THE RITT–RAUDENBUSH BASIS THEOREM

STEVEN V SAM

The exposition here follows [K].

Definition 1. Let A be a ring. A **derivation** of A is a linear operator $d\colon A \to A$ such that $d(xy) = d(x)y + xd(y)$ for all $x, y \in A$. A **differential ring** is a pair (A, d) where A is a commutative ring and d is a derivation of A. An ideal I of A is called a **differential ideal** if it is closed under d, i.e., for all $x \in I$, we have $d(x) \in I$. □

We will the following shorthand from calculus: $d(x)$ is denoted x' and for any positive integer n, $d^n(x)$ is denoted $x^{(n)}$.

If I is an ideal of a ring A and S is any subset, recall that the **quotient ideal** is defined as

$$(I : S) = \{x \in A \mid xS \subseteq I\},$$

which is in fact an ideal.

Proposition 2. *If I is a radical differential ideal and S is any subset, then $(I : S)$ is a radical differential ideal.*

Proof. If $x^n S \subseteq I$ for some positive integer n, then for any $s \in S$, we have $(xs)^n = s^{n-1}(x^n s) \in I$ and hence $xs \in I$ since I is radical, and so $x \in (I : S)$.

Next, suppose that $x \in (I : S)$. Then for any $s \in S$, we have $xs \in I$ by definition, $(xs)' \in I$ since I is differential, and hence $x's(xs)' \in I$. On the other hand, we have $x's(xs)' = (x's)^2 + (x's')(xs)$. The second term belongs to I since $xs \in I$ and hence $(x's)^2 \in I$. Since I is radical, we see that $x's \in I$ and hence $x' \in (I : S)$. □

If $\{I_\alpha\}$ is a collection of radical differential ideals, then the intersection $\bigcap_\alpha I_\alpha$ is again radical and differential. Hence for any subset S, we can define $\langle S \rangle$[1] to be the smallest radical and differential ideal that contains S.

A radical differential ideal I is of **finite type** if there exists a finite subset $S \subseteq A$ such that I is the smallest radical differential ideal containing S.

Corollary 3. *For any subsets S, T of A, we have $\langle S \rangle \langle T \rangle \subseteq \langle ST \rangle$ where $ST = \{xy \mid x \in S,\ y \in T\}$.*

Proof. Given $s \in S$, we have $T \subseteq (\langle sT \rangle : \{s\})$ by definition. By Proposition 2, $(\langle sT \rangle : \{s\})$ is a radical differential ideal, and so it contains $\langle T \rangle$ by definition. Also given $s \in S$, we have $\langle sT \rangle \subseteq \langle ST \rangle$, so that $s \in (\langle ST \rangle : \langle T \rangle)$. Again, $(\langle ST \rangle : \langle T \rangle)$ is a radical differential ideal, so it contains $\langle S \rangle$. □

Lemma 4. *If I is a differential ideal and x is any element such that $\langle x, I \rangle$ is of finite type, then there exist $a_1, \dots, a_r \in I$ such that $\langle x, I \rangle = \langle x, a_1, \dots, a_r \rangle$.*

Date: February 19, 2023.

[1] Kaplansky uses the notation $\{S\}$ but this seems too confusing to me.

Proof. Pick a finite generating set for $\langle I, x\rangle$. Then by definition, some power of each generator can be built using finitely many operations of addition, multiplication, derivatives from the elements x and some finite set of elements of I. Taking the union of these finitely many elements of I gives $a_1, \dots, a_r$. $\square$

Proposition 5. *Let A be a differential ring containing the ring of rational numbers $\mathbf{Q}$. If I is a differential ideal, then its radical $\sqrt{I}$ is also a differential ideal.*

Proof. Suppose that $x \in \sqrt{I}$, so that there exists a positive integer n such that $x^n \in I$. We will prove by induction that for all $k = 1, \dots, n$ that $x^{n-k}(x')^{2k-1} \in I$. For the base case $k = 1$, note that $(x^n)' \in I$ since I is differential, and that we have $(x^n)' = nx^{n-1}x'$. Since $\mathbf{Q} \subseteq A$, we see that $x^{n-1}x' \in I$ as desired.

