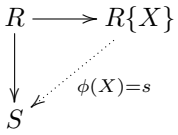
LECTURE 2. RITT THEORY

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

- the differential ring $R\{X\}$ can be defined by the following universal property: whenever $R \to S$ is a morphism of differential rings and $s \in S$, there is a unique morphism of differential rings $\phi : R\{X\} \to S$ such that the following diagram commuted



  and $\phi(X) = s$.
- the differential ring $R\{X\}$ is 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 is the unique derivation $\partial \in \mathrm{Der}(R\{X\})$ 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. The goal of this section is to describe some basic theory of *differential polynomials of one variable, of prime and radical ideals of* $R\{X\}$. This is the subject of Ritt-Raudenbush theory.

2.1. **Terminology on differential polynomials.** Let $f \in R\{X\}$ be a differential polynomial. 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 moreover 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 $f_0 \in R[X]$ $f_1 \ll f$, $n = \mathrm{ord}(f)$, $d = \deg(f)$ 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

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

More concretely, if f is given as in Equation (1) then its separant s_f is given by

$$s_f = \sum_{i=0}^{d} i a_i \cdot (X^{(n)})^{i-1} = \sum_{i=0}^{d-1} (i+1) a_{i+1} (X^{(n)})^i. \tag{2}$$

It follows easily from the previous formula that $s_f \ll f$.

Lemma 2.2. *Assume that $n = \mathrm{ord}(f) \geq 0$ and let $k \geq 1$. Then*

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

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

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

By definition $d \geq 1$, so that $X^{(n+1)}$ appears non trivially on the right terms of the previous sum but not on the left terms. 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. **Two division lemmas in $R\{X\}$.** If $f \in R\{X\}$ is a differential polynomial, we denote by $\langle f \rangle$ the differential ideal of $R\{X\}$ generated by f.

Lemma 2.3. *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 1.2, 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 2.4. *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 1.3, 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 ideals of $k\{X\}$.** Let k be a differential field.

Theorem 2.5 (Prime ideals of $k\{X\}$)**.** *The map*

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

defines a one-to-one correspondence between the set of irreducible differential polynomials of $k\{X\}$ and the set of non-zero differential prime ideals of $k\{X\}$.

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

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

Proof of Theorem 1.5. 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 1.3, 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 $\operatorname{ord}(r), \operatorname{ord}(s) \leq \operatorname{ord}(f)$. Now since $u \cdot v \in I(f)$, it follows easily that for some $m \geq 0$,

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

and $\operatorname{ord}(s_f^m \cdot r \cdot s) \leq \operatorname{ord}(f) = n$. The rest of Step 1 follows from the following claim.

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

Proof of the claim. We can write

$$s_f^n \cdot g = a_0 f + \cdots + a_k f^{(k)} \tag{3}$$

If $k \geq 1$ in this expression, using Lemma 1.2, 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 Equation (3), 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 $k = 0$. In that case, f divides $s_f^n \cdot g$ and since $s_f \ll f$ and f is irreducible, this implies that f divides g as required. □

- **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, we must have that f is irreducible. We show that $I = I(f)$.

$\supset$ Since $s_f \ll f$, we must have that $s_f \notin I$. 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 1.4 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 $g_0 \in I$ which implies $g_0 = 0$ by minimality of f.

This completes the proof of the theorem □

2.4. **Radical ideals of $R\{X\}$.** The previous result is an analogue for $k\{X\}$ for prime differential ideals of the well-known result in commutative algebra that $k[X]$ is a principal ring. Similarly, one could hope that every $k\{X\}$ is noetherian with respect to differential ideals:

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

This is (unfortunately?) not true as one can show that the sequence of differential ideals

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

is an infinite increasing chain of differential ideals of $k\{X\}$. The next theorem says that the next best thing happens.

Theorem 2.6 (Description of radical ideals)**.** *Let R be a differential ring satisfying (ACC) for radical differential ideals. The differential ring $R\{X\}$ also satisfies (ACC) for radical differential ideals.*

Terminology on radical 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 $\sqrt{I}$. More concretely,

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

Lemma 2.7. *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 $(n-1)x^{n-2}\partial(x) + x^{n-1}\partial^2(x) \in I$ which after multiplying by $\partial(x)$ implies that

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

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

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

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

Notation 2.8. 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 2.9 (Lemma of radical ideals)**.** *For any $S, T \subset R$, we have $\{S\} \cdot \{T\} \subset \{S \cdot T\}$.*

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 from which the first step of the lemma follows.

