alpha \in \{0, .., d\}$ then $\mathrm{rk}\, z \leq r_G(f)$ by the definition of $r_G(f)$. If $\mathrm{rk}\, y = r_G(f)$ and z appears in f_α for some $\alpha \in \{0, .., d\}$ then $\mathrm{rk}\, z < \mathrm{rk}\, y =\leq r_G(f)$ by the definition of $r_G(f)$ and the choice of the f_α's. This shows $r_G(h) \leq r_G(f)$ and $r_G(h) < r_G(f)$ if $\mathrm{rk}\, y = \mathrm{rk}_G(f)$. It remains to prove $\mathrm{rk}\, S(g)^\alpha \cdot h \leq \mathrm{rk}\, f$.

Let $u := u_{S(g)^\alpha \cdot h}$. If u does not appear in $S(g)$ and in $[\theta]g$, then u^* appears in some f_α, hence $\mathrm{rk}\, S(g)^\alpha \cdot h \leq \mathrm{rk}\, f$. If u_h appears in $S(g)$, then $\mathrm{rk}\, u \leq \mathrm{rk}\, g < \mathrm{rk}\, \theta u_g \leq \mathrm{rk}\, f$, so $\mathrm{rk}\, S(g)^\alpha \cdot h < \mathrm{rk}\, f$. If u appears in $[\theta]g$, then $\mathrm{rk}\, u \leq \mathrm{rk}[\theta]g < \mathrm{rk}\, \theta u_g \leq \mathrm{rk}\, f$ (by 3.3), hence $\mathrm{rk}\, S(g)^\alpha \cdot h < \mathrm{rk}\, f$. □

4.3. **Notation** If $f \in A$ is not weakly reduced with respect to G then we define

$$G_{\leq f} := \{\theta g \mid g \in G, \theta \in \mathscr{D} \text{ and } \mathrm{rk}(\theta u_g) \leq r_G(f)\}$$
$$G_{< f} := \{\theta g \mid g \in G, \theta \in \mathscr{D} \text{ and } \mathrm{rk}(\theta u_g) < r_G(f)\}$$

Observe that for $g \in G$ we do not have $g \in G_{\leq f}$ in general, even if u_g appears in f.

Moreover, if $y \in \mathscr{D}Y$ appears in f with $\mathrm{rk}(y) = r_G(f)$, then $G_{\leq f} = G_{\leq y}$ and $G_{<f} = G_{<y}$. (See 2.8 for definitions.)

If f is weakly reduced with respect to G we define $G_{\leq f} := G_{\leq u_f}$ and $G_{<f} := G_{<u_f}$.

4.4. **Corollary.** *Let* $G \subseteq A$ *be a reduced set and let* $f \in A$*. Then there is some* $\tilde{f} \in A$ *which is weakly reduced with respect to* G *and some* $S \in S_G$ *such that* $\mathrm{rk}(\tilde{f}) \leq \mathrm{rk}(f)$ *and*

$$S \cdot f \equiv \tilde{f} \bmod (G_{\leq f}).$$

In particular

$$S \cdot f \equiv \tilde{f} \bmod (G_{\leq u_f}).$$

Proof. If f is weakly reduced with respect to G we may take $\tilde{f} = f$ and $S = 1$. If f is not weakly reduced with respect to G, we apply 4.2 to f and denote the resulting polynomial by f_1. If f_1 is not weakly reduced with respect to G we apply 4.2 to f_1. Ongoing in this way we get a sequence $f = f_0, f_1, f_2, ...$ of polynomials with $r_G(f) > r_G(f_1) > ...$ and $\mathrm{rk}\, f \geq \mathrm{rk}\, f_1 \geq ....$ As such a sequence can not be infinite, some f_m has to be weakly reduced with respect to G. We have $\operatorname{rk} f_m \leq \operatorname{rk} f$ and $S_i \cdot f_i \equiv f_{i+1} \operatorname{mod}(D^i g_i)$ for some $S_i \in S_G$, $\theta^i \in \mathscr{D}$ and $g_i \in G$ with $r_G(f) \geq r_G(f_i) = \operatorname{rk} \theta^i u_{g_i}$. Thus $\theta^i g_i \in G_{\leq f}$ and $S_0 \cdot \ldots \cdot S_{m-1} f \equiv f_m \operatorname{mod}(G_{\leq f})$. So we may take $\tilde{f} = f_m$. □

