Testing the irreducibility of central differential operators with a local-to-global principle

JNCF 2026

Raphaël Pagès[1]

[1]Johannes Kepler Unversität
(Linz, Austria)

March 4, 2026

Algebra of differential operators

Object of study

Differential operators in $k(t)\langle\partial\rangle = \{a_n(t)\partial^n + \cdots + a_1(t)\partial + a_0(t)\}$.

Algebra of differential operators

Object of study

Differential operators in $k(t)\langle\partial\rangle = \{a_n(t)\partial^n + \cdots + a_1(t)\partial + a_0(t)\}$.

Commutation rule:

$$\partial f = f\partial + f'$$

Derivation:

$$f' = \frac{\mathrm{d}}{\mathrm{d}t}f$$

Algebra of differential operators

Object of study

Differential operators in $k(t)\langle\partial\rangle = \{a_n(t)\partial^n + \cdots + a_1(t)\partial + a_0(t)\}$.

Commutation rule:

$$\partial f = f\partial + f'$$

Derivation:

$$f' = \frac{\mathrm{d}}{\mathrm{d}t} f$$

Central operators: which commute t and ∂

Algebra of differential operators

Object of study

Differential operators in $k(t)\langle\partial\rangle = \{a_n(t)\partial^n + \cdots + a_1(t)\partial + a_0(t)\}$.

Commutation rule:

$$\partial f = f\partial + f'$$

Derivation:

$$f' = \frac{\mathrm{d}}{\mathrm{d}t} f$$

Central operators: which commute t and ∂

$$Lt = tL + \frac{\mathrm{d}}{\mathrm{d}\partial} L \qquad \partial L = L\partial + \frac{\mathrm{d}}{\mathrm{d}t} L$$

Algebra of differential operators

Object of study

Differential operators in $k(t)\langle\partial\rangle = \{a_n(t)\partial^n + \cdots + a_1(t)\partial + a_0(t)\}$.

Commutation rule:

$$\partial f = f\partial + f'$$

Derivation:

$$f' = \frac{\mathrm{d}}{\mathrm{d}t}f$$

Central operators: which commute t and ∂

$$Lt = tL + \frac{\mathrm{d}}{\mathrm{d}\partial}L \qquad \partial L = L\partial + \frac{\mathrm{d}}{\mathrm{d}t}L$$

If k is a field of characteristic p, $k(t^p)[\partial^p]$ is the center.

Why are central operators interesting ?

Fact:

There exists a unique map $\mathcal{N} : \mathbb{F}_q(t)\langle\partial\rangle \to \mathbb{F}_q(t^p)[\partial^p]$ such that:

Why are central operators interesting ?

Fact:

There exists a unique map $\mathcal{N} : \mathbb{F}_q(t)\langle\partial\rangle \to \mathbb{F}_q(t^p)[\partial^p]$ such that:

- $\mathcal{N}$ is multiplicative
- $\mathcal{N}_{|\mathbb{F}_q(t^p)[\partial^p]}$ is the Frobenius endomorphism.
- $L|\mathcal{N}(L)$

Why are central operators interesting ?

Fact:

There exists a unique map $\mathcal{N} : \mathbb{F}_q(t)\langle\partial\rangle \to \mathbb{F}_q(t^p)[\partial^p]$ such that:

- $\mathcal{N}$ is multiplicative
- $\mathcal{N}_{|\mathbb{F}_q(t^p)[\partial^p]}$ is the Frobenius endomorphism.
- $L|\mathcal{N}(L)$

If $N(t^p, \partial^p)$ is a non trivial factor of $\mathcal{N}(L)$ then $\mathrm{GCRD}(N(t^p, \partial^p), L) \neq 1$.

Why are central operators interesting ?

Fact:

There exists a unique map $\mathcal{N} : \mathbb{F}_q(t)\langle\partial\rangle \to \mathbb{F}_q(t^p)[\partial^p]$ such that:

- $\mathcal{N}$ is multiplicative
- $\mathcal{N}_{|\mathbb{F}_q(t^p)[\partial^p]}$ is the Frobenius endomorphism.
- $L | \mathcal{N}(L)$

If $N(t^p, \partial^p)$ is a non trivial factor of $\mathcal{N}(L)$ then $\mathrm{GCRD}(N(t^p, \partial^p), L) \neq 1$.

