计算微分代数引论

liwei@mmrc.iss.ac.cn

40学时，9月10日－12月17日（12.10领试卷，12月17日交卷）

1. Basic notions of differential algebra
   - 1.1 Differential rings
   - 1.2 Differential ideals
   - 1.3 Decomposition of radical differential ideals
2. Differential polynomial rings and differential varieties
   - 2.1 Differential characteristic sets
   - 2.2 Ritt-Raudenbush basis theorem

3. Differential algebra-geometry dictionary
   - 3.1 Ideal-variety correspondence in differential algebra
   - 3.2 Differential Hilbert Nullstellensatz
   - 3.3 Irreducible decomposition of differential varieties

4. Extentions of differential fields
   - 4.1 Differential primitive theorem
   - 4.2 Differential transcendence degree
   - 4.3 Applications to differential varieties

5. Symbolic-integration for elementary funetions
   Liouville Theorem and its applications

6. Algorithms and problems in differential elimination theory

Text: 1. Lecture notes will be posted every Tuesday after class via http://mmrc.iss.ac.cn/~weili/ or group chat (wechat).

References (E-books will be given for reference when necessary):

« An introduction to differential algebra », I. Kaplansky, 1957.

« Differential algebra », J.F. Ritt, 1950

« Differential algebra and algebraic groups », E.R. Kolchin, 1973.

What is differential algebra? It is the subject studying algebraic differential equations from the algebraic standpoint.

Examples of algebraic differential equations:

1) $\frac{d^2y}{dt^2} + 2\frac{dy}{dt} + 5y = 0$ (linear ordinary differential equation)
2) $\left(\frac{dy}{dt}\right)^2 - 4y = 0$ (nonlinear ordinary differential equation)
3) Heat Equation: $\frac{\partial u}{\partial t} = \gamma\left(\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2}\right)$ (linear partial diff equation)
4) KDV Equation: $\frac{\partial u}{\partial t} - \frac{\partial^3 u}{\partial x^3} - 6u\frac{\partial u}{\partial x} = 0$ (nonlinear partial diff equation).

In differential algebra, we are not interested in "solving". In fact, it is very hard to solve differential equations in closed form solutions and in general impossible. Our perspective is rather to study the solutions and their properties from an abstract, purely algebraic point of view. This subject enjoys many analogies with commutative algebra and algebraic geometry. Since polynomial equations are algebraic differential equations of order 0, differential algebra could be regarded as a generalization of classical algebraic geometry.

The main focus of this course is to study the set of solutions of a general system of differential polynomials in finitely many differential variables over a differential field. These solution sets are called differential varieties.

We address questions like:

1) Can we replace an infinite system of algebraic differential equations by a finite system without changing the solutions? (Ritt-Raudenbush basis theorem)
2) Decompose a system of algebraic differential equations into finitely many "irreducible" system?
3) Give a criterion to test whether a system of differential equations have a solution or not (Differential Hilbert's Nullstellensatz).

Chapter 1. Basic notions of differential algebra

In this chapter, we introduce the very basic definitions and constructions of differential algebra and establish some first theorems concerning differential ideals.

1.1 Differential rings

All rings in this course are assumed to be commutative rings with unity 1.

Def 1.1 A **derivation** on a ring R is a map $\delta: R \to R$ s.t. for $\forall a, b \in R$,

1) $\delta(a+b) = \delta(a) + \delta(b)$;

2) (Leibniz rule) $\delta(ab) = \delta(a)b + a\delta(b)$.

In this case, the element $\delta(a)$ is called the **derivative** of a. Denote $\delta(a)$, $\delta^2(a)$ $\cdots$, $\delta^n(a)$ for the successive derivatives, by induction on n, we obtain

Leibniz rule: $\delta^n(ab) = \sum_{i=0}^{n} \binom{n}{i} \delta^{n-i}(a)\delta^i(b)$.

Clearly, 1) $\forall a \in R$, $\delta(a^n) = na^{n-1}\delta(a)$

2) $\delta(0) = \delta(0+0) = 2\delta(0) \Rightarrow \delta(0) = 0$

$\delta(1) = \delta(1^2) = 2\delta(1) \Rightarrow \delta(1) = 0 \Rightarrow \forall n \in \mathbb{Z}$, $\delta(n) = 0$.

3) If $a^{-1} \in R$, $\delta(1) = \delta(a \cdot a^{-1}) = \delta(a) \cdot a^{-1} + a\delta(a^{-1}) = 0 \Rightarrow \delta(a^{-1}) = -\frac{\delta(a)}{a^2}$.