4.5. **Definition.** If $G \subseteq A$ is finite we define

$$H_G := \{L \cdot S \mid L \in L_G,\ S \in S_G\}$$

and

$$H(G) := L(G) \cdot S(G).$$

We summarize both reduction processes:

4.6. **Theorem.** *Let $G \subseteq A$ be a reduced set and let $f \in A$. Then there is some $\tilde{f} \in A$, which is reduced with respect to G and some $H \in H_G$ such that*

$$H \cdot f \equiv \tilde{f} \operatorname{mod}(G_{\leq u_f}).$$

In particular $H \cdot f \equiv \tilde{f} \operatorname{mod}[G]$.

Proof. By 4.4 there is some $h \in A$, which is weakly reduced with respect to G such that $S \cdot f \equiv h \operatorname{mod}(G_{\leq u_f})$ for some $S \in S_G$ and such that $\operatorname{rk}(h) \leq \operatorname{rk}(f)$. By 2.9 there is some $\tilde{f} \in A$, which is reduced with respect to G and some $L \in L_G$ such that $L \cdot h \equiv \tilde{f} \operatorname{mod}(G \cap G_{\leq u_h})$. As $\operatorname{rk}(h) \leq \operatorname{rk}(f)$ we get $G_{\leq u_h} \subseteq G_{\leq u_f}$, hence $H \cdot f \equiv \tilde{f} \operatorname{mod}(G_{\leq u_f})$ with $H := L \cdot S$. □

4.7. **Corollary.** *Let R be a domain. Let $0 \neq \mathfrak{a} \subseteq A$ be a differential ideal, $\mathfrak{a} \cap R = 0$ and let $G \subseteq \mathfrak{a} \setminus R$ be a characteristic set of $\mathfrak{a}$. Then*

(i)

$$\mathfrak{a} \subseteq Sat_{H_G}[G].$$

(ii) (Coherence of the characteristic set G)
If $g_1, g_2 \in G$, $g_1 \neq g_2$ and $\theta^1, \theta^2 \in \mathscr{D}$ such that $\theta^1 u_{g_1} = \theta^2 u_{g_2} =: y$, then there is some $H \in H_G$ such that

$$H \cdot (S(g_2) \cdot \theta^1 g_1 - S(g_1) \cdot \theta^2 g_2) \in (G_{<y}).$$

(Recall that $G_{<y} := \{\theta g \mid g \in G,\ \theta \in \mathscr{D} \text{ and } \operatorname{rk}(\theta u_g) < \operatorname{rk}(y)\}$.)

(iii) If $\mathfrak{a}$ is prime then

$$\mathfrak{a} = Sat_{H_G}[G].$$

Proof. (i) and (ii). Let $f \in \mathfrak{a}$ and take $\tilde{f}$ and H as in 4.6. Since $f \in \mathfrak{a}$ we get $\tilde{f} \in \mathfrak{a}$ from $\tilde{f} \in [G] + f \cdot A$. Since $\tilde{f}$ is reduced with respect to G this is only possible if $\tilde{f} \in R$ (by 2.3). So $\tilde{f} \in R \cap \mathfrak{a} = 0$ and $H \cdot f \in (G_{\leq u_f})$. In particular $f \in Sat_{H_G}[G]$.

If $f = S(g_2) \cdot \theta^1 g_1 - S(g_1) \cdot \theta^2 g_2$, then $\operatorname{rk}(u_f) < \operatorname{rk}(y)$ and 4.6 shows $H \cdot f \in (G_{<y})$.

