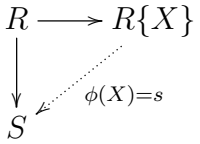
LECTURE 2. RITT-RAUDENBUSH THEORY

Convention. *All differential rings are commutative and contain* $\mathbb{Q}$. If R is a differential ring, we denote by $R\{X\}$ the differential ring of differential polynomials with one variable and coefficients in R.

- $R\{X\}$ is characterized by the following universal property: whenever $R \to S$ is a morphism (of differential rings) and $s \in S$, there is a unique morphism $\phi : R\{X\} \to S$ such that



  commutes and $\phi(X) = s$.
- $R\{X\}$ can be constructed as follows: as a ring,

$$R\{X\} = R[X_i \mid i \in \mathbb{N}]$$

  is the polynomial ring in infinitely many indeterminates. The derivation $\partial \in \mathrm{Der}(R\{X\})$ is the unique one satisfying:

$$\partial_{|R} = \partial_R \text{ and } \partial(X_i) = X_{i+1}$$

  where $\partial_R : R \to R$ is the given derivation on R. Because of the definition of the derivation, the variables X_i can be interpreted as the successive derivatives of the variable $X_0 = X$. To emphasize this, we will write

$$X = X_0, X' = X_1, \ldots, X^{(n)} = X_n \cdots$$

An element f of $R\{X\}$ is called a *differential polynomial of one variable with coefficients in* R. Starting from a differential field k, one obtains inductively the differential algebra $k\{X_1, \ldots, X_n\}$ of differential polynomials with n variables for every $n \geq 1$ The goal of this section is to describe some foundational algebra of *differential polynomials*. This is the subject of Ritt-Raudenbush theory.

2.1. **Terminology on differential polynomials.** Let $f \in R\{X\}$. We define the *order of* f is the maximal $n = \mathrm{ord}(f)$ such that $X^{(n)}$ appears nontrivially in f. It is convenient to set $\mathrm{ord}(f) = -\infty$ if $f \in R$. Hence, if $\mathrm{ord}(f) \geq 0$, we can write

$$f = \sum_{i=0}^{d} a_i \cdot (X^{(n)})^i \tag{1}$$

where all the $a_i \in R\{X\}$ have order $< n$. If $a_d \neq 0$, we say that f has *degree* d and that a_d is the *initial of* f. The degree of f will be denoted $\deg(f)$ and its initial will be denoted i_f. This information is organized as follows:

- the pair $(\mathrm{ord}(f), \deg(f))$ defines a preorder on the set of differential polynomials

$$f \ll g \text{ iff } \mathrm{ord}(f) < \mathrm{ord}(g) \text{ or } \mathrm{ord}(f) = \mathrm{ord}(g) \text{ and } \deg(f) < \deg(g).$$

- any differential polynomial $f \in R\{X\}$ of order ≥ 0 can be written as
$$f = i_f \cdot (X^{(n)})^d + f_0$$
where $f_0 \in R[X]$ $f_0 \ll f$, $n = \mathrm{ord}(f)$, $d = \deg(f)$ and i_f is the initial of f.

Definition 2.1. Assume that $\mathrm{ord}(f) \geq 0$. The *separant* of $f \in R\{X\}$ denoted $s_f \in R\{X\}$ is the differential polynomial defined by

$$s_f = \frac{\partial f}{\partial X^{(n)}} \neq 0. \tag{2}$$

Explicitly, if f is given as in (1) then its separant s_f is given by

$$s_f = \sum_{i=0}^{d} i a_i \cdot (X^{(n)})^{i-1} = \sum_{i=0}^{d-1} (i+1) a_{i+1} (X^{(n)})^i. \tag{3}$$

It follows easily that we always have $s_f \ll f$.

Example 2.2. In practice, we often can reduce to study algebraic differential equations which are explicitly presented as

$$y^{(n)} = F(y, \ldots, y^{(n-1)}).$$

It is defined as the solution set of the differential polynomial $P(X) = X^{(n)} - F(X, \ldots, X^{(n-1)})$. P has order n, its initial term and its separant are both equal to 1.