Next, suppose that $x^{n-k}(x')^{2k-1} \in I$ for some $1 \le k < n$. Then

$$I \ni d(x^{n-k}(x')^{2k-1}) = (n-k)x^{n-k-1}(x')^{2k} + (2k-1)x^{n-k}(x')^{2k-2}x''.$$

Multiply the result by $x'/(n-k)$; the second term belongs to I by assumption, and so $x^{n-k-1}(x')^{2k+1} \in I$, which proves the induction step. Finally, taking $k = n$ shows that $(x')^{2n-1} \in I$, i.e., $x' \in \sqrt{I}$. $\square$

Remark 6. The statement can fail if we do not assume that $\mathbf{Q} \subseteq A$. For example, consider $\mathbf{F}_2[x]$ with the usual derivative. Then the ideal (x^2) is differential but its radical is (x), which is not differential. $\square$

In light of the above facts, we make the following definition.

Definition 7. A **Ritt algebra** is a differential ring which contains the ring of rational numbers $\mathbf{Q}$. $\square$

The above results tell us that for a subset S of a Ritt algebra, $\langle S\rangle$ is the radical of the smallest differential ideal containing S, i.e., we can first consider the differential ideal generated by S and then take its radical.

Definition 8. Let (A, d) be a differential ring, and let x be an indeterminate. We define $A\{x\}$ to be polynomial ring $A[x_0, x_1, \dots]$ in countably many variables equipped with the unique derivation (again called d) which agrees with d on A and satisfies $d(x_i) = x_{i+1}$ for all $i \ge 0$. This is the ring of **differential polynomials** in x and we will also use the following notation: $x_0 = x$ and $x_n = x^{(n)}$ for $n > 0$. $\square$

Our goal now is to prove a differential analogue of the Hilbert basis theorem. Say that a differential ring is **d-noetherian** if it satisfies the ascending chain condition on differential ideals; equivalently, every differential ideal can be generated by a finite subset. The obvious variant of the Hilbert basis theorem with d-noetherian rings turns out to fail, as the next example shows.

Example 9. Let $\mathbf{k}$ be any field with the 0 derivation and let $A = \mathbf{k}\{x\}$. Then $\mathbf{k}$ is certainly d-noetherian. For each nonnegative integer n, let I_n be the differential ideal of A generated by $x^2, (x')^2, \dots, (x^{(n)})^2$. We claim that $(x^{(n)})^2 \notin I_{n-1}$. To see this, note that applying the derivation or multiplying by elements of A cannot decrease the degree of an element when considered as a polynomial in $x, x', \dots$, and so it suffices to show that $(x^{(n)})^2$ is not obtained by taking $\mathbf{k}$-linear combinations of derivatives of $x^2, (x')^2, \dots, (x^{(n-1)})^2$. If we define the "derivative degree" of $x^{(i)}x^{(j)}$ to be $i + j$, then all elements of derivative degree $2n$ in I_{n-1}

must be obtained by taking $\mathbf{k}$-linear combinations of derivatives of $x^{(a)}x^{(b)}$ with $a+b = 2n-1$. We omit the routine check that this space does not contain $(x^{(n)})^2$. This implies that I_n is properly contained in I_{n+1} and hence A is not d-noetherian. $\square$

Interestingly though, there is a workaround. Say that a differential ring A is **topologically d-noetherian** if it satisfies the ascending chain condition on radical differential ideals.[2] Then the following variant can be proven.

Theorem 10 (Ritt-Raudenbush basis theorem)**.** *If A is a Ritt algebra which is topologically d-noetherian, then $A\{x\}$ is also topologically d-noetherian.*

To prove the basis theorem, it is equivalent to show that every radical differential ideal in a Ritt algebra is finite type.

Proposition 11. *Consider a differential ring which is not topologically d-noetherian. Then any maximal element I in the poset of radical differential ideals that are not finite type must be a prime ideal.*

Proof. If I is not prime, then there exist $x, y \notin I$ such that $xy \in I$. But then $\langle I, x\rangle$ and $\langle I, y\rangle$ both strictly contain I and hence must be finite type. By Lemma 4, there exist $e_1, \ldots, e_r \in I$ such that $\langle I, x\rangle = \langle x, e_1, \ldots, e_r\rangle$ and similarly, there exist $f_1, \ldots, f_s \in I$ such that $\langle I, y\rangle = \langle y, f_1, \ldots, f_s\rangle$. By Corollary 3, we have

$$I^2 \subseteq \langle I, x\rangle\langle I, y\rangle \subseteq \langle \{x, e_1, \ldots, e_r\}\{y, f_1, \ldots, f_s\}\rangle \subseteq I.$$