Lemma 1.2 Let R be an integral domain and δ a derivation on R. Then δ has a unique extension to the quotient field $Frac(R)$.

proof. To show Existance. Define for each $\frac{a}{b} \in Frac(R)$,

$\delta\left(\frac{a}{b}\right) = \frac{\delta(a)b - a\delta(b)}{b^2}$ and show $\delta: Frac(R) \to Frac(R)$ is

① well-defined and ② it is a derivation.

① Suppose $\frac{a}{b} = \frac{c}{d} \Rightarrow ad = bc$ & $\delta(a)d + a\delta(d) = \delta(b)c + b\delta(c)$.

Show $\delta\left(\frac{a}{b}\right) = \frac{\delta(a)b - a\delta(b)}{b^2} \overset{?}{=} \delta\left(\frac{c}{d}\right) = \frac{\delta(c)d - c\delta(d)}{d^2}$.

② Show $\delta\left(\frac{a}{b} + \frac{c}{d}\right) = \delta\left(\frac{a}{b}\right) + \delta\left(\frac{c}{d}\right)$ & $\delta\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \delta\left(\frac{a}{b}\right)\frac{c}{d} + \frac{a}{b}\delta\left(\frac{c}{d}\right)$.

Uniqueness. $\forall \frac{a}{b} \in Frac(R)$, $\delta(a) = \delta\left(\frac{a}{b} \cdot b\right) = \delta\left(\frac{a}{b}\right)b + \frac{a}{b}\delta(b) \Rightarrow \delta\left(\frac{a}{b}\right) = \frac{b\delta(a) - a\delta(b)}{b^2}$. ∎

Def 1.3 A **differential ring** is a commutative ring R with unity 1 together with a finite set $\Delta=\{\delta_1,\cdots,\delta_m\}$ of mutually commuting derivation operators (i.e., $\forall a\in R$, $\delta_i(\delta_j(a))=\delta_j(\delta_i(a))$), denoted by (R,Δ).

If $\text{card}(\Delta)=1$ (i.e., $\Delta=\{\delta\}$), (R,δ) is called an ordinary differential ring.

If $\text{card}(\Delta)>1$, (R,Δ) is called a partial differential ring.

If R is also a field, (R,Δ) is called a differential field.

Examples

1) Let R be a commutative ring with unity. Define $\delta: R\to R$ by $\delta(a)=0$ for $\forall a\in R$. Then (R,δ) is a differential ring.

The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Z}_n$ have no other derivation operators than the zero derivation.

2) Let $R=\mathbb{Q}[x]$, $\delta(x)=1$. For any $a_0,a_1,\cdots,a_n\in\mathbb{Q}$,

$$\delta(a_0+a_1x+\cdots+a_nx^n)=\delta(a_0)+\delta(a_1x)+\cdots+\delta(a_nx^n)$$
$$=a_1+2a_2x+\cdots+na_nx^{n-1}.$$

(R,δ) is a differential ring.

3) Let F be a field of meromorphic functions of n complex variables $x_1,\cdots,x_n$ in a region of $\mathbb{C}^n$. Then $(F,\{\frac{\partial}{\partial x_1},\cdots,\frac{\partial}{\partial x_n}\})$ is a differential field.

4) If (S,δ) is an ordinary differential ring and $R=S[x]$, then for an arbitrary $f\in R$, $\delta(x)=f$ turns R into a differential ring.

But this notion of arbitrarily defining derivation doesn't work for the partial case.

Non-Example: $R=\mathbb{Q}[x]$. Let $\delta_1(x)=1$, $\delta_2(x)=x$. Since $\delta_1\delta_2(x)=1\neq\delta_2\delta_1(x)=0$, $(R,\{\delta_1,\delta_2\})$ is not a differential ring.

In this course, we focus on the ordinary differential case and for simplicity, we sometimes use "δ-" instead of "differential". Denote $\Theta=\{\delta^i\mid i\in\mathbb{N}\}$.

Definition 1.4. Let (R, δ) be a differential ring and $R_0 \subseteq R$ be a subring of R. If $\delta(R_0) \subseteq R_0$, then $(R_0, \delta|_{R_0})$ is a differential ring. In this case, we say R_0 a differential subring of R and say R a differential overring of R_0.