Assumption:

$L \in \mathbb{F}_q(t)\langle\partial\rangle$ is a divisor of $N(t^p, \partial^p)$ where $N \in \mathbb{F}_q[X, Y]$ is irreducible.

State of the art on factorisation

- M. van der Put. Modular methods for factoring differential operators. Unpublished manuscript, 1997.
- M. Giesbrecht, Y. Zhang, Factoring and decomposing Ore polynomials over $\mathbb{F}_p(t)$, ISSAC 2003.
- T. Cluzeau, factorisation of differential systems in characteristic p, ISSAC 2003.
- J. Gomez-Torrecillas, F. J. Lobillo, G. Navarro, Computing the bound of an Ore polynomial. Applications to factorisation, JSC 2019.

Parametrizing irreducible divisors

Notation

- Let y_N be a root of $N(x^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.

Parametrizing irreducible divisors

Notation

- Let y_N be a root of $N(x^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.

Parametrizing irreducible divisors

Notation

- Let y_N be a root of $N(x^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.

Theorem (van der Put)

If $N(t^p, \partial^p)$ is reducible, the irreducible divisors of $N(t^p, \partial^p)$ are parametrized by the solutions of

$$f^{(p-1)} + f^p = y_N$$

in K_N. If $N(t^p, \partial^p)$ is irreducible then this equation has no solution in K_N.

Parametrizing irreducible divisors

Notation

- Let y_N be a root of $N(x^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.

Theorem (van der Put)

If $N(t^p, \partial^p)$ is reducible, the irreducible divisors of $N(t^p, \partial^p)$ are parametrized by the solutions of

$$f^{(p-1)} + f^p = y_N$$

in K_N. If $N(t^p, \partial^p)$ is irreducible then this equation has no solution in K_N.

Theorem (van der Put)

Let L be a non trivial divisor of $N(t^p, \partial^p)$ and
$\mathrm{GCRD}(L, \partial^p - y_N) = \partial^m + l_{m-1}\partial^{m-1} + \cdots + l_0 \in K_N\langle\partial\rangle$. *Then*

$$l_{m-1}^{(p-1)} + l_{m-1}^p = -m y_N.$$

Theorem (Pagès 2024)

Let S be a set a places of K_N generating $\mathrm{Pic}(K_N)/p\mathrm{Pic}(K_N)$.
If $N(t^p, \partial^p)$ is reducible then a solution of $f^{(p-1)} + f^p = y_N$ lives in the Riemann-Roch space

$$\mathcal{L}\Big(\max\Big(\sum_{\mathfrak{P}\in S}\mathfrak{P} + \mathrm{Diff}(K_N) - 2(t)_\infty, p^{-1}\cdot(y_N)_\infty\Big)\Big)$$

Problem: Computing $\mathrm{Pic}(K_N)/p\mathrm{Pic}(K_N)$ is hard !

The Brauer group

Definition

Let K be a field. The Brauer group of K, $\mathrm{Br}(K)$, is a commutative group

The Brauer group

Definition

Let K be a field. The Brauer group of K, $\mathrm{Br}(K)$, is a commutative group whose underlying set is a set of equivalence classes of finite dimensional central simple K-algebras such that

The Brauer group

Definition

Let K be a field. The Brauer group of K, $\mathrm{Br}(K)$, is a commutative group whose underlying set is a set of equivalence classes of finite dimensional central simple K-algebras such that

- If $A \simeq B$ then $\overline{A} = \overline{B}$ in $\mathrm{Br}(K)$

The Brauer group

Definition

Let K be a field. The Brauer group of K, $\mathrm{Br}(K)$, is a commutative group whose underlying set is a set of equivalence classes of finite dimensional central simple K-algebras such that

- If $A \simeq B$ then $\bar{A} = \bar{B}$ in $\mathrm{Br}(K)$
- $\overline{M_n(A)} = \overline{M_m(A)}$ in $\mathrm{Br}(K)$ for all m, n.

