“Linear” Wittferential Equations

Taylor Dupuy (w/Alexandru Buium)
Lubbock Texas - Central Sectional Meeting

PART 1

Wifferential Algebra

Fermat's Little Theorem

$\forall n \in \mathbb{Z}, \forall p$ prime

$$n \equiv n^p \mod p$$

Fermat's Little Theorem

$\forall n \in \mathbb{Z}, \forall p$ prime

$$n \equiv n^p \mod p$$

$$n - n^p = p \cdot \text{CRAP}$$

This is a p-derivation

$$\text{CRAP} = \frac{n - n^p}{p}$$

$$\delta_p(n) = \frac{n - n^p}{p}$$

$$\delta_p(n) = \frac{n - n^p}{p}$$

Zero mod p

Zero mod p

Decreases valuation:

$$\delta_p(p) = \frac{p - p^p}{p}$$
$$= 1 - p^{p-1}$$

$$\delta_p(p^m) = p^{m-1} \cdot \ (\text{ unit mod } p \ )$$

Decreases valuation:

$$\delta_t = \tfrac{d}{dt}$$
$$\delta_t(t^n) = n \cdot t^{n-1}$$

$$\delta_p(n) = \frac{n - n^p}{p}$$

Product Rule

$$\delta_p(ab) = \delta_p(a)b^p + a^p\delta_p(b) + p\delta_p(a)\delta_p(b)$$

Sum Rule

$$\delta_p(a+b) = \delta_p(a) + \delta_p(b) - \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j} a^{p-j} b^j$$

non-linear

Kills Unit

$$\delta(1) = 0$$

derivations ⟷ **ring homomorphisms**

$\delta : A \to A$ 　　　　 $f : A \to A[\varepsilon]/\langle\varepsilon^2\rangle$

$$A[\varepsilon]/\langle\varepsilon^2\rangle = \text{ ring of dual numbers}$$

$$(a_0 + \varepsilon a_1)(b_0 + \varepsilon b_1) \quad = \quad a_0 b_0 + \varepsilon(a_0 b_1 + b_0 a_1)$$

derivations ⟷ ring homomorphisms

$\delta : A \to A$ $\quad$ $f : A \to A[\varepsilon]/\langle \varepsilon^2 \rangle$

"dual numbers"

"infinitesimals"

p-derivations ⟷ ring homomorphisms

$\delta_p : A \to A$ $\quad$ $f : A \to W_1(A)$

"Witt vectors"

"wittfinitesimals"

"Wittferentiation"

Witt Vectors.

$$(x_0, x_1)(y_0, y_1) = (x_0 y_0, x_1 y_0^p + y_1 x_0^p + p x_1 y_1)$$

$$(x_0, x_1) + (y_0, y_1) = (x_0 + y_0, x_1 + y_1 + C_p(x_0, y_0))$$

$$C_p(X, Y) = \frac{X^p + Y^p - (X+Y)^p}{p} \in \mathbf{Z}[X, Y]$$

$$\delta_p(ab) = \delta_p(a) b^p + a^p \delta_p(b) + p \delta_p(a) \delta_p(b)$$

$$\delta_p(a + b) = \delta_p(a) + \delta_p(b) - \sum_{j=1}^{p-1} \frac{1}{p} \binom{p}{j} a^{p-j} b^j$$

$\phi : A \to B$

$\phi(a) \equiv a^p \mod p$

$\delta_p(a) := \frac{\phi(a) - a^p}{p}$

p-torsion free

lifts of the Frobenius $\approx$ p-derivations

$\delta_p : A \to B$ + rules

$\phi(a) := a^p + p\delta_p(a)$

Always an A-algebra

Defn. (Buium, Joyal)

A **p-derivation** is a map of sets $\delta_p : A \to B$ such that

$\forall a, b \in A$

$$\delta_p(ab) = \delta_p(a)b^p + a^p\delta_p(b) + p\delta_p(a)\delta_p(b)$$

$$\delta_p(a+b) = \delta_p(a) + \delta_p(b) - \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j} a^{p-j}b^j$$

EXAMPLES

example. $R = \mathbf{Z}_p$

$$\delta_p(x) = \frac{x - x^p}{p}$$

example. $R = \mathbf{Z}_p[\zeta]$

ζ = root of unity coprime to p

$$\delta_p(x) = \frac{\phi(x) - x^p}{p}$$

$\phi(x) =$ unique lift of the frobenius

$$= \begin{cases} \zeta \mapsto \zeta^p, & \text{on roots of unity} \\ identity, & \text{else} \end{cases}$$

example $\begin{aligned} R &= \mathbf{Z}_p^{ur} \\ &= \mathbf{Z}_p[\zeta : \zeta^n = 1, p \nmid 1] \end{aligned}$

$$\delta_p(x) = \frac{\phi(x) - x^p}{p}$$

Constants

Constants of a derivation:

(K, δ) (ring with der)

$K^\delta = \{c \in K : \delta(c) = 0\}$ (subring)

Constants of a p-derivation:

$R = \widehat{\mathbf{Z}}_p^{\mathrm{ur}}$ (ring with p-der)

$R^\delta = \{r \in R : \delta_p(r) = 0$ (submonoid)

$$R = \widehat{\mathbf{Z}}_p^{\mathrm{ur}}$$

Properties:

1) unramified CDVR, residue field $\overline{\mathbf{F}}_p$

2) $\widehat{\mathbf{Z}}_p^{\mathrm{ur}} = \mathbf{Z}_p[\zeta; \zeta^n = 1, p \nmid n]^{\widehat{}}$

3) unique lift of the Frobenius: $\exists ! \phi : R \to R$

$$\phi(\zeta) = \zeta^p$$

PART 2

“Linear” Wittferential Equations

Simplest Possible Equation:

$x = (x_{ij})$

$\alpha \in \mathrm{GL}_n(R)$

$$\delta x = \alpha x^{(p)}$$

$x^{(p)} = (x_{ij}^p)$

Remarks.

$x \mapsto \delta(x)(x^{(p)})^{-1}$ almost a cocycle

Theorem (existence and uniqueness)

$\alpha \in \mathfrak{gl}_n(R)$, $u_0 \in \mathrm{GL}_n(R)$

$$\begin{cases} \delta u = \alpha u^{(p)} \\ u \equiv u_0 \mod p \end{cases}$$

has a unique solution

$$\epsilon = 1 + p\alpha$$

proof.

$$\delta u = \alpha u^{(p)} \iff \phi(u) = \epsilon u^{(p)}$$

Contraction mapping: $f : \mathrm{GL}_n(R) \to \mathrm{GL}_n(R)$

$$f(x) = \phi^{-1}(\epsilon x^{(p)})$$

matrix norms

$$|x - y|_p \leq 1 \implies |f(x) - f(y)|_p \leq \frac{1}{p}|x - y|_p$$

$$u = \lim_{n\to\infty} f^n(u_0)$$

Theorem (coeffs in CDVR)

$$\begin{cases} \delta u = \alpha u^{(p)} \\ u \equiv u_0 \mod p \end{cases}$$

$\mathcal{O}$ = Complete Discrete Valuation Subring

$$u_0 \in \mathrm{GL}_n(\mathcal{O}) \text{ and } \alpha \in \mathfrak{gl}_n(\mathcal{O}) \implies u \in \mathrm{GL}_n(\mathcal{O})$$

Proof. $\mathcal{O} = R^{\phi^\nu}$ (characterization)

$\epsilon = 1 + p\alpha$

$$\phi^\nu(u_0) = u_0, \quad \phi^\nu(\alpha) = \alpha\,, \quad \phi^\nu(\epsilon) = \epsilon$$

$$\phi(u) = \epsilon u^{(p)}$$

$$\phi^{\nu+1}(u) = \phi^\nu(\epsilon u^{(p)})$$

$$\phi(\phi^\nu(u)) = \epsilon(\phi^\nu(u))^{(p)}$$

Theorem (coeffs in valuation delta subring)

$$\begin{cases} \delta u = \alpha u^{(p)} \\ u \equiv u_0 \mod p \end{cases}$$

$\mathcal{O}$ = valuation delta-subring

$$u_0 \in \mathrm{GL}_n(\mathcal{O}) \text{ and } \alpha \in \mathfrak{gl}_n(\mathcal{O}) \implies u \in \mathrm{GL}_n(\mathcal{O}')$$

$\mathcal{O}'/\mathcal{O}$ finite extension of delta-subrings

Strategy: reformulate as dynamics problem!!

Proof. $u_0, \alpha, \epsilon = 1 + p\alpha \in \mathfrak{gl}_n(\widehat{\mathcal{O}})$ ← complete

CDVR regularity Lemma $\implies \exists \nu \geq 0, \phi^{\nu}(u) = u$

Theorem (coeffs in valuation delta subring)

$$u_0 \in \mathrm{GL}_n(\mathcal{O}) \text{ and } \alpha \in \mathfrak{gl}_n(\mathcal{O}) \implies u \in \mathrm{GL}_n(\mathcal{O}')$$

$\mathcal{O}'/\mathcal{O}$ finite extension of delta-subrings

Strategy: reformulate as dynamics problem!!