Lemma 2.3. *Assume that $n = \mathrm{ord}(f) \geq 0$ and let $k \geq 1$. Then*

$$f^{(k)} = s_f X^{(n+k)} + f_k \text{ with } \mathrm{ord}(f_k) < \mathrm{ord}(f^{(k)})$$

Hence, $\mathrm{ord}(f^{(k)}) = \mathrm{ord}(f) + k$, $\deg(f^{(k)}) = 1$ *and that the initial of $f^{(k)}$ is the separant of f.*

Proof. As in (1), we write $f = \sum_{i=0}^{d} a_i \cdot (X^{(n)})^i$ and using the Leibniz rule, we obtain:

$$f' = \sum_{i=0}^{d} \Big(a_i' (X^{(n)})^i + i \cdot a_i (X^{(n)})^{i-1} X^{(n+1)} \Big) = \sum_{i=0}^{d} a_i' (X^{(n)})^i + s_f X^{(n+1)}$$

Since $s_f \neq 0$, $X^{(n+1)}$ appears non trivially on the right-hand side but not on the left-hand side. Hence, $\mathrm{ord}(f') = n + 1$ and

$$f' = \Big(\sum_{i=0}^{d} i a_i (X^{(n)})^{i-1} \Big) X^{(n+1)} + f_1 = s_f X^{(n+1)} + f_1$$

where f_1 is a differential polynomial of order $< n+1$. The rest of the statement is obtained by induction on k noting that $s_f = s_{f'}$ by the previous formula. □

2.2. **Euclidean division in $R\{X\}$.** If $f \in R\{X\}$, we denote by $\langle f \rangle$ the differential ideal of $R\{X\}$ generated by f, that is, the ideal

$$\langle f \rangle = (f, f', \ldots, f^{(k)}, \ldots)$$

of $R\langle X \rangle$ generated by f and all its derivatives.

Lemma 2.4. *Assume that $n = \mathrm{ord}(f) \geq 0$. For every $g \in R\{X\}$, there exists $m \geq 0$ and $r \in R\{X\}$ with $\mathrm{ord}(r) \leq \mathrm{ord}(f)$ such that*

$$s_f^m \cdot g = r \bmod \langle f \rangle.$$

Proof. We may assume that $\mathrm{ord}(g) > n = \mathrm{ord}(f)$. Write

$$g = i_g \cdot (X^{(n+k)})^d + g_0 \text{ with } g_0 \ll g.$$

which after multiplication by s_f^d can be written as

$$s_f^d \cdot g = i_g \cdot (s_f \cdot X^{(n+k)})^d + s_f^d \cdot g_0$$

By Lemma 2.3, we can write

$$f^{(k)} = s_f X^{(n+k)} + f_k \text{ with } f_k \ll f$$

and combining the two, we obtain

$$s_f^d \cdot g = i_g \cdot (f^{(k)} - f_k)^d + s_f^d \cdot g_0 = (-1)^d f_k^d \cdot i_g + s_f^d \cdot g_0 \bmod \langle f \rangle.$$

After setting $g_1 = (-1)^d f_k^d \cdot i_g + s_f^d \cdot g_0$, an easy computation — using $\mathrm{ord}(f) < \mathrm{ord}(g)$ — shows that $g_1 \ll g$ and we conclude by induction on $\ll$. □

Lemma 2.5. *Assume that $n = \mathrm{ord}(f) \geq 0$. For every $g \in R\{X\}$, there exists $m, l \geq 0$ and $r \in R\{X\}$ with $r \ll f$ such that*

$$i_f^l \cdot s_f^m \cdot g = r \bmod \langle f \rangle.$$

Proof. By Lemma 2.4, we can find r_1 with $\mathrm{ord}(r_1) \leq \mathrm{ord}(f)$ and m such that $s_f^m \cdot g = r_1 \bmod \langle f \rangle$. Now we can think about f and r_1 as elements of

$$R[X, \ldots, X^{(n-1)}][X^{(n)}] = S[X^{(n)}]$$

The usual division algorithm in polynomial rings shows that we can find r_2 with $\deg(r_2) < \deg(f)$ and $l \geq 0$ such that

$$r_2 = i_f^l \cdot r_1 \bmod (f)$$

in $S[X]$. Putting everything together, we have obtain that

$$i_f^l \cdot s_f^m \cdot g = r_2 \bmod \langle f \rangle$$

and $r_2 \ll f$ as required. □

2.3. **Prime differential ideals of $k\{X\}$.** Let k be a differential field.