The Brauer group

Definition

Let K be a field. The Brauer group of K, $\mathrm{Br}(K)$, is a commutative group whose underlying set is a set of equivalence classes of finite dimensional central simple K-algebras such that

- If $A \simeq B$ then $\overline{A} = \overline{B}$ in $\mathrm{Br}(K)$
- $\overline{M_n(A)} = \overline{M_m(A)}$ in $\mathrm{Br}(K)$ for all m, n.

The multiplication is given by the tensor product

The Brauer group

Definition

Let K be a field. The Brauer group of K, $\mathrm{Br}(K)$, is a commutative group whose underlying set is a set of equivalence classes of finite dimensional central simple K-algebras such that

- If $A \simeq B$ then $\overline{A} = \overline{B}$ in $\mathrm{Br}(K)$
- $\overline{M_n(A)} = \overline{M_m(A)}$ in $\mathrm{Br}(K)$ for all m, n.

The multiplication is given by the tensor product, the neutral is the equivalence class of matrix rings

The Brauer group

Definition

Let K be a field. The Brauer group of K, $\mathrm{Br}(K)$, is a commutative group whose underlying set is a set of equivalence classes of finite dimensional central simple K-algebras such that

- If $A \simeq B$ then $\bar{A} = \bar{B}$ in $\mathrm{Br}(K)$
- $\overline{M_n(A)} = \overline{M_m(A)}$ in $\mathrm{Br}(K)$ for all m, n.

The multiplication is given by the tensor product, the neutral is the equivalence class of matrix rings and the inverse of A is A^{op}.

The Brauer group

Definition

Let K be a field. The Brauer group of K, $\mathrm{Br}(K)$, is a commutative group whose underlying set is a set of equivalence classes of finite dimensional central simple K-algebras such that

- If $A \simeq B$ then $\overline{A} = \overline{B}$ in $\mathrm{Br}(K)$
- $\overline{M_n(A)} = \overline{M_m(A)}$ in $\mathrm{Br}(K)$ for all m, n.

The multiplication is given by the tensor product, the neutral is the equivalence class of matrix rings and the inverse of A is A^{op}.

A a central simple K-algebra of dimension n^2.

The Brauer group

Definition

Let K be a field. The Brauer group of K, $\mathrm{Br}(K)$, is a commutative group whose underlying set is a set of equivalence classes of finite dimensional central simple K-algebras such that

- If $A \simeq B$ then $\overline{A} = \overline{B}$ in $\mathrm{Br}(K)$
- $\overline{M_n(A)} = \overline{M_m(A)}$ in $\mathrm{Br}(K)$ for all m, n.

The multiplication is given by the tensor product, the neutral is the equivalence class of matrix rings and the inverse of A is A^{op}.

A a central simple K-algebra of dimension n^2.

$A \simeq M_n(K)$ iff $\overline{A} = 0$ in $\mathrm{Br}(K)$

The Brauer group

Theorem

Let K be a global field,

A a central simple K-algebra of dimension n^2.

$A \simeq M_n(K)$ iff $\overline{A} = 0$ in $\mathrm{Br}(K)$

The Brauer group

Theorem

Let K be a global field, S the set of its places

A a central simple K-algebra of dimension n^2.

$A \simeq M_n(K)$ iff $\overline{A} = 0$ in $\mathrm{Br}(K)$

The Brauer group

Theorem

Let K be a global field, S the set of its places and $K_{\mathfrak{P}}$ denote the completion of K in $\mathfrak{P}$ for any $\mathfrak{P} \in S$.

A a central simple K-algebra of dimension n^2.