(iii). If $\mathfrak{a}$ is a differential prime ideal and $f \in Sat_{H_G}[G]$ then $H \cdot f \in \mathfrak{a}$ for some $H \in H_G$. Since $H \neq 0$ and each leading coefficient and each separant of an element in G is reduced with respect to G we get $H \notin \mathfrak{a}$ from 2.3 again. Hence $f \in \mathfrak{a}$. □

5. Coherence and the Rosenfeld Lemma

We start with a lemma about saturations when passing to polynomial rings

5.1. **Generation of the saturation** *Let B ba a ring and let Y be a set of indeterminates over B. Let $G \subseteq B$ and let $H \subseteq B$ be multiplicatively closed. Let $A := B[Y]$ and let $(G)_B$, $(G)_A$ be the ideal generated by G in B and in A respectively . Let*

$$\mathfrak{b} = \{f \in B \mid h \cdot f \in (G)_B \text{ for some } h \in H\}$$
$$\mathfrak{a} = \{f \in B[Y] \mid h \cdot f \in (G)_A \text{ for some } h \in H\}.$$

Then

(i) The ideal $\mathfrak{a}$ of A is generated by the ideal $\mathfrak{b}$ of B.
(ii) $\mathfrak{a} \cap B = \mathfrak{b}$.
(iii) $\mathfrak{a}$ is radical if and only if $\mathfrak{b}$ is radical and $\mathfrak{a}$ is prime if and only if $\mathfrak{b}$ is prime.

Proof. Clearly (ii) holds and (iii) follows from (i). In order to see (i) we may assume that Y is a finite set of indeterminates. Then the claim follows by induction on the number of variables from the one variable case. So we may assume that $A = B[Y]$ is the polynomial ring over B in one indeterminate Y.

We prove (i) by induction on the degree of $f \in \mathfrak{a}$ in Y. If $\deg f = 0$, then we have $f \in \mathfrak{b}$. Now suppose $f = \hat{f} \cdot Y + r \in \mathfrak{a}$ with $r \in B$ and $\deg \hat{f} < \deg f$. Take $h \in H, f_i \in A$ and $g_i \in G$ with $h \cdot f = \sum f_i \cdot g_i$. Setting $Y = 0$ shows $r \in \mathfrak{b}$, hence we may assume that $r = 0$. Let $f_i = f_i^* Y + r_i$ with $r_i \in B$. Then $h \cdot \hat{f} \cdot Y = \sum_{i \in I} f_i^* g_i \cdot Y + \sum r_i g_i$, so $\sum r_i g_i = 0$ and $h \cdot \hat{f} = \sum_{i \in I} f_i^* g_i$. This means $\hat{f} \in \mathfrak{a}$ and by the inductive hypothesis, $\hat{f}$ is in the ideal generated by $\mathfrak{b}$ in A. So $f = \hat{f} \cdot Y$ is in the ideal generated by $\mathfrak{b}$ in A as well. □

Again R is a differential domain containing $\mathbb{Z}$ in K commuting derivatives and $A := R\{Y_1, ..., Y_N\}$ is the differential polynomial ring in N variables and K derivations. Recall from 2.8 that for $G \subseteq A$ and $y \in \mathscr{D}Y$ we have defined

$$G_{\leq y} = \{\theta g \mid g \in G,\ \theta \in \mathscr{D} \text{ and } \operatorname{rk}(\theta u_g) \leq \operatorname{rk}(y)\}$$
$$G_{< y} = \{\theta g \mid g \in G,\ \theta \in \mathscr{D} \text{ and } \operatorname{rk}(\theta u_g) < \operatorname{rk}(y)\}$$

Recall that G is in general not a subset of $G_{\leq y}$, even if y is a proper derivative of some u_g, $g \in G$.

Clearly $G_{<y} = \bigcup \{G_{\leq z} \mid \operatorname{rk} z < \operatorname{rk} y\}$. Moreover $G \cup \partial_i(G_{\leq y}) \subseteq G_{\leq \partial_i y}$, thus

$$\partial_i((G_{\leq y})) \subseteq (G_{\leq \partial_i y}).$$

5.2. **Definition.** A reduced subset G of A is called **coherent** if for all g_1, g_2 for which u_{g_1} and u_{g_2} have a common (higher) derivative the following condition holds.