Theorem 2.6. *For every* irreducible *differential polynomial f,*

$$I(f) = \{g \in k\{X\} \mid \exists m \geq 0, s_f^m \cdot g \in \langle f \rangle\}$$

is a prime differential ideal *of $k\{X\}$ and all the nonzero prime differential ideals of $k\{X\}$ are of this form.*

Here, we say that a differential polynomial $f \in k\{X\}$ is irreducible if $n = \mathrm{ord}(f) \geq 0$ and it is irreducible as a polynomial of $k[X, X', \ldots, X^{(n)}]$.

Exercise 2.7. *Show that $f = (X'')^2 - 2X'$ is irreducible but that $\langle f \rangle$ is not a prime ideal.*

Proof of Theorem 2.6. Clearly, $I(f)$ is a differential ideal of $k\langle X \rangle$. To see that it is differential, note that

$$(s_f^{m+1} \cdot g)' = (m+1) \cdot (s_f^m \cdot g) + s_f^{m+1} \cdot g'$$

and hence that $s_f^m \cdot g \in \langle f \rangle \Rightarrow s_f^{m+1} \cdot g' \in \langle f \rangle$.

- **Step 1**. *$I(f)$ is a* prime *differential ideal of $k\{X\}$ if f is irreducible.*

Assume that $u \cdot v \in I(f)$ for some $u, v \in k\{X\}$. Using Lemma 2.4, we can write

$$s_f^{n_1} \cdot u = r \bmod \langle f \rangle \text{ and } s_f^{n_2} \cdot v = s \bmod \langle f \rangle$$

with $\mathrm{ord}(r), \mathrm{ord}(s) \leq \mathrm{ord}(f)$. Now since $u \cdot v \in I(f)$, for some $m \geq 0$ we have

$$s_f^m \cdot r \cdot s \in \langle f \rangle$$

and $\mathrm{ord}(s_f^m \cdot r \cdot s) \leq \mathrm{ord}(f) = n$. The following claim shows that f must divides $s_f^m \cdot r \cdot s$. Since f is irreducible and $s_f \ll f$, we conclude that f must divides r or s. This finishes the proof of Step 1.

Claim. *Assume that f is irreducible and that $g \in I(f)$ is a differential polynomial of order $\leq \mathrm{ord}(f)$ then f divides g in $k\{X\}$.*

Proof of the claim. We can write

$$s_f^n \cdot g = a_0 f + \cdots + a_k f^{(k)} \tag{4}$$

If $k \geq 1$ in this expression, using Lemma 2.3, we can write

$$f^{(k)} = s_f X^{(n+k)} + f_k$$

Since $X^{(n+k)}$ does not appear on the left-hand side of (4), after making the subtitution

$$X^{(n+k)} \mapsto -f_k / s_f$$

and clearing the denominators, we obtain a new expression of the form

$$s_f^{n+N} \cdot g = b_0 f + \cdots + b_{k-1} f^{(k-1)}.$$

Repeating this process, we can assume that $k = 1$. Since f divides $s_f^n \cdot g$ and $s_f \ll f$, this implies that f divides g. □

- **Step 2**. *Every nonzero prime differential ideal of $k\{X\}$ is of this form.*

Consider I a nonzero prime ideal and set f to be a minimal nonzero polynomial in I with respect to $\ll$. Since I is prime, f is irreducible. We show that $I = I(f)$.