- *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.

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

To prove the lemma, it is then enough to repeat the first step to prove 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). □

Lemma 2.10. *Let R be a differential ring. The following are equivalent:*

(i) *R satisfies (ACC) on radical differential ideals.*
(ii) *Every radical differential ideal is finitely generated.*

Furthermore, if R satisfies the two previous properties then any radical differential ideal is the intersection of finitely many prime ideals.

Proof. (i) $\Leftrightarrow$ (ii). One direction is clear. For the converse, consider

$$I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$$

an ascending chain of radical differential ideals. An easy verification shows that $I = \bigcup_{i\in\mathbb{N}} I_i$ is a radical differential ideal and is therefore finitely generated by say $f_1, \ldots, f_r$. Take N large enough so that $f_1, \ldots, f_r \in I_N$. It follows that $I = I_N$ and therefore that the chain is stationary.

For the second part of the statement, for the sake of contradiction assume otherwise. By (ACC), there is a maximal radical ideal I which is not the intersection of finitely many prime differential ideals. As I is not prime, we can find $a, b \in R$ such that

$$ab \in I \text{ and } a, b \notin I.$$

Hence $\{I, a\}$ and $\{I, b\}$ are both intersection of finitely many prime differential ideals. To get our contradiction, it is therefore enough to see that

$$I = \{I, a\} \cap \{I, b\}$$

Let $c \in \{I, a\} \cap \{I, b\}$. Then by Lemma 1.9

$$c^2 \in \{I, a\} \cdot \{I, b\} \subset \{I, a \cdot b\} = I$$

and hence $c \in I$ as I is radical. This concludes the proof of the lemma. □

Proof of Theorem 1.6. Using the previous lemma, it is enough to see that every radical differential ideal is finitely generated. Assume otherwise for the sake of the contradiction and consider the (nonempty by assumption) set

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

Certainly, $\mathcal{S}$ is partially ordered by inclusion and is inductive (exercise). By Zorn's lemma, we can consider a maximal element of $\mathcal{S}$ say I.

Claim. *I is prime.*

Proof of the claim. Otherwise, we can find $a, b \in R$ such that $a, b \notin I$ and $a \cdot b \in I$. It follows that $\{I, a\}$ and $\{I, b\}$ are finitely generated. Since by Lemma 1.6, we have

$$\{I, a\} = \sqrt{\langle I, a\rangle}$$

and similarly for $\{I, b\}$, we can find generating systems 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. We claim that $I = \{f_i \cdot g_j \mid i = 0, \ldots, s, j = 0, \ldots r\}$: first, $f_i \cdot g_j \in I$ for every i, j follows from the construction. So we consider $c \in I$ so that applying the lemma of radical ideals,

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

and since this ideal is radical, we conclude $c \in \{f_i \cdot g_j \mid i = 0, \ldots, s, j = 0, \ldots r\}$ as required. So I is finitely generated which is a contradiction. Hence, I is prime. □

So we have obtain a differential ideal I which is prime and not finitely generated. 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 the ideal 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 llf, we obtain $i_f \in J$. But since
$$f = i_f X^{(n)} + f_0 \text{ with } f_0 \ll f$$
we would 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 as before shows that $s_f \in J$ but then
$$g = f - \frac{1}{d} X^{(n)} s_f \ll f$$
also belongs to I and hence in J. This is again a contradiction as this implies $f \in J$.

□

By maximality of I, the radical ideal $\{I, i_f \cdot s_f\}$ is therefore finitely generated. The same argument as in the proof of the first claim shows that we can find $c_1, \ldots, c_m \in I$ such that
$$\{I, i_f \cdot s_f\} = \{c_0 = i_f \cdot s_f, c_1, \ldots, c_m\}$$

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 1.4
$$i_f^s \cdot s_f^t \cdot g = g_0 \bmod \langle f \rangle$$
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. □