Let $\theta_1, \theta_2 \in \mathscr{D}$ be such that $y := \theta_1 u_{g_1} = \theta_2 u_{g_2}$ is the least common derivative of u_{g_1} and u_{g_2}. Then there is some $n \in \mathbb{N}_0$ such that

$$H(G)^n (S(g_2)\theta_1 g_1 - S(g_1)\theta_2 g_2) \in (G_{<y}).$$

If $w := \theta_1 u_{g_1} = \theta_2 u_{g_2}$ is any common derivative of u_{g_1} and u_{g_2}, then one checks that there is some $n \in \mathbb{N}_0$ with

$$H(G)^n (S(g_2)\theta_1 g_1 - S(g_1)\theta_2 g_2) \in (G_{<w}).$$

This is done in the following lemma.

5.3. **Lemma.** *Let $G\subseteq A$, $g_1,g_2\in G$, $\theta_1,\theta_2\in\mathscr{D}$, $h,s_1,s_2\in A$ and $y\in\mathscr{D}Y$ such that y is a derivative of $\theta_1 u_{g_1}$ and of $\theta_2 u_{g_2}$. If*

$$h^n(s_1\theta_1 g_1 - s_2\theta_2 g_2)\in (G_{\leq y})$$

then

$$h^{n+1}(s_1\partial_i\theta_1 g_1 - s_2\partial_i\theta_2 g_2)\in (G_{\leq \partial_i y})$$

Proof. Let $f:=s_1\theta_1 g_1 - s_2\theta_2 g_2$. Then

$$\begin{aligned} h\cdot\partial_i(h^n\cdot f) &= nh^n f\partial_i h + h^{n+1}\partial_i f = \\ &= nh^n f\partial_i h + \\ &+ h^{n+1}(\partial_i(s_1)\theta_1 g_1 - \partial_i(s_2)\theta_2 g_2) + \\ &+ h^{n+1}(s_1\partial_i\theta_1 g_1 - s_2\partial_i\theta_2 g_2)\end{aligned}$$

Since $h^n\cdot f\in (G_{\leq y})$ by assumption we get that $h\cdot\partial_i(h^n\cdot f)$, $nh^n f\partial_i h$, $\theta_1 g_1$ and $\theta_2 g_2$ are in $(G_{\leq\partial_i y})$, so $h^{n+1}(s_1\partial_i\theta_1 g_1 - s_2\partial_i\theta_2 g_2)\in (G_{\leq\partial_i y})$ as well. □

5.4. **Proposition.** *Let $G\subseteq A$ be a reduced and coherent set. If $f\in A$ is weakly reduced with respect to G and $f\in Sat_{H_G}[G]$, then $f\in Sat_{H_G}(G)$, where (G) denotes the ideal generated by G in A.*

Proof. Let $g_1,...,g_m\in G$ and let $\theta_1,...,\theta_m\in\mathscr{D}$ of order >0 such that

$$(*)\qquad H\cdot f = \sum_{i=1}^m f_i\cdot\theta_i g_i + \sum_{g\in G} h_g\cdot g$$

for some $H\in H_G$ and polynomials $f_i,h_g\in A$ ($1\leq i\leq m$, $g\in G$). Let $\alpha := \max\{\operatorname{rk}\theta_i u_{g_i}\mid 1\leq i\leq m\}$. We'll reduce $(*)$ to an equation of the form $(*)$ where the corresponding α is smaller than the present one. After applying this argument finitely many times we get a representation of f in $Sat_{H_G}(G)$ which proves the proposition. The reduction goes as follows.

We may assume that there is some $l\in\{1,...,m\}$ such that $\operatorname{rk}\theta_i u_{g_i}=\alpha$ ($l\leq i\leq m$) and $\operatorname{rk}\theta_i u_{g_i}<\alpha$ ($1\leq i<l$). Let $y=\theta_l u_{g_l}=...=\theta_m u_{g_m}$. By $(*)$ we know that $H\cdot f\in\sum_{i=l}^m f_i\cdot\theta_i g_i + (G_{<y}) + (G)$. We have

$$S(g_m)\cdot\sum_{i=l}^m f_i\cdot\theta_i g_i = \sum_{i=l}^m (S(g_m)f_i\cdot\theta_i g_i - S(g_i)\cdot f_i\theta_m g_m) + \sum_{i=l}^m S(g_i)\cdot f_i\theta_m g_m.$$