Now apply radicals to each ideal and keep in mind that I is radical:

$$I \subseteq \sqrt{\langle I, x\rangle\langle I, y\rangle} \subseteq \langle \{x, e_1, \ldots, e_r\}\{y, f_1, \ldots, f_s\}\rangle \subseteq I.$$

This implies that all of these ideals are equal. Since the third ideal is finite type, we conclude that I is as well. This is a contradiction, so we conclude that I must be a prime ideal. $\square$

We develop a few things before proceeding to the proof of this theorem. Given $\alpha \in A\{x\}$, there is an integer r so that we can write α as a polynomial in $x, x', \ldots, x^{(r)}$ with coefficients in A. The **order** of α, written $\mathrm{ord}(\alpha)$, is the largest r so that $x^{(r)}$ is actually used; if we think of all other $x, x', \ldots, x^{(r-1)}$ as constants, then the **degree** of α, written $\deg(\alpha)$, is just its degree as a polynomial in $x^{(r)}$. If $\mathrm{ord}(\alpha) = r$ and $\deg(\alpha) = d$, then we can write $\alpha = \sum_{i=0}^{d} \alpha_i (x^{(r)})^i$ where $\alpha_i \in A[x, x', \ldots, x^{(r-1)}]$. Then α_d is the **leading coefficient** of α, denoted $\mathrm{lc}(\alpha)$, and $\mathrm{sep}(\alpha) = \sum_{i=1}^{d} i\alpha_i(x^{(r)})^{i-1}$ is the **separant** of α, i.e., the derivative of α with respect to $x^{(r)}$ when thought of as a variable.

Example 12. If $\alpha = xx' + (x^{(2)})^4 + x^{(2)}(x^{(3)})^2 + x^{(3)}$, then its order is 3, its degree is 2, and its leading coefficient is $\mathrm{lc}(\alpha) = x^{(2)}$; its separant is $\mathrm{sep}(\alpha) = 2x^{(2)}x^{(3)} + 1$. $\square$

Given $\alpha, \beta \in A\{x\}$ with $\alpha \neq 0$, we say that β is **below** α if $(\mathrm{ord}(\beta), \deg(\beta)) < (\mathrm{ord}(\alpha), \deg(\alpha))$ with respect to lexicographic ordering. For any nonzero α, $\mathrm{sep}(\alpha)$ and $\mathrm{lc}(\alpha)$ are always below α.

Lemma 13. *Let A be a Ritt algebra and let $\alpha \in A\{x\}$ and let I be the differential ideal in $A\{x\}$ generated by α. Given any $f \in A\{x\}$, there exist nonnegative integers m, n and $g \in A\{x\}$ which is below α such that*

$$\mathrm{lc}(\alpha)^m \mathrm{sep}(\alpha)^n f - g \in I.$$

[2] "Topologically" refers to the fact that two ideals with the same radical define the same closed subset of usual prime spectrum $\mathrm{Spec}(A)$.

Proof. Let $r = \mathrm{ord}(\alpha)$ and $d = \deg(\alpha)$. Then we can write $\alpha = \sum_{i=0}^{d} \alpha_i (x^{(r)})^i$ where $\alpha_i \in A[x, x', \dots, x^{(r-1)}]$. Then we have

$$\alpha' = \mathrm{sep}(\alpha) x^{(r+1)} + \sum_{i=0}^{d} \alpha_i' (x^{(r)})^i.$$

Denoting the sum by T_1, we see that $\mathrm{ord}(T_1) \le r$. For general k, we get an expression of the form

$$\alpha^{(k)} = \mathrm{sep}(\alpha) x^{(r+k)} + T_k$$

where $\mathrm{ord}(T_k) \le r + k - 1$.

Now we prove the result by induction on $\mathrm{ord}(f)$. If $\mathrm{ord}(f) < r$, then we can take $g = f$ and $m = n = 0$. Next suppose that $\mathrm{ord}(f) = r$. We will show by induction on $\deg(f)$ that the result holds with $n = 0$. If $\deg(f) < d$, then f is below α so we can take $m = n = 0$ and $g = f$. Otherwise, if $\deg(f) \ge d$, then $h = \mathrm{lc}(\alpha) f - \mathrm{lc}(f)\alpha$ has strictly smaller degree than f, and so by induction, there exists m_0 and $g \in A\{x\}$ below α such that $\mathrm{lc}(\alpha)^{m_0} h - g \in I$. This implies that $\mathrm{lc}(\alpha)^{m_0+1} f - g \in I$ which proves the induction.