- $\supset$ Since $s_f \ll f$, $s_f \notin I$. Hence if $g \in I(f)$ then for some m, $s_f^m \cdot g \in \langle f \rangle \subset I$ and since I is prime, we conclude that $g \in I$.
- $\subset$ Take $g \in I$. Applying Lemma 2.5 to g, we can write

  $$i_f^l \cdot s_f^k \cdot g = g_0 \bmod \langle f \rangle$$

  for some $g_0 \ll f$. The previous equality implies that $g_0 \in I$ and hence that $g_0 = 0$ by minimality of f.

This completes the proof of the theorem. □

The geometric intepretation of this theorem can be phrased as follows: If f is an irreducible differential polynomial of order $n \geq 1$ then f seen as an ordinary polynomial of several variables cuts off an hypersurface

$$Z(f) := \{(x_0, \ldots, x_n) \mid f(x_0, \ldots, x_n) = 0\} \subset \mathbb{A}_k^{n+1}$$

The restriction of the projection on the first n coordinates to Z defines a morphism

$$f : Z(f) \to \mathbb{A}_k^n \tag{5}$$

The ramification locus of f — that is the set of points where the differential df is not invertible is equal to

$$\mathrm{Sing}(f) = \{(x_0, \ldots, x_n) \mid f(x_0, \ldots, x_n) = s_f(x_0, \ldots, x_n) = 0\} \subsetneq Z(f).$$

Outside of $\mathrm{Sing}(f)$, f is an étale morphism. If R denotes the ring of regular focus on $Z(f) \setminus \mathrm{Sing}(f)$, this means the module of Kähler differentials (see Lecture 5) satisfy that $\Omega^1(R/k[X_0, \ldots, X_{n-1}])$ is trivial. In other words,

> every derivation of $k[X_0, \ldots, X_{n-1}]$ with values in a R-module M uniquely to a derivation of R with values in M.

Applied to

$$D = X_1 \frac{\partial}{\partial X_0} + \cdots + X_n \frac{\partial}{\partial X_{n-1}} : k[X_0, \ldots, X_{n-1}] \to k[X_0, \ldots, X_n] \to R$$

this produces a differential ring structure on R isomorphic to $k\{X\}/I(f)$. In particular, this geometric proof shows that in fact that $k\{X\}/I(f)$ is not only an integral domain but also a finitely generated k-algebra.

2.4. **Radical ideals of $R\{X\}$.** Pursuing the analogy, it is natural to ask whether $k\{X\}$ is noetherian with respect to differential ideals, that is,

> (ACC): every increasing chain of differential ideals is stationary.

Exercise 2.8. *Show that the sequence of differential ideals $I_n = \langle X^2, (X')^2, \ldots, (X^{(n)})^2 \rangle$ is an infinite increasing chain of differential ideals of $k\{X\}$.*

This becomes true after restricting to *radical* differential ideals.

Theorem 2.9. *Let R be a differential ring satisfying (ACC) for radical differential ideals. The differential ring $R\{X\}$ also satisfies (ACC) for radical differential ideals.*

Recall that an ideal I of R is *radical* if the ring R/I does not contain any nonzero nilpotent element[1] or equivalently if $a^n \in I \Rightarrow a \in I$. Every ideal I of R is contained in a smaller radical ideal called *the radical of I* and denoted $\sqrt{I}$. Explicitly, we have:

$$\sqrt{I} = \{x \in R \mid x^n \in I \text{ for some } n\}.$$

Lemma 2.10. *Assume that R is a differential ring and that I is a differential ideal. Then $\sqrt{I}$ is a radical differential ideal.*

Proof. Assume that $x^n \in I$ for some n. Since I is a differential ideal, we have

$$\partial(x^n) = nx^{n-1}\partial(x) \in I$$

so that $x^{n-1}\partial(x) \in I$. Taking the derivative again, we see that $(n-1)x^{n-2}(\partial(x))^2 + x^{n-1}\partial^2(x) \in I$ which after multiplying by $\partial(x)$ implies that

$$(n-1)x^{n-2}(\partial(x))^3 + (x^{n-1}\partial(x))\partial^2(x) \in I$$

and that $x^{n-2}(\partial(x))^2 \in I$. Iterating the process, we obtain that for every $1 \leq k \leq n$,

$$x^{n-k}(\partial(x))^{2k-1} \in I$$

and hence that $\partial(x)^n \in I$ as required. □

[1] an element a is nilpotent if and only if $a^n = 0$ for some $n \geq 1$.