$$\begin{aligned} u &= \phi^{\nu}(u) \\ &= \phi^{\nu-1}(\epsilon u^{(p)}) \\ &= \cdots \\ &= \phi^{\nu-1}(\epsilon)(\phi^{\nu-2}(\epsilon)(\cdots(\epsilon u^{(p)})\cdots)^{(p)})^{(p)} \end{aligned}$$

$w \in \mathrm{GL}_n(R)$ $\qquad$ $w_{(m)}$ = pick out mth column

properties

1) $(w^{(p)})_{(m)} = (w_{(m)})^{(p)}$

2) $(vw)_{(m)} = (vw_{(m)})$

Theorem (coeffs in valuation delta subring)

$$u_0 \in \mathrm{GL}_n(\mathcal{O}) \text{ and } \alpha \in \mathfrak{gl}_n(\mathcal{O}) \implies u \in \mathrm{GL}_n(\mathcal{O}')$$

Strategy: reformulate as dynamics problem!!

$$\begin{aligned} u &= \phi^{\nu}(u) \\ &= \phi^{\nu-1}(\epsilon u^{(p)}) \\ &= \cdots \\ &= \phi^{\nu-1}(\epsilon)(\phi^{\nu-2}(\epsilon)(\cdots(\epsilon u^{(p)})\cdots)^{(p)})^{(p)} \end{aligned}$$

properties

$$(w^{(p)})_{(m)} = (w_{(m)})^{(p)}$$

$$(vw)_{(m)} = (vw_{(m)})$$

$$u_{(m)} = \epsilon_{\nu-1}(\epsilon_{\nu-2}(\cdots(\epsilon u_{(m)}^{(p)})\cdots)^{(p)})^{(p)}$$

$$\varphi : \mathbf{A}^n_F \to \mathbf{A}^n_F$$

$$\varphi(\eta) = \epsilon_{\nu-1}(\epsilon_{\nu-2}(\cdots(\epsilon\eta^{(p)})\cdots)^{(p)})^{(p)}$$

$u_{(m)}$ **fixed point of** $\varphi : \mathbf{A}^n(K^a) \to \mathbf{A}^n(K^a)$

Theorem (coeffs in valuation delta subring)

$$u_0 \in \mathrm{GL}_n(\mathcal{O}) \text{ and } \alpha \in \mathfrak{gl}_n(\mathcal{O}) \implies u \in \mathrm{GL}_n(\mathcal{O}')$$

$$u_{(m)} = \epsilon_{\nu-1}(\epsilon_{\nu-2}(\cdots(\epsilon u_{(m)}^{(p)})\cdots)^{(p)})^{(p)}$$

Dynamics! $\varphi : \mathbf{A}_F^n \to \mathbf{A}_F^n$ $\qquad F = \mathrm{Frac}(\mathcal{O})$

$$\varphi(\eta) = \epsilon_{\nu-1}(\epsilon_{\nu-2}(\cdots(\epsilon\eta^{(p)})\cdots)^{(p)})^{(p)}$$

Lemma.

fixed points of

$$\varphi : \mathbf{A}^n(K^a) \to \mathbf{A}^n(K^a) < \infty$$

Theorem (coeffs in valuation delta subring)

$$u_0 \in \mathrm{GL}_n(\mathcal{O}) \text{ and } \alpha \in \mathfrak{gl}_n(\mathcal{O}) \implies u \in \mathrm{GL}_n(\mathcal{O}')$$

Lemma.

fixed points of

$$\varphi : \mathbf{A}^n(K^a) \to \mathbf{A}^n(K^a) < \infty$$

general principle:

$\varphi / F \implies$ fixed points of $\varphi : \mathbf{A}^n(K^a) \to \mathbf{A}^n(K^a)$

$\subset \mathbf{A}^n(F^a)$

$\implies$ columns are in finite algebraic extensions

Lemma. (Fornaes and Sibonay)

fixed points of

$$\varphi : \mathbf{A}^n(K^a) \to \mathbf{A}^n(K^a) < \infty$$

proof. $\varphi(x_1, \ldots, x_n) = (x_1, \ldots, x_n)$

homogenize

φ built from $\eta \mapsto e_j \eta$, $\eta \mapsto \eta^{(p)}$ $\rightsquigarrow$ $Y: \quad \varphi_j(x_1, \ldots, x_n) - x_0^{d-1} x_j = 0$

Claim

$Y \cap \{x_0 = 0\} = \emptyset$

$\implies Y$ zero dimensional in $\mathbf{P}^n$

$\implies$ fixed points of $\varphi : \mathbf{A}^n(K^a) \to \mathbf{A}^n(K^a)$ ={ (1,u) }