$A \simeq M_n(K)$ iff $\overline{A} = 0$ in $\mathrm{Br}(K)$

The Brauer group

Theorem

Let K be a global field, S the set of its places and $K_{\mathfrak{P}}$ denote the completion of K in $\mathfrak{P}$ for any $\mathfrak{P} \in S$. The map

$$\begin{array}{rcl} \mathrm{Br}(K) & \to & \bigoplus_{\mathfrak{P}\in S} \mathrm{Br}(K_{\mathfrak{P}}) \\ \bar{A} & \mapsto & (\overline{A \otimes_K K_{\mathfrak{P}}})_{\mathfrak{P}} \end{array}$$

is injective.

A a central simple K-algebra of dimension n^2.

$A \simeq M_n(K)$ iff $\bar{A} = 0$ in $\mathrm{Br}(K)$

The Brauer group

Theorem

Let K be a global field, S the set of its places and $K_{\mathfrak{P}}$ denote the completion of K in $\mathfrak{P}$ for any $\mathfrak{P} \in S$. The map

$$\begin{array}{rcl} \mathrm{Br}(K) & \rightarrow & \bigoplus_{\mathfrak{P}\in S} \mathrm{Br}(K_{\mathfrak{P}}) \\ \bar{A} & \mapsto & (\overline{A \otimes_K K_{\mathfrak{P}}})_{\mathfrak{P}} \end{array}$$

is injective.

A a central simple K-algebra of dimension n^2.

$A \simeq M_n(K)$ iff $\overline{A \otimes_K K_{\mathfrak{P}}} = 0$ in $\mathrm{Br}(K_{\mathfrak{P}})$ for all $\mathfrak{P}$.

The Brauer group

Theorem

Let K be a global field, S the set of its places and $K_{\mathfrak{P}}$ denote the completion of K in $\mathfrak{P}$ for any $\mathfrak{P} \in S$. The map

$$\begin{array}{ccc} \mathrm{Br}(K) & \to & \bigoplus_{\mathfrak{P}\in S} \mathrm{Br}(K_{\mathfrak{P}}) \\ \bar{A} & \mapsto & (\overline{A \otimes_K K_{\mathfrak{P}}})_{\mathfrak{P}} \end{array}$$

is injective.

A a central simple K-algebra of dimension n^2.

$A \simeq M_n(K)$ iff $A \otimes_K K_{\mathfrak{P}} \simeq M_n(K_{\mathfrak{P}})$ for all $\mathfrak{P}$.

A central simple algebra

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.

A central simple algebra

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.
- $\mathcal{D}_N = \mathbb{F}_q(t)\langle\partial\rangle / N(t^p, \partial^p)$

A central simple algebra

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.
- $\mathcal{D}_N = \mathbb{F}_q(t)\langle\partial\rangle / N(t^p, \partial^p)$

Fact (van der Put, Jacobson?)

$\mathcal{D}_N$ is a central simple C_N-algebra of dimension p^2.

A central simple algebra

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.
- $\mathcal{D}_N = \mathbb{F}_q(t)\langle\partial\rangle / N(t^p, \partial^p)$

Fact (van der Put, Jacobson?)

$\mathcal{D}_N$ is a central simple C_N-algebra of dimension p^2.

Corollary (Wedderburn)

$\mathcal{D}_N$ is either

A central simple algebra

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.
- $\mathcal{D}_N = \mathbb{F}_q(t)\langle\partial\rangle / N(t^p, \partial^p)$

Fact (van der Put, Jacobson?)

$\mathcal{D}_N$ is a central simple C_N-algebra of dimension p^2.

Corollary (Wedderburn)

$\mathcal{D}_N$ is either

- A division algebra

A central simple algebra

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.
- $\mathcal{D}_N = \mathbb{F}_q(t)\langle\partial\rangle / N(t^p, \partial^p)$

Fact (van der Put, Jacobson?)

$\mathcal{D}_N$ is a central simple C_N-algebra of dimension p^2.

Corollary (Wedderburn)

$\mathcal{D}_N$ is either

- A division algebra$\Leftrightarrow$ $N(t^p, \partial^p)$ is irreducible

A central simple algebra

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.
- $\mathcal{D}_N = \mathbb{F}_q(t)\langle\partial\rangle / N(t^p, \partial^p)$

Fact (van der Put, Jacobson?)