Finally, we deal with the case that $\mathrm{ord}(f) > r$. Let $k = \mathrm{ord}(f) - r$. Then $h = \mathrm{sep}(\alpha) f - \mathrm{lc}(f)\alpha^{(k)}$ satisfies $\mathrm{ord}(h) < \mathrm{ord}(f)$, so that by induction, there exist integers m, n_0 and $g \in A\{x\}$ below α such that $\mathrm{lc}(\alpha)^m \mathrm{sep}(\alpha)^{n_0} h - g \in I$. This implies that $\mathrm{lc}(\alpha)^m \mathrm{sep}(\alpha)^{n_0+1} f - g \in I$, which proves the induction. ☐

Proof of Theorem 10. Suppose the theorem fails, so that there is at least one radical differential ideal in $A\{x\}$ which is not of finite type. Given a chain of such ideals, their union also fails to be finite type, so we can use Zorn's lemma to pick a radical differential ideal I which is not of finite type and is maximal amongst all such ideals; I is prime by Proposition 11.

Then $I \cap A$ is finite type since A is topologically d-noetherian; let J be the radical differential ideal generated by $I \cap A$ in $A\{x\}$. Then $J \subseteq I$; since J is finite type, it must be strictly contained in I. Pick $\alpha \in I \setminus J$ such that $(\mathrm{ord}(\alpha), \deg(\alpha)) = (r, d)$ is minimal amongst elements of $I \setminus J$. Then we can write

$$\alpha = \mathrm{lc}(\alpha)(x^{(r)})^d + \gamma$$

for some γ which is below α. We claim that $\mathrm{lc}(\alpha) \notin I$. If it were, then $\gamma \in I$. Since both $\mathrm{lc}(\alpha)$ and γ are below α, we must have $\mathrm{lc}(\alpha), \gamma \in J$. But that implies that $\alpha \in J$, which is a contradiction and the claim follows.

We also claim that the separant $\mathrm{sep}(\alpha)$ is not in I. Suppose it does belong to I. Then $\mathrm{sep}(\alpha)$ it is below α, it belongs to J. But $\alpha - \frac{1}{d} x^{(r)} \mathrm{sep}(\alpha)$ is also below α and belongs to I so it must belong to J. Once again this implies that $\alpha \in J$, which is a contradiction, so the claim follows.

Next, let $a = \mathrm{lc}(\alpha)\mathrm{sep}(\alpha)$. Then $a \notin I$ because I is prime. Hence $\langle a, I \rangle$ strictly contains I so must be finite type. By Lemma 4, we can find $e_1, \dots, e_r$ so that $\langle a, I \rangle = \langle a, e_1, \dots, e_r \rangle$. Let K be the differential ideal generated by α. Now pick $f \in I$. It follows from Lemma 13 that there exist integers m, n and $g \in A\{x\}$ which is below α such that

$$\mathrm{lc}(\alpha)^m \mathrm{sep}(\alpha)^n f - g \in K \subseteq I.$$

Since $f \in I$, we also have $g \in I$, and since g is below α, we in fact have $g \in J$. In particular, $af \in \langle \alpha, J \rangle$. Since this is true for any $f \in I$, we conclude that $aI \subseteq \langle \alpha, J \rangle$. Now we use

Corollary 3 to conclude that

$$I^2 \subseteq \langle a, I\rangle I \subseteq \langle aI, e_1 I, \ldots, e_r I\rangle \subseteq \langle \alpha, J, e_1, \ldots, e_r\rangle \subseteq I.$$

Now take radicals to get

$$I \subseteq \sqrt{\langle a, I\rangle I} \subseteq \langle aI, e_1 I, \ldots, e_r I\rangle \subseteq \langle \alpha, J, e_1, \ldots, e_r\rangle \subseteq I,$$

which implies that all ideals in the above expression are equal. Since J is finite type, this implies that I is as well, which is a contradiction. □

References

[K] Irving Kaplansky, *An Introduction to Differential Algebra*, Publications de l'institut de mathématique de l'université de Nancago, 1957.