Notation 2.11. For any $S \subset R$, we denote by $\{S\}$ the smallest radical differential ideal containing S. By the previous lemma, we have

$$\{S\} = \sqrt{\langle S \rangle}$$

where as previously $\langle S \rangle$ denotes the differential ideal generated by S.

Lemma 2.12 (Lemma of radical ideals)**.** *For any $S, T \subset R$, we have $\{S\} \cdot \{T\} \subset \{S \cdot T\}$ where $S \cdot T$ denotes the set of products of elements of S and elements of T.*

Proof. We prove the lemma in two steps: we first prove that $a \cdot \{S\} \subset \{a \cdot S\}$ for any $a \in R$: consider

$$T = \{x \in R \mid a \cdot x \in \{a \cdot S\}\}$$

Clearly, T is an ideal and we claim that it is a radical differential ideal:

- *differential.* take $x \in T$. Since $\{a.S\}$ is a differential ideal, we have taking the derivative and multiplying by $a\partial(x)$ that
$$a\partial(x) \cdot \partial(a \cdot x) = (a\partial(x))^2 + \partial(x)\partial(a) \cdot (a \cdot x) \in \{a \cdot S\}$$
which implies that $(a\partial(x))^2 \in \{a.S\}$. Hence so does $a\partial(x)$ and $\partial(x) \in T$ as required.
- *radical.* Assume $x^n \in T$
$$ax^n \in \{a \cdot S\} \Rightarrow a^n x^n \in \{a \cdot S\} \Rightarrow a \cdot x \in \{a \cdot S\}$$
and hence $x \in T$ as required.

By minimality of $\{S\}$, it follows that $a \cdot \{S\} \subset \{a \cdot S\}$ To finish the proof of the lemma, it is then enough to repeat the same argument to conclude that

$$T_2 = \{x \in R \mid x \cdot \{T\} \subset \{S \cdot T\}\}$$

is a radical differential ideal which contains S by the first step (exercise). □

Proof of Theorem 2.9. It is enough to prove that every radical differential ideal is finitely generated (exercise). Assume otherwise and consider

$$\mathcal{S} = \{I \subset R\{X\} \mid I \text{ is a radical differential ideal NOT finitely generated }\}.$$

$\mathcal{S}$ is partially ordered by inclusion, inductive and nonempty by assumption. By Zorn's lemma, we can take a maximal element I of $\mathcal{S}$.

Claim. *I is prime.*

Proof of the claim. Otherwise, one can find $a, b \in R$ such that $a, b \notin I$ and $ab \in I$. It follows that $\{I, a\}$ and $\{I, b\}$ are finitely generated. A straightforward computation shows that we can find generators of the form

$$\{I, a\} = \{a = f_0, f_1, \ldots, f_s\} \text{ and } \{I, b\} = \{b = g_0, g_1, \ldots, g_r\}$$

where the f_i and g_j belong to I for every $i, j \geq 1$. Since I is an ideal and $ab \in I$, it follows that

$$I \subset \{f_i \cdot g_j \mid i = 0, \ldots, s, j = 0, \ldots r\}.$$

Conversely if $c \in I$, the lemma of radical ideals implies that

$$c^2 \in \{I, a\} \cdot \{I, b\} = \{f_0, \ldots, f_s\} \cdot \{g_0, \ldots, g_r\} \subset \{f_i \cdot g_j \mid i = 0, \ldots, s, j = 0, \ldots r\}$$

so that $c \in \{f_i \cdot g_j \mid i = 0, \ldots, s, j = 0, \ldots r\}$. So I is finitely generated which is a contradiction. Hence, I is prime. □

By assumption on R, $I \cap R$ is a radical ideal of R and hence finitely generated. It follows that the $R\{X\}$-ideal $J \subset I$ generated by $I \cap R$ is also finitely generated. Consider f a differential polynomial minimal with respect to $\ll$ in $I \setminus J$.