$\mathcal{D}_N$ is a central simple C_N-algebra of dimension p^2.

Corollary (Wedderburn)

$\mathcal{D}_N$ is either

- A division algebra$\Leftrightarrow$ $N(t^p, \partial^p)$ is irreducible
- Isomorphic to $M_p(C_N)$

A central simple algebra

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.
- $\mathcal{D}_N = \mathbb{F}_q(t)\langle\partial\rangle / N(t^p, \partial^p)$

Fact (van der Put, Jacobson?)

$\mathcal{D}_N$ is a central simple C_N-algebra of dimension p^2.

Corollary (Wedderburn)

$\mathcal{D}_N$ is either

- A division algebra$\Leftrightarrow$ $N(t^p, \partial^p)$ is irreducible
- Isomorphic to $M_p(C_N)$$\Leftrightarrow$ $N(t^p, \partial^p)$ is reducible

The p-Riccati equation

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.
- $\mathcal{D}_N = \mathbb{F}_q(t)\langle\partial\rangle / N(t^p, \partial^p)$

The p-Riccati equation

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.
- $\mathcal{D}_N = \mathbb{F}_q(t)\langle\partial\rangle / N(t^p, \partial^p)$

Theorem (van der Put)

$N(t^p, \partial^p)$ is reducible iff the equation $f^{(p-1)} + f^p = y_N$ has a solution in K_N

The p-Riccati equation

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.
- $\mathcal{D}_N = \mathbb{F}_q(t)\langle\partial\rangle / N(t^p, \partial^p)$

Theorem (van der Put)

$N(t^p, \partial^p)$ is reducible iff the equation $f^{(p-1)} + f^p = y_N$ has a solution in K_N

$$\begin{tikzcd}
N(t^p,\partial^p) \text{ reducible} \arrow[r, leftrightarrow] \arrow[dr, leftrightarrow] & \mathcal{D}_N \simeq M_p(C_N) \arrow[d, leftrightarrow] \\
& \begin{array}{c} f^{(p-1)}+f^p=y_N \\ \text{has a solution in } K_N \end{array}
\end{tikzcd}$$

The p-Riccati equation

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.
- $\mathcal{D}_N = \mathbb{F}_q(t)\langle\partial\rangle / N(t^p, \partial^p)$

Theorem (van der Put)

$N(t^p, \partial^p)$ is reducible iff the equation $f^{(p-1)} + f^p = y_N$ has a solution in K_N

$$\begin{tikzcd}
N(t^p,\partial^p) \text{ reducible} \arrow[r, leftrightarrow] \arrow[dr, leftrightarrow] & \mathcal{D}_N \simeq M_p(C_N) \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & \mathcal{D}_N \otimes_{C_N} C_{N,\mathfrak{P}} \simeq M_p(C_{N,\mathfrak{P}}) \text{ for all } \mathfrak{P} \\
 & \begin{array}{c} f^{(p-1)}+f^p=y_N \\ \text{has a solution in } K_N \end{array} &
\end{tikzcd}$$

The p-Riccati equation

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.
- $\mathcal{D}_N = \mathbb{F}_q(t)\langle\partial\rangle / N(t^p, \partial^p)$

Theorem (van der Put)

$N(t^p, \partial^p)$ is reducible iff the equation $f^{(p-1)} + f^p = y_N$ has a solution in K_N

$$
\begin{tikzcd}
N(t^p,\partial^p) \text{ reducible} \arrow[r, leftrightarrow] \arrow[dr, leftrightarrow] & \mathcal{D}_N \simeq M_p(C_N) \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & \mathcal{D}_N \otimes_{C_N} C_{N,\mathfrak{P}} \simeq M_p(C_{N,\mathfrak{P}}) \text{ for all } \mathfrak{P} \arrow[d, leftrightarrow] \\
 & \substack{f^{(p-1)}+f^p=y_N \\ \text{has a solution in } K_N} & \substack{f^{(p-1)}+f^p=y_N \\ \text{has a solution in } K_{N,\mathfrak{P}}} \text{ for all } \mathfrak{P}
\end{tikzcd}
$$

