CIMAT

Centro de Investigación en Matemáticas, A.C.

Two applications of p-derivations in commutative algebra

I. Derivations

Def: A derivation on a ring R is a map $\partial : R \longrightarrow R$ s.t.

(1) $\partial(x+y) = \partial(x) + \partial(y)$ $\quad \forall x, y \in R$

(2) $\partial(xy) = x\partial(y) + y\partial(x)$

(1) means that ∂ is $\mathbb{Z}$-linear

Ex: If $R = A[x_1, \dots, x_n]$, then $\frac{\partial}{\partial x_i} : R \longrightarrow R$ "formal differentiation" is an A-linear derivation.

If A has char 0, $f \in A[\underline{x}]$, and $f \in (x_i^n) \setminus (x_i^{n+1})$ some $n > 0$, then $\frac{\partial}{\partial x_i}(f) \in (x_i^{n-1}) \setminus (x_i^n)$.

The conditions ②

(1) $\partial(x+y) = \partial(x) + \partial(y)$ $\forall x,y \in R$

(2) $\partial(xy) = x\partial(y) + y\partial(x)$

are linear in "∂", so

* the set of A-linear derivations is an R-module by postmultiplication
* can define $\partial : R \to M$ (R-module).

There is a universal object:

Kähler differentials

$$\begin{tikzcd} & \Omega_{R|A} \arrow[d, "\exists!\text{ linear map}"] \\ R \arrow[ur, "d_{R|A}"] \arrow[r, "\text{for any derivation}"'] & M \end{tikzcd} \rightsquigarrow \begin{array}{c} \mathrm{Der}_{R|A}(M) \\ \text{is} \\ \mathrm{Hom}_R(\Omega_{R|A}, M) \end{array}$$

Ex: 1) For $R = A[\underline{x}]$,

$$\mathrm{Der}_{R|A}(R) = \bigoplus R \cdot \frac{\partial}{\partial x_i}.$$

2) For $\dfrac{k[x,y,z]}{(x^2+y^2+z^2)}$ $\operatorname{char}(k)\neq 2$,

$$\operatorname{Der}_{R|k}(R) = R\left\langle x\frac{\partial}{\partial x}+y\frac{\partial}{\partial y}+z\frac{\partial}{\partial z},\ x\frac{\partial}{\partial y}-y\frac{\partial}{\partial x},\ y\frac{\partial}{\partial z}-z\frac{\partial}{\partial y},\ z\frac{\partial}{\partial x}-x\frac{\partial}{\partial z}\right\rangle.$$

No derivations that decrease degree or order; nothing like $\frac{\partial}{\partial x}$.

Thm [Nagata-Zariski-Lipman]: If $(R,\mathfrak{m})$ has equal char 0, $x\in\mathfrak{m}$, $\partial\in \operatorname{Der}(R)$ s.t. $\partial(x)=1$, then

$$\hat{R}\simeq R'[\![x]\!].$$

$\Rightarrow$ x is a formal reg. parameter.

II. p-derivations

Def [Joyal, Buium]: Let p a prime number, R a ring. A <u>p-derivation</u> on R is a map $\delta: R \longrightarrow R$ s.t.

$$(0) \quad \delta(1) = 0$$

$$(1) \quad \delta(x+y) = \delta(x) + \delta(y) - \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} x^i y^{p-i}$$

$$(2) \quad \delta(xy) = x^p \delta(y) + y^p \delta(x) + p\delta(x)\delta(y)$$

since $i!(p-i)! \mid (p-1)!$ for $0<i<p$, this is sensible in any characteristic.

Evidently, p-drivations are NOT $\mathbb{Z}$-linear / additive.

Moreover, those conditions are NOT linear in "δ," so

* cannot define p-der. $\delta : R \to M$ (M module)
* there is no analogue of Kähler differentials.

What do the axioms mean?

If $\delta : R \to R$ is a p-der.,
$\Phi : R \to R$ $\Phi(x) = x^p + p\,\delta(x)$ is a ring homomorphism s.t.

$$\begin{array}{ccc} R & \xrightarrow{\Phi} & R \\ \downarrow & & \downarrow \\ R/pR & \xrightarrow[x \mapsto x^p]{F} & R/pR \end{array}$$

commutes.