If $S \subseteq R$, there exists a smallest differential subring of R containing all the elts of R_0 and S, denoted by $R_0\{S\}$, and S is said to be a set of generators of the differential ring $R_0\{S\}$ over R_0. $R_0\{S\}$ coincides, as a ring, with the ring $R_0[(\delta^i s)_{s\in S, i\in\mathbb{N}}]$. A differential overring of a differential ring R_0 is said to be finitely generated over R_0 if it has a finite set of generators over R_0. If both R_0 and R are differential fields, R_0 is said to be a differential subfield of R and R is said to be a differential field extention of R_0.

Let L be a differential field extension of K and $S \subseteq L$. Denote by $K[S]$, $K\{S\}$, $K(S)$ and $K\langle S\rangle$ the smallest ring, the smallest differential ring, the smallest field, the smallest differential field containing K and S. Let $\Theta(S) = \{\delta^i(s) \mid i\in\mathbb{N}, s\in S\}$. Then $K\{S\} = K[\Theta(S)]$, $K\langle S\rangle = K(\Theta(S))$. L is said to be finitely generated if $\exists$ a finite subset $\{a_1, \cdots, a_n\} \subseteq L$ s.t. $L = K\langle a_1, \cdots, a_n\rangle$.

Def 1.5 Let (R, δ) be a differential ring. An elt $c\in R$ is said to be a <u>constant</u> if $\delta(c) = 0$. The set of all constants of R is a differential subring of R, called the <u>ring of constants of R</u>, denoted by C_R. If R is a differential field, C_R is a field, called the field of constants of R.

Examples: 1) $R = \mathbb{Q}[x]$, $\delta(x) = 1$. $C_R = \mathbb{Q}$.

2) $R = \mathbb{Z}_p(x^p)$, $\delta(x) = 1$. Then $C_R = R$.

Lemma 1.6 Let $(\mathcal{F}, \delta)$ be a differential field of char 0 and $C_{\mathcal{F}} = \mathcal{F}$. Let $L \supseteq \mathcal{F}$ be a differential field extension and L be algebraic over $\mathcal{F}$. Then $C_L = L$.

Proof. Let $a \in L$. Suppose $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathcal{F}[x]$ is the minimal poly of a. Then $\delta(p(a)) = \frac{\partial p}{\partial x}(a) \cdot \delta(a) + \sum_{i=0}^{n} \delta(a_i) a^i = \frac{\partial p}{\partial x}(a) \cdot \delta(a) = 0$.
Since $\mathrm{char}(\mathcal{F}) = 0$, $\frac{\partial p}{\partial x}(a) \neq 0$. Thus $\delta(a) = 0$. ∎

Remark: Let $L \supseteq \mathcal{F} \supseteq \mathbb{Q}$ and $a \in L$. If a is algebraic over $C_{\mathcal{F}}$, then $\delta(a) = 0$.

1.2. Differential ideals

Def 1.7. Let (R, δ) be a differential ring. An ideal $I \lhd R$ is a **differential ideal** if $\delta(I) \subseteq I$.

Example: Both $I = (0)$ and $I = R$ are differential ideals of R.

Prop 1.8 Let $I = (f_1, \cdots, f_s) \subseteq (R, \delta)$ be the ideal in (R, Δ) generated by $f_1, \cdots, f_s$. Then I is a differential ideal $\iff \forall\, i,\ \delta(f_i) \in I$.

Proof. "$\Rightarrow$" Trivial by definition.

"$\Leftarrow$" For each $f \in I$, $\exists\, g_1, \cdots, g_s \in R$ s.t. $f = g_1 f_1 + \cdots + g_s f_s$.

So $\delta(f) = \sum_{i=1}^{s} \delta(g_i) f_i + \sum_{i=1}^{s} \delta(f_i) g_i \in I$, for $\delta(f_i) \in I$ by hypothesis. Thus, $\delta(I) \subseteq I$. ∎

Notation. Let $S \subseteq (R, \Delta)$. We use $[S]$ to denote the smallest differential ideal of R generated by S. Clearly, $[S] = (\Theta(S)) = (\delta^i s : s \in S)$.

Example: Consider $(\mathbb{Q}[x], \delta)$ with $\delta(x) = 1$. Then $[0]$ and $\mathbb{Q}[x]$ are the only differential ideals in $\mathbb{Q}[x]$. (Indeed, Let $[0] \neq I \lhd \mathbb{Q}[x]$ be a differential ideal.