The p-Riccati equation

Notation

- Let y_N be a root of $N(t^p, Y)$ in a separable closure of $\mathbb{F}_q(t)$.
- $C_N = \mathbb{F}_q(t^p)[y_N]$, $K_N = \mathbb{F}_q(t)[y_N]$.
- $\mathcal{D}_N = \mathbb{F}_q(t)\langle\partial\rangle / N(t^p, \partial^p)$

Theorem (van der Put)

$N(t^p, \partial^p)$ is reducible iff the equation $f^{(p-1)} + f^p = y_N$ has a solution in K_N

$$\begin{tikzcd}
N(t^p,\partial^p) \text{ reducible} \arrow[r, leftrightarrow] \arrow[dr, leftrightarrow] & \mathcal{D}_N \simeq M_p(C_N) \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & \mathcal{D}_N \otimes_{C_N} C_{N,\mathfrak{P}} \simeq M_p(C_{N,\mathfrak{P}}) \text{ for all } \mathfrak{P} \arrow[d, leftrightarrow] \\
 & \substack{f^{(p-1)}+f^p=y_N \\ \text{has a solution in } K_N} \arrow[r, leftrightarrow] & \substack{f^{(p-1)}+f^p=y_N \\ \text{has a solution in } K_{N,\mathfrak{P}}} \text{ for all } \mathfrak{P}
\end{tikzcd}$$

A Hensel lemma

Want to solve $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N$ in some $\mathbb{F}_{q'}((T))$.

A Hensel lemma

Want to solve $\left(T'\frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N$ in some $\mathbb{F}_{q'}((T))$.

Notation

- $\nu : \mathbb{F}_{q'}((T)) \to \mathbb{Z}$ the canonical valuation.

A Hensel lemma

Want to solve $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N$ in some $\mathbb{F}_{q'}((T))$.

Notation

- $\nu : \mathbb{F}_{q'}((T)) \to \mathbb{Z}$ the canonical valuation.
- $e := 1 - \nu(T')$

A Hensel lemma

Want to solve $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N$ in some $\mathbb{F}_{q'}((T))$.

Notation

- $\nu : \mathbb{F}_{q'}((T)) \to \mathbb{Z}$ the canonical valuation.
- $e := 1 - \nu(T')$

Remember that $\mathbb{F}_{q'}((T))$ is the completion of K_N in a place $\mathfrak{P}$. If $\mathfrak{P}$ is tamely ramified, e is the ramification index of $\mathfrak{P}$.

A Hensel lemma

Want to solve $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N$ in some $\mathbb{F}_{q'}((T))$.

Notation

- $\nu : \mathbb{F}_{q'}((T)) \to \mathbb{Z}$ the canonical valuation.
- $e := 1 - \nu(T')$

Lemma

Let $f_0 \in \mathbb{F}_{q'}((T))$ be such that $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f_0 + f_0^p = y_N + O(T^{pn})$.

A Hensel lemma

Want to solve $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N$ in some $\mathbb{F}_{q'}((T))$.

Notation

- $\nu : \mathbb{F}_{q'}((T)) \to \mathbb{Z}$ the canonical valuation.
- $e := 1 - \nu(T')$

Lemma

Let $f_0 \in \mathbb{F}_{q'}((T))$ be such that $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f_0 + f_0^p = y_N + O(T^{pn})$. There exists $f_1 \in \mathbb{F}_{q'}((T))$ such that

- $f_1 = f_0 + O(T^{pn+(p-1)e})$.

A Hensel lemma

Want to solve $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N$ in some $\mathbb{F}_{q'}((T))$.

Notation

- $\nu : \mathbb{F}_{q'}((T)) \to \mathbb{Z}$ the canonical valuation.
- $e := 1 - \nu(T')$

Lemma

Let $f_0 \in \mathbb{F}_{q'}((T))$ be such that $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f_0 + f_0^p = y_N + O(T^{pn})$. There exists $f_1 \in \mathbb{F}_{q'}((T))$ such that

- $f_1 = f_0 + O(T^{pn+(p-1)e})$.
- $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f_1 + f_1^p = y_N + O(T^{p(pn+(p-1)e)})$.