Such a Φ is a lift of Frobenius. (LOF)

If p is a reg. elt. on R, then this yields a bijection

$$\{p\text{-derivations}\} \longleftrightarrow \{\text{lifts of Frobenius}\}.$$

We will mostly be focused on this case (mixed characteristic).

Ex: 1) $R = \mathbb{Z}$

For any p, $\mathrm{id}_{\mathbb{Z}}$ is unique LOF,

so $\quad \delta_p(n) = \dfrac{n - n^p}{p}$ is unique p-der.

e.g., for $p=3$: $\quad 1 \longmapsto 0$

$2 \longmapsto -2$

$3 \longmapsto -8$

$4 \longmapsto -20$

2) $R = \widehat{\mathbb{Z}}_{(p)}$ p-adic integers

id is unique LOF,

unique p-der by same formula

3) [strict p-rings] If (V, pV, k) is a complete DVR with unif. p and k perfect, then V admits unique LOF / p-der.

4) Let A be a ring w/ p-der δ. Then for any $f_1, \ldots, f_n \in A[x_1, \ldots, x_n]$, $\exists!$ p-der on $A[\underline{x}]$ s.t.
$$\tilde{\delta}|_A = \delta, \quad \tilde{\delta}(x_i) = f_i.$$

For $f_1 = \cdots = f_n = 0$ call it std. extension, or std p-derivation.

e.g.: on $\mathbb{Z}[\underline{x}]$, std. p-derivation corresponds to LOF φ with $\varphi(x_i) = x_i^p$ all i, so

$$\delta(f(\underline{x})) = \frac{f(\underline{x}^p) - f(\underline{x})^p}{p}$$

"freshman's nightmare"

(0) $\delta(1) = 0$

(1) $\delta(x+y) = \delta(x) + \delta(y) - \sum_{i=1}^{p-1} \frac{(p-1)!}{i(p-i)!} x^i y^{p-i}$

(2) $\delta(xy) = x^p \delta(y) + y^p \delta(x) + p\delta(x)\delta(y)$

Prop: R ring with p-der δ, p ~~reg. elt.~~ prime elt. on R. Then for $f \in (p^n) \setminus (p^{n+1})$ some $n > 0$, $\delta(f) \in (p^{n-1}) \setminus (p^n)$.

pf: Any p-der restricts to a p-der on $\mathbb{Z}$, so $\delta(p) = 1 - p^{p-1}$.

(0) $\delta(1) = 0$

(1) $\delta(x+y) = \delta(x) + \delta(y) - \sum_{i=1}^{p-1} \frac{(p-1)!}{i!(p-i)!} x^i y^{p-i}$

(2) $\delta(xy) = x^p \delta(y) + y^p \delta(x) + p\delta(x)\delta(y)$

If $f = pg$, $g \in (p^{n-1}) \setminus (p^n)$.

$$\delta(f) = \delta(pg) = p^p \delta(g) + g^p \delta(p) + p\delta(p)\delta(g)$$
$$= p\,\delta(g) + g^p \delta(p).$$

ord_p:

If $n=1$, $\underbrace{p}_{1}\delta(g) + \underbrace{g^p}_{0}\underbrace{\delta(p)}_{0}$. $\rightsquigarrow 0$

If $n>1$, $\underbrace{p}_{1}\underbrace{\delta(g)}_{n-2} + \underbrace{g^p}_{p(n-1)}\delta(p)$. $\rightsquigarrow n-1$.

$\square$

$\rightsquigarrow$ might think of δ as like $\frac{\partial}{\partial p}$.

Ex: 5) If $\Delta \subseteq \mathbb{N}^n$ semigroup, $V[\Delta] \subseteq V[x]$ semigroup ring, standard LOF restricts to endo. of $V[\Delta]$, so std p-der. restricts to $V[\frac{1}{p}]$.

6) [Zdanowicz]: If $f \in V[x_1, \dots, x_n]$ is of degree $> n$, and $k[\underline{x}]/(f)$ is normal, then $V[\underline{x}]/(f)$ does not admit a p-derivation.