Since G is a coherent set we get that $S(g_m)\cdot\sum_{i=l}^m f_i\cdot\theta_i g_i\in\tilde f\cdot\theta_m g_m + (G_{<y})$, where $\tilde f=\sum_{i=l}^m S(g_i)\cdot f_i$. Hence

$$S(g_m)\cdot H\cdot f\in\tilde f\cdot\theta_m g_m + (G_{<y}) + (G).$$

This means that there is an equation of the form $(*)$ such that $\theta_i u_{g_i}=y$ for at most one index $i\in\{1,...,m\}$. Say $y=\theta_m u_{g_m}$. Then $\theta_m u_{g_m}$ does not appear in $H,f,\theta_1 g_1,...,\theta_{m-1}g_{m-1}$ nor in any $g\in G$. We have $\theta_m g_m = S(g_m)\cdot\theta_m u_{g_m} + [\theta_m]g_m$ and $\theta_m u_{g_m}$ does not appear in $[\theta_m]g_m$. So if we replace $\theta_m u_{g_m}$ by $-[\theta_m]g_m/S(g_m)$ in $(*)$ we get an equation

$$(**)\qquad H\cdot f = \sum_{i=1}^{m-1}\tilde f_i\cdot\theta_i g_i + \sum_{g\in G}\tilde h_g\cdot g$$

with rational functions $\tilde{f}_i, \tilde{h}_g \in A_{S(g_m)}$. By multiplying with a suitable power p of $S(g_m)$ we get $S(g_m)^p \cdot H \cdot f \in (G_{<y}) + (G)$ as desired. □

5.5. **Corollary.** *Let $G \subseteq A$ be reduced and coherent. If $Sat_{H_G}(G)$ is reduced then $Sat_{H_G}[G]$ is reduced. If $Sat_{H_G}(G)$ is prime then $Sat_{H_G}[G]$ is prime.*

Proof. Let $f_1, f_2 \in A$ with $f_1 f_2 \in Sat_{H_G}(G)$. Let $H_i \in H_G$ and $\tilde{f}_i \in A$ reduced with respect to G such that $H_i f_i \equiv \tilde{f}_i \bmod [G]$. Since $H \cdot f_1 f_2 \in [G]$ for some $H \in H_G$ it follows that $\tilde{f}_1 \tilde{f}_2 \in Sat_{H_G}[G]$. As $\tilde{f}_1 \tilde{f}_2$ is weakly reduced with respect to G it follows $\tilde{f}_1 \tilde{f}_2 \in Sat_{H_G}(G)$ from 5.4. Hence $\tilde{f}_1 \in Sat_{H_G}(G)$ or $\tilde{f}_2 \in Sat_{H_G}(G)$ if $Sat_{H_G}(G)$ is prime and f_1 or f_2 is in $Sat_{H_G}[G]$. This shows that $Sat_{H_G}[G]$ is prime if $Sat_{H_G}(G)$ is prime. The same argument proves that $Sat_{H_G}[G]$ is reduced if $Sat_{H_G}(G)$ is reduced. □

5.6. **Theorem.** *(The Rosenfeld Lemma)*
Let $G \subseteq A$ be a reduced set. Then the following are equivalent.

(1) G is a characteristic set of $[G] : H_G^\infty$ and $[G] : H_G^\infty \cap R = 0$.
(2) (a) G is coherent and
   (b) The ideal $(G)_A : H_G^\infty$ of A does not contain non zero elements of A, reduced with respect to G.
(3) Let B denote the R-algebra $R[y \in \mathscr{D}Y \mid y$ appears in g for some $g \in G]$.
   (a) G is coherent and
   (b) The ideal $(G)_B : H_G^\infty$ of B does not contain non zero elements of B, reduced with respect to G.

In this case $[G] : H_G^\infty$ is reduced respectively prime if and only if $(G)_A : H_G^\infty$ is reduced respectively prime.

Proof. (1)⇒(2) follows from 4.7 and 2.3.