Galois Theory

$\mathcal{O} \subset R$, $\alpha \in \mathfrak{gl}_n(\mathcal{O})$

$$\delta u = \alpha u^{(p)}$$

$\mathcal{O}[u] = \mathcal{O}[u_{ij}]$ = Picard-Vessiot ring

= Ring obtained by adjoining entries of u

Galois Group

=

$$\{c \in \mathrm{GL}_n(\mathcal{O}) : \exists \sigma \in \mathrm{Aut}_{\mathcal{O}}(\mathcal{O}[u]), \sigma \circ \delta = \delta \circ \sigma, \sigma(u) = uc\}$$

$$G_{u/\mathcal{O}}$$

Galois Group of $\delta u = \alpha u^{(p)}$

=

$$\{c \in \mathrm{GL}_n(\mathcal{O}) : \exists \sigma \in \mathrm{Aut}_{\mathcal{O}}(\mathcal{O}[u]), \sigma \circ \delta = \delta \circ \sigma, \sigma(u) = uc\}$$

$$G_{u/\mathcal{O}}$$

Alternative Descriptions:

1) $\Gamma_{u/\mathcal{O}} = \{\sigma \in \mathrm{Aut}_{\mathcal{O}}(\mathcal{O}[u]); \sigma \circ \delta = \delta \circ \sigma \qquad \}$

$$\Gamma_{u/\mathcal{O}} \cong G_{u/\mathcal{O}}$$

2) $$0 \to I_{u/\mathcal{O}} \to \mathcal{O}[x, 1/\det(x)] \to \mathcal{O}[u] \to 0$$

$$\mathrm{Stab}_{\mathrm{GL}_n(R)}(I_{u/\mathcal{O}}) \cong G_{u/\mathcal{O}}$$

$$\delta u = \alpha u^{(p)}$$

Question: For what $c \in \mathrm{GL}_n(R)$ do we get

$$\delta(uc) = \alpha(uc)^{(p)} \text{ ?}$$

$$\delta(uc) = u^{(p)}\delta(c) + \delta(u)c^{(p)} + p\delta(u)\delta(c) + \{u, c\}^*$$

$$\{u, c\}^* = \frac{u^{(p)}c^{(p)} - (uc)^{(p)}}{p}$$

$\delta(uc) = u^{(p)}\delta(c) + \delta(u)c^{(p)} + p\delta(u)\delta(c) + \{u,c\}^*$ $\qquad$ $\{u,c\}^* = \frac{u^{(p)}c^{(p)} - (uc)^{(p)}}{p}$

Claim.

1) $\{u,c\}^* = 0$
2) $\delta c = 0$

$\Longrightarrow \quad \delta(uc) = \alpha(uc)^{(p)}$

Main Example:

subgroup of $\mathrm{GL}_n(\mathbf{F}_1^a)$

T = maximal torus of diagonals

W = permutation matrices

$N = WT = TW$

G^δ = matrices with roots of unity entries

$N^\delta = T^\delta W = WT^\delta$ = permutation matrices with roots of unity entries

Theorem.

$\mathcal{O} \subset R$ delta subring

$\mathcal{O} \subset R^{\phi^\nu}$ $\quad u \in \mathcal{O} \implies G_{u/\mathcal{O}}$ finite

$$\Gamma_{u/\mathcal{O}} = \{\sigma \in \mathrm{Aut}_{\mathcal{O}}(\mathcal{O}[u]); \sigma \circ \delta = \delta \circ \sigma \quad \}$$

$= G_{u/\mathcal{O}}$

finite to begin with

Theorem A.

$\exists \Omega \subset \mathbf{Q}^2$ "thin set"

$\forall \alpha \in \mathbf{Z}^2 \setminus \Omega$, $\exists u \in \mathrm{GL}_n(R)$ $\delta u = \alpha u^{(p)}$

$G_{u/\mathcal{O}}$ = finite group containing W

$\Omega \subset \mathbf{Z}^{n^2}$

Theorem B.

$$X = \{u \in \mathrm{GL}_n(R); u \equiv 1 \mod p\}$$

= ball around identity

$\exists \Omega \subset X$ of the second category

$\forall u \in X \setminus \Omega$, $\forall \mathcal{O} \subset R$ δ-closed subring

1) $\delta(u)(u^{(p)})^{-1} \in \mathfrak{gl}_n(\mathcal{O})$

2) $R^{\delta} \subset \mathcal{O}$

$$\Longrightarrow \quad G_{u/\mathcal{O}} = N^{\delta}$$

Theorem C.

$\exists \Omega \subset \mathrm{GL}_n(K^a)$ Zariski closed

$\forall u \in \mathrm{GL}_n(R) \setminus \Omega$

$$u' = \alpha u^{(p)}$$

$\mathcal{O} \ni \alpha$ δ-closed subring of R

$$\dim((Z \cdot G_{u/\mathcal{O}})^{\mathrm{Zar}}) \leq n$$