Then $\exists 0 \neq f \in \mathbb{Q}[x]$ s.t. $I = (f)$. Since I is a differential ideal, $\delta(f) = \frac{\partial f}{\partial x} \in (f)$. If $f \notin \mathbb{Q}$, $f \nmid \frac{\partial f}{\partial x}$. So, $f \in \mathbb{Q} \setminus \{0\}$ and $I = \mathbb{Q}[x]$ follows.)

An ideal $I \lhd (R, \delta)$ is called a radical (resp. prime) differential ideal if 1) $\delta(I) \subseteq I$, and
2) I is a radical ideal (resp. prime ideal).

Notation. Given $I \lhd R$, $\sqrt{I} = \{ f \in R \mid \exists n \in \mathbb{N} \text{ s.t. } f^n \in I \}$.

Given $S \subseteq (R, \Delta)$, Let $\{S\}$ be the smallest radical differential ideal containing S, and say $\{S\}$ is a radical differential ideal generated by S. (It will be clear in which context $\{\cdot\}$ denotes a radical differential ideal or a set).

Now, we turn to the construction of radical differential ideals. Normally, one may intuitively start with S, consider $[S]$ and then take its radical $\sqrt{[S]}$. However, this might not be sufficient.

Example. Let (R, δ) with $R = \mathbb{Z}_2[x, y]$, $\delta(x) = y$ and $\delta(y) = 0$. Consider $I = [x^2]$. Since $\delta(x^2) = 0$, $I = (x^2)$. So $\sqrt{I} = (x)$. But $\sqrt{I}$ is not a differential ideal, for $\delta(x) = y \notin \sqrt{I}$. So $\{x^2\} \neq \sqrt{[x^2]}$.

Exercise. Construct an example of an ideal $I \subseteq (R, \delta)$ s.t. $\sqrt{[I]}$ is not radical.
(Let $R = \mathbb{C}[x, y]$, $\delta(x) = y$ and $\delta(y) = 0$. Let $I = (xy)$. $\sqrt{I} = (xy)$, $[\sqrt{I}] = [xy] = (xy, y^2)$. $\bar{J} = [\sqrt{I}]$ is not radical for $y^2 \in J$ but $y \notin J$.)

Example. A maximal differential ideal (i.e., a maximal ett in the set of all proper differential ideals) is not necessarily prime. For example, let $R = \mathbb{Z}_2[x]$ with $\delta(x) = 1$. Let $J = [x^2] = (x^2)$. Clearly, J is not prime but J is a maximal differential ideal. Indeed, if $\exists\, I \lhd (R, \delta)$ with $J \subsetneq I \subseteq R$, then $\exists\, x + b \in I$. But $\delta(x + b) = 1 \in I$, so $I = R$.

However, if the ring R contains the rational field $\mathbb{Q}$, then the radical of a differential ideal is a radical differential ideal (i.e., $\{S\} = \sqrt{[S]}$).

Thm 1.9. Let (R, δ) be a differential ring, $\mathbb{Q} \subseteq R$ and let $I \subseteq (R, \delta)$ be a differential ideal. Then, $\sqrt{I}$ is a radical differential ideal.

Proof. It suffices to show $\sqrt{I}$ is a differential ideal. For this purpose, for each $a \in \sqrt{I}$ (i.e., $\exists a \in \mathbb{N}$, $a^n \in I$), to show $\delta(a) \in \sqrt{I}$.

Claim: For each k, $1 \le k \le n$, $a^{n-k}(\delta(a))^{2k-1} \in I$.

We show the claim by induction on k and $\delta(a) \in \sqrt{I}$ will follow by allowing $k = n$ $\left((\delta(a))^{2n-1} \in I \Rightarrow \delta(a) \in \sqrt{I}\right)$.

If $k = 1$, $\delta(a^n) = n a^{n-1} \delta(a) \in I$. Since $\mathbb{Q} \subseteq R$, $a^{n-1}\delta(a) \in I$.

Suppose $a^{n-k}(\delta(a))^{2k-1} \in I$ for some $1 \le k < n$. Then

$$\delta\left(a^{n-k}(\delta(a))^{2k-1}\right) = (n-k)a^{n-(k+1)}(\delta(a))^{2k} + a^{n-k}(2k-1)\delta(a)^{2k-2}\delta^2(a) \in I.$$

Multiply the above by $\delta(a)$, we get $a^{n-(k+1)}(\delta(a))^{2(k+1)-1} \in I$ and we are done. ∎