Reduction to the poles of t and y_N

Corollary

If $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N + O(T^{p\nu(T')})$ *has a solution in* $\mathbb{F}_{q'}((T))$ *then* $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N$ *has a solution in* $\mathbb{F}_{q'}((T))$.

Reduction to the poles of t and y_N

Corollary

If $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N + O(T^{p\nu(T')})$ *has a solution in* $\mathbb{F}_{q'}((T))$ *then* $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N$ *has a solution in* $\mathbb{F}_{q'}((T))$.

In particular if $p^{-1} \cdot \nu(y_N) \geqslant \nu(T')$ *then a solution exists.*

Reduction to the poles of t and y_N

Corollary

If $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N + O(T^{p\nu(T')})$ *has a solution in* $\mathbb{F}_{q'}((T))$ *then* $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N$ *has a solution in* $\mathbb{F}_{q'}((T))$.

In particular if $p^{-1} \cdot \nu(y_N) \geqslant \nu(T')$ *then a solution exists.*

Corollary

The equation $f^{(p-1)} + f^p = y_N$ *has a solution in* $K_{N,\mathfrak{P}}$ *for all places* $\mathfrak{P}$ *which are not poles of* y_N *or infinity places.*

Reduction to the poles of t and y_N

Corollary

If $\left(T'\frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)}f+f^p=y_N+O(T^{p\nu(T')})$ *has a solution in* $\mathbb{F}_{q'}((T))$ *then* $\left(T'\frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)}f+f^p=y_N$ *has a solution in* $\mathbb{F}_{q'}((T))$.

In particular if $p^{-1}\cdot\nu(y_N)\geqslant\nu(T')$ *then a solution exists.*

Corollary

The equation $f^{(p-1)}+f^p=y_N$ *has a solution in* $K_{N,\mathfrak{P}}$ *for all places* $\mathfrak{P}$ *which are not poles of* y_N *or infinity places.*

For the remaining places checking the existence of a solution is a matter of solving a non invertible linear system of $(\nu(T')-p^{-1}\cdot\nu(y_N))\log_p(q')$ *equations in just as many variables.*

A polynomial time irreducibility test

Input: $N \in \mathbb{F}_q[X, Y]$ separable and irreducible.

A polynomial time irreducibility test

Input: $N \in \mathbb{F}_q[X, Y]$ separable and irreducible.
Output: Is $N^p(t, \partial)$ irreducible in $\mathbb{F}_q(t)\langle\partial\rangle$.

A polynomial time irreducibility test

Input: $N \in \mathbb{F}_q[X, Y]$ separable and irreducible.
Output: Is $N^p(t, \partial)$ irreducible in $\mathbb{F}_q(t)\langle\partial\rangle$.

- Set a a root of $N(t, Y)$ in a separable closure of $\mathbb{F}_q(t)$, $K_N = \mathbb{F}_q(t)[a]$.

A polynomial time irreducibility test

Input: $N \in \mathbb{F}_q[X, Y]$ separable and irreducible.
Output: Is $N^p(t, \partial)$ irreducible in $\mathbb{F}_q(t)\langle\partial\rangle$.

- Set a a root of $N(t, Y)$ in a separable closure of $\mathbb{F}_q(t)$, $K_N = \mathbb{F}_q(t)[a]$.
- Let S be the set of poles of a and infinity places.

A polynomial time irreducibility test

Input: $N \in \mathbb{F}_q[X, Y]$ separable and irreducible.
Output: Is $N^p(t, \partial)$ irreducible in $\mathbb{F}_q(t)\langle\partial\rangle$.

- Set a a root of $N(t, Y)$ in a separable closure of $\mathbb{F}_q(t)$, $K_N = \mathbb{F}_q(t)[a]$.
- Let S be the set of poles of a and infinity places.
- For $\mathfrak{P} \in S$:
    - Choose a representation of $K_{N,\mathfrak{P}}$ as $\mathbb{F}_{q'}((T))$.