Call a map $\delta : R/p^n \to R/p^{n-1}$ satisfying p-derivation axioms a p-der mod p^n.

<u>Prop</u> [Zdanowicz]: Let $f \in V[\underline{x}]$, δ std p-der. on $V[\underline{x}]$.

$$\exists \ p\text{-der mod } p^2 \text{ on } \frac{V[\underline{x}]}{(f)} \iff \delta(f) \in (p, f, \underbrace{\left(\tfrac{\partial f}{\partial x_1}\right)^p, \dots, \left(\tfrac{\partial f}{\partial x_n}\right)^p}_{p^{th} \text{ powers of partials.}})$$

where do these show up?

Joyal: study Witt vectors

Buium: construction of arith
get space + intersection theory
⇒ explicit bounds on rat'l points

Bhatt-Scholze: certain data of ring
w/ p-der. "deperfection of
perfectoid ring"

Buium-Miller. Borger, Buium, Manin.

III. Jacobian criterion

Q: How do we find the singular locus of a k-algebra?

Given: • A ring

• $A[\underline{x}] = A[x_1, \ldots, x_n]$ poly ring/A

• $\underline{f} = f_1, \ldots, f_m \in A[\underline{x}]$

$$J(\underline{f}) := \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_1} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_1}{\partial x_n} & \cdots & \frac{\partial f_m}{\partial x_n} \end{bmatrix}$$ Jacobian matrix.

Then, if k perfect field, $R = k[\underline{x}]/I$, $I = (\underline{f})$ of pure ht h,

$$\mathrm{Sing}(R) = V(I_h(J(\underline{f})R))$$

In terms of Kähler differentials,

$$\Omega_{R|K} = \operatorname{coker}_R(J(\underline{f}))$$

Fitting ideals of $\Omega_{R|K}$ $\longleftrightarrow$ ideals of minors of $J(\underline{f})$

$\operatorname{Reg}(R) =$ locus where $\Omega_{R|K}$ is free of "correct" rank.

If we replace K by arb. ring A, the Jacobian criterion generalizes to detect smooth locus of $A \to R$.

Ex: $R = \dfrac{V[x,y]}{(p-xy)}$. R is not smooth over V: fiber over pV is $\dfrac{k[x,y]}{(xy)}$. (not regular)

But R is regular. $J(f) = \begin{bmatrix} -y \\ -x \end{bmatrix}$.

$$V(I_1(J(\underline{f}))) = V(x,y,p) = \{\mathfrak{m}\}$$

unique max'l ideal.

Q: How do we find the singular locus in mixed char.?

Given:
- A ring w/ p-der δ
- $A[\underline{x}]$ poly ring over A
- $\tilde{\delta}$ p-der extending δ (any).
- $\underline{f} = f_1, \ldots, f_m \in A[\underline{x}]$

$$J_{\tilde{\delta}}(\underline{f}) := \begin{bmatrix} \delta(f_1) & \cdots & \delta(f_m) \\ \left(\frac{\partial f_1}{\partial x_1}\right)^p & \cdots & \\ \vdots & \ddots & \\ & & \left(\frac{\partial f_m}{\partial x_n}\right)^p \end{bmatrix}$$

mixed Jacobian matrix.

Thm [Hochster–J]: Let V be a strict p-ring (e.g., $\widehat{\mathbb{Z}_{(p)}}$), $R = V[\underline{x}]/I$, $I = (\underline{f})$ of pure ht h, $\tilde{\delta}$ any p-der on $V[\underline{x}]$. Then,

$$\operatorname{Sing}(R) \setminus V(p) = V(I_h(J(\underline{f})R)) \setminus V(p)$$

$$\operatorname{Sing}(R) \cap V(p) = V(I_h(\tilde{J}_{\tilde{\delta}}(\underline{f})R)) \cap V(p).$$