(2)⇒(1). Let $G = \{g_1, ..., g_l\}$ with $\operatorname{rk} g_1 < ... < \operatorname{rk} g_l$ and let $\tilde{G} = \{\tilde{g}_1, ..., \tilde{g}_m\}$ be a characteristic set of $\mathfrak{a} := [G] : H_G^\infty$ such that $\operatorname{rk} \tilde{g}_1 < ... < \operatorname{rk} \tilde{g}_m$. As $\operatorname{rk} \tilde{G} \leq \operatorname{rk} G$ we have $\operatorname{rk} \tilde{g}_1 \leq \operatorname{rk} g_1$. Suppose $\operatorname{rk} \tilde{g}_1 < \operatorname{rk} g_1$. Then $\tilde{g}_1 \in \mathfrak{a}$ is reduced with respect to G. By (a) and 5.4 we have $\tilde{g}_1 \in (G)_A : H_G^\infty$. By (2)(b) we have $\tilde{g}_1 = 0$, which is impossible.

Thus $\operatorname{rk} \tilde{g}_1 = \operatorname{rk} g_1$ and we may replace $\tilde{g}_1$ with g_1 in $\tilde{G}$. The same argument now applies to $\tilde{g}_2$ and we may replace $\tilde{g}_2$ by g_2. Ongoing in this way we obtain $l \leq m$ and $G \subseteq \tilde{G}$. But $l < m$ is not possible either, otherwise the argument above, applied to $\tilde{g}_m$ produces a contradiction, too. This shows that G is a characteristic set of $[G] : H_G^\infty$, hence (1) and (2) are equivalent.

Clearly (2) implies (3). We prove (3)(b)⇒(2)(b) now. Let $f \in (G)_A : H_G^\infty$ and suppose $f \neq 0$. We consider f as a polynomial over $R[y \in \mathscr{D}Y \mid y \notin B]$ and write $f = \sum f_i m_i$, where m_i are mutually different monomials in the variables from B and f_i are polynomials not containing any variable from B. As $f \neq 0$ there is at least one f_j among the f_i such that $f_j \neq 0$. Let $\psi : A \longrightarrow B$ be a B-algebra homomorphism sending f_j to a nonzero element of R and every variable $y \in \mathscr{D}Y \setminus B$ to an element from R. Let $H \in H_G$ with $H \cdot f \in \sum_{g \in G} Ag$. Then $H \cdot \psi(f) \in \sum_{g \in G} Bg$ and $\psi(f) \neq 0$. Moreover $\psi(f)$ is reduced with respect to G, so the ideal $(G)_A : H_G^\infty$ of B contains the nonzero element $\psi(f)$, which is reduced with respect to G.

So we know that (1), (2) and (3) are equivalent. Finally suppose $[G] : H_G^\infty$ is prime and let $B := R[y \mid y \in \mathscr{D}Y$ appears in some $g \in G]$. By 5.1 it is enough to show that $(G)_B : H_G^\infty$ is prime. So let $f_1, f_2 \in B$ with $f_1 \cdot f_2 \in (G)_B : H_G^\infty$. By assumption we may assume that $f_1 \in [G] : H_G^\infty$. Since $f_1 \in B$, B is weakly reduced with respect to G, hence $f_1 \in R \cap (G)_A : H_G^\infty = (G)_B : H_G^\infty$. A similar argument shows that $(G)_A : H_G^\infty$ is reduced if $[G]_A : H_G^\infty$ is reduced. Finally 5.5 finishes the proof of the theorem. □

5.7. *Example.* Suppose $G \subseteq A$ is reduced, $(G)_B$ is prime and $L(g), S(g) \notin (G)_B$ $(g \in G)$, where $B = R[y \mid y \in G]$. Then $(G)_A : H_G^\infty = (G)_A$ by 5.1.

References

[Kol] E. R. Kolchin. Differential algebra and algebraic groups. Academic Press, New York, 1973. Pure and Applied Mathematics, Vol. 54. 1, 2

The University of Manchester, School of Mathematics, Oxford Road, Manchester M13 9PL, UK

Email address: marcus.tressl@manchester.ac.uk