Claim. $i_f \cdot s_f \notin I$

Proof of the claim. Since I is prime, it is enough to show that $i_f \notin I$ and $s_f \notin I$.

- *Case of the initial.* assume $i_f \in I$. Since $i_f \ll f$, we obtain $i_f \in J$. Writing $f = i_f X^{(n)} + f_0$ with $f_0 \ll f$ we also obtain that $f_0 \in I$ and therefore in J. This is a contradiction as this implies $f \in J$.
- *Case of the separant.* assume $s_f \in I$. The same argument shows that $s_f \in J$ and also
$$g = f - \frac{1}{d} X^{(n)} s_f \ll f$$
also belongs to I and hence in J. This again implies that $f \in J$.

□

By maximality of I, $\{I, i_f \cdot s_f\}$ is therefore finitely generate and one can find a system of generators $g_1, \ldots, g_m \in I$ such that

$$\{I, i_f \cdot s_f\} = \{g_0 = i_f \cdot s_f, g_1, \ldots, g_m\}$$

Claim. $I = \{J, f, c_1, \ldots, c_m\}$

Proof of the claim. The inclusion $\supset$ is clear. Conversely, consider $g \in I$ and write using Lemma 2.5

$$i_f^s \cdot s_f^t \cdot g = g_0 \bmod \langle f \rangle$$

with $g_0 \ll f$. Since $g_0 \in I$, we must have $g_0 \in J$ by minimality of f. Hence, $i_f \cdot s_f \cdot g \in \{J, f\}$ and we have shown that $i_f \cdot s_f \cdot I \subset \{J, f\}$. It follows using the lemma of radical ideals that

$$I^2 \subset I \cdot \{i_f \cdot s_f, I\} = I \cdot \{i_f \cdot s_f, c_1, \ldots, c_m\} \subset \{J, f, c_1, \ldots, c_m\}$$

Since the latter is a radical ideal, we conclude that $I \subset \{J, f, c_1, \ldots, c_m\}$ as required. □

As J is finitely generated, we conclude that I is finitely generated which is our final contradiction. This completes the proof of the theorem. □

2.5. **Kolchin's primitive element theorem.** Finally, we have Kolchin's primitive element theorem whose proof will be the subject of the homework.

Theorem 2.13. *Let k be a nonconstant differential field and let $K = k\langle \alpha_1, \ldots, \alpha_n \rangle$ be a finitely generated differential field extension of k such that each α_i is a solution of a nonzero differential polynomial $A_i \in k\{X\}$. Then there exists $\gamma \in K$ such that*

$$K = k\langle \alpha_1, \ldots, \alpha_n \rangle = k\langle \gamma \rangle.$$

2.6. **References.** The results presented in this lecture constitutes the modern foundation of differential algebra and are due to the Joseph Ritt [Rit30]. Essentially, all the results of this section extends to the case of *partial differential fields*: differential fields equipped with n commmuting derivations. The partial case was treated later on by Ritt in [Rit45]. This lecture follows the presentation of Ritt's results of Irving Kaplansky in [Kap76] and Dave Marker in [MMP96].

References

[Kap76] Irving Kaplansky. *An introduction to differential algebra*. Publications de l'Institut de Mathématique de l'Université de Nancago, No. V. Hermann, Paris, second edition, 1976. Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics], No. 1251.

[MMP96] D. Marker, M. Messmer, and A. Pillay. *Model theory of fields*, volume 5 of *Lecture Notes in Logic*. Springer-Verlag, Berlin, 1996.

[Rit30] J. F. Ritt. Manifolds of functions defined by systems of algebraic differential equations. *Trans. Amer. Math. Soc.*, 32(4):569–599, 1930.

[Rit45] J. F. Ritt. On the manifold of partial differential polynomials. *Ann. of Math. (2)*, 46:102–112, 1945.