__Ex:__ Let $R = \dfrac{V[x,y]}{(p-xy)}$. $\tilde{\delta}$ std. p-der on $V[x,y]$.

$$\tilde{\delta}(p-xy) = \frac{(p - x^p y^p) - (p-xy)^p}{p}$$

$$= 1 + \underline{\sum_{i=1}^{p} (-1)^{i+1} \binom{p}{i} (xy)^i p^{p-i-1}}$$

$$\tilde{J}_{\tilde{\delta}}(f) = \begin{bmatrix} \underline{\qquad\qquad} \\ -x^p \\ -y^p \end{bmatrix}$$

and $V(I_1(\widetilde{J}_{\widetilde{\delta}}(\underline{f})), p) = V(1) = \emptyset$,

$\Longrightarrow$ R is regular.

$$\operatorname{coker}_{R/pR}(\widetilde{J}_{\widetilde{\delta}}(\underline{f}))$$ is indep't of presentation $R = V[\underline{x}]/(\underline{f})$ and choice of $\widetilde{\delta}$ p-der. on V.

(compare with

$$\operatorname{coker}_R(J(\underline{f})) \simeq \Omega_{R/A}$$
)

$\to$ Represents a functor with properties akin to derivations, "perivations".

Idea of using p-der as "missing derivation" was used earlier to characterize $P^{(n)}$ a la Zariski-Nagata [De Stefani-Grifo-J].

IV. Direct summands

X_n^{gen} $n \times n$ generic matrix of vars / A

X_n^{sym} — " — symmetric — " —

X_n^{alt} — " — alternating — " —

$$R \hookrightarrow S$$

$$\frac{A[X_n^{gen}]}{\det(X)} \hookrightarrow A[Y_{n\times(n-1)}, Z_{(n-1)\times n}]$$
$$X \longmapsto YZ$$

$$\frac{A[X_n^{sym}]}{\det(X)} \hookrightarrow A[Y_{n\times(n-1)}]$$
$$X \longmapsto YY^T$$

$$\frac{A[X_{2n}^{alt}]}{\mathrm{pf}(X)} \hookrightarrow A[Y_{2n\times(2n-2)}]$$
$$X \longmapsto Y\Omega Y^T$$

If $A^\times$ infinite, then $R = S^G$ for $G = GL_{n-1}, O_{n-1}, Sp_{2n-2}$ resp.

These have many good properties over

$A \to$ char 0 field,

$\to$ " p " ,

$\to$ " $(0,p)$ DVR,

e.g., they are Cohen-Macaulay / pseudorational.

Deduce from different techniques:

* standard monomial theory / Hodge algebra [De Concini, Eisenbud, Procesi, ...]
* Over fields of char 0, the groups G admit averaging operators, so $R \hookrightarrow S$ splits as R-modules. (direct summands of poly rings) [Hilbert, Noether, Hochster-Roberts, ...]

In other characteristics, $R \hookrightarrow S$ do not split.

<u>Thm</u> [J-Singh]: For V strict p-ring, (e.g. $\mathbb{Z}_{(p)}$) the classical det'l hypersurfaces

$$\frac{V[X_n^{gen}]}{\det} \qquad \frac{V[X_n^{sym}]}{\det} \qquad \frac{V[X_{2n}^{alt}]}{pf}$$

$n \geq 3$ $\qquad$ $p=2$, $n \geq 3$ or $p \geq 3$, $n \geq 4$ $\qquad$ $n \geq 3$

are not ducks, i.e., are not direct summands of poly. rings by any embedding.

<u>Rmk</u>: Over $\mathbb{F}_p$, don't know for any of these.

<u>Sketch</u>: ✱ If $R \hookrightarrow S$ V-algebras

S has p-der mod p^2 &

$R \hookrightarrow S$ splits, then R has p-der. mod p^2.

* Use equational criterion to see that these classical det'l hypersurfaces do not. $\boxed{\text{L}}$

$\mathrm{Per} : R/pR\text{-mod} \longrightarrow R/pR\text{-mod}$

represented by $\operatorname{coker}(\widetilde{J}_\delta(\underline{f}))$

$$\operatorname{coker}(\widetilde{J}_\delta(\underline{f})) \simeq \widetilde{\Omega}_{R/V}.$$

$$\operatorname{Hom}_R(\widetilde{\Omega}_{R/V}, M) \simeq \mathrm{Per}(M)$$

$$\delta(pf) \equiv f^p \mod p.$$