A polynomial time irreducibility test

Input: $N \in \mathbb{F}_q[X, Y]$ separable and irreducible.
Output: Is $N^p(t, \partial)$ irreducible in $\mathbb{F}_q(t)\langle\partial\rangle$.

- Set a a root of $N(t, Y)$ in a separable closure of $\mathbb{F}_q(t)$, $K_N = \mathbb{F}_q(t)[a]$.
- Let S be the set of poles of a and infinity places.
- For $\mathfrak{P} \in S$:
  - Choose a representation of $K_{N,\mathfrak{P}}$ as $\mathbb{F}_{q'}((T))$.
  - Compute a and T' at relative precision $\nu_{\mathfrak{P}}(T') - \nu_{\mathfrak{P}}(a)$.

A polynomial time irreducibility test

Input: $N \in \mathbb{F}_q[X, Y]$ separable and irreducible.
Output: Is $N^p(t, \partial)$ irreducible in $\mathbb{F}_q(t)\langle\partial\rangle$.

- Set a a root of $N(t, Y)$ in a separable closure of $\mathbb{F}_q(t)$, $K_N = \mathbb{F}_q(t)[a]$.
- Let S be the set of poles of a and infinity places.
- For $\mathfrak{P} \in S$:
  - Choose a representation of $K_{N,\mathfrak{P}}$ as $\mathbb{F}_{q'}((T))$.
  - Compute a and T' at relative precision $\nu_{\mathfrak{P}}(T') - \nu_{\mathfrak{P}}(a)$.
  - Check for a solution of the $\mathbb{F}_p$-linear system $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N + O(T^{p\nu(T')})$

A polynomial time irreducibility test

Input: $N \in \mathbb{F}_q[X, Y]$ separable and irreducible.
Output: Is $N^p(t, \partial)$ irreducible in $\mathbb{F}_q(t)\langle\partial\rangle$.

- Set a a root of $N(t, Y)$ in a separable closure of $\mathbb{F}_q(t)$, $K_N = \mathbb{F}_q(t)[a]$.
- Let S be the set of poles of a and infinity places.
- For $\mathfrak{P} \in S$:
  - Choose a representation of $K_{N,\mathfrak{P}}$ as $\mathbb{F}_{q'}((T))$.
  - Compute a and T' at relative precision $\nu_{\mathfrak{P}}(T') - \nu_{\mathfrak{P}}(a)$.
  - Check for a solution of the $\mathbb{F}_p$-linear system $\left(T' \frac{\mathrm{d}}{\mathrm{d}T}\right)^{(p-1)} f + f^p = y_N + O(T^{p\nu(T')})$
- If the check fails at least once $N^p(t, \partial)$ is irreducible, otherwise it is reducible.

A polynomial time irreducibility test

Input: $N \in \mathbb{F}_q[X, Y]$ separable and irreducible.
Output: Is $N^p(t, \partial)$ irreducible in $\mathbb{F}_q(t)\langle\partial\rangle$.

- Set a a root of $N(t, Y)$ in a separable closure of $\mathbb{F}_q(t)$, $K_N = \mathbb{F}_q(t)[a]$.
- Let S be the set of poles of a and infinity places.
- For $\mathfrak{P} \in S$:
  - Choose a representation of $K_{N,\mathfrak{P}}$ as $\mathbb{F}_{q'}((T))$.
  - Compute a and T' at relative precision $\nu_{\mathfrak{P}}(T') - \nu_{\mathfrak{P}}(a)$.
  - Check for a solution of the $\mathbb{F}_p$-linear system $\frac{\mathrm{d}^{p-1}}{\mathrm{d}T^{p-1}}(T'^{\,p-1}f) + f^p = y_N + O(T^{p\nu(T')})$
- If the check fails at least once $N^p(t, \partial)$ is irreducible, otherwise it is reducible.

Thank you for your attention.