Algebraic Extensions for Summation in Finite Terms

Burçin Eröcal

Research Institute for Symbolic Computation
Johannes Kepler University, Linz

May 4, 2010
SD 20.5, Fields Institute

Summation in finite terms

- Given an *elementary function* f, find g such that

$$g(n) = \sum_{a \leq i < n} f(i)$$

$$\Delta g(n) = g(n+1) - g(n) = f(n)$$

$$\sum_{0 \leq i < n} f(i) = g(n) - g(1)$$

Summation in finite terms

- Given an *elementary function* f, find g such that

$$g(n) = \sum_{a \leq i < n} f(i)$$

$$\Delta g(n) = g(n+1) - g(n) = f(n)$$

$$\sum_{0 \leq i < n} f(i) = g(n) - g(1)$$

Summation in finite terms

- Given an *elementary function* f, find g such that

$$g(n) = \sum_{a \leq i < n} f(i)$$

$$\Delta g(n) = g(n+1) - g(n) = f(n)$$

$$\sum_{0 \leq i < n} f(i) = g(n) - g(1)$$

Summation in finite terms

Definition

A difference field is a field F together with an automorphism σ of F. The constant field $K \subset F$ is the fixed field of σ.

$$\Delta g = f$$

$$\sigma(g) - g = f$$

Summation in finite terms

Definition

A difference field is a field F together with an automorphism σ of F. The constant field $K \subset F$ is the fixed field of σ.

$$\Delta g = f$$

$$\sigma(g) - g = f$$

Summation in finite terms

Definition

A difference field is a field F together with an automorphism σ of F. The constant field $K \subset F$ is the fixed field of σ.

$$\Delta g = f$$

$$\sigma(g) - g = f$$

Karr's algorithm

Given an elementary summand $f(i)$, i.e., a sum $\sum_{a\leq i<n} f(i)$,

- construct a field K containing all the constants appearing in f,
- then the rational function field $K(n)$ with the automorphism $\sigma(n) = n + 1$,
- then build a tower $K(n)(\theta_1, \ldots, \theta_m)$ where the θ_i are elementary functions needed to express f.
- Solve the first order linear difference equation

$$\sigma(g) - g = f$$

over $K(n)(\theta_1, \ldots, \theta_m)$.

Example

$$\sum_{1\leq i<n} H_i^2 = \sum_{1\leq i<n} \left(\sum_{1\leq j<i+1} \frac{1}{j} \right)^2$$

- $H_n^2 \in QQ(n)(h)$ where $\sigma(n) = n + 1$ and $\sigma(h) = h + \frac{1}{n+1}$
- Solve $\sigma(g) - g = h^2$ in $\mathbb{Q}(n)(h)$ to get

$$g(n) = H_n^2 n - 2H_n n - H_n + 2n$$

- $$\sum_{1\leq i<n} H_i^2 = g(n) - g(1) = H_n^2 n - 2H_n n - H_n + 2n$$

ΠΣ fields

Building towers

At each step

- constants are not extended
- transcendental

First order linear extensions

$\sigma(g) = \alpha g - \beta$, g transcendental

- inhomogeneous: $\beta \neq 0$
- homogeneous: $\beta = 0$
  - algebraic: α is a σ-radical
  - transcendental

ΠΣ fields

Building towers

At each step

- constants are not extended
- transcendental

First order linear extensions

$\sigma(g) = \alpha g - \beta$, g transcendental

- inhomogeneous: $\beta \neq 0$
- homogeneous: $\beta = 0$
  - algebraic: α is a σ-radical
  - transcendental

ΠΣ fields

Building towers

At each step

- constants are not extended
- transcendental

First order linear extensions

$\sigma(g) = \alpha g - \beta$, g transcendental

- inhomogeneous: $\beta \neq 0$
- homogeneous: $\beta = 0$
    - algebraic: α is a σ-radical
    - transcendental

ΠΣ fields

Building towers

At each step

- constants are not extended
- transcendental

First order linear extensions

$\sigma(g) = \alpha g - \beta$, g transcendental

- inhomogeneous: $\beta \neq 0$
- homogeneous: $\beta = 0$
  - algebraic: α is a σ-radical
  - transcendental

ΠΣ fields

Definition (Π-extensions)

We say that $F(t), \sigma$ is a Π-extension of F, σ if and only if

- $\sigma(t) = \alpha t$ where $\alpha \in F^*$,
- t is transcendental over F and
- the constant field is not extended.

Example

$$
\begin{array}{ll}
Q(i, 2^i) & \sigma(2^i) = 2(2^i) \\
\quad | & \\
Q(i) & \sigma(i) = i + 1 \\
\quad | & \\
Q &
\end{array}
$$

ΠΣ fields (contd.)

Definition (Σ-extensions)

We say that $F(t), \sigma$ is a Σ-extension of F, σ if and only if

- $\sigma(t) = \alpha t + \beta$ where $\alpha \in F^*$, $\beta \in F$,
- the equation $\sigma(w) - \alpha w = \beta$ has no solution in F and
- If there exists $g \in F$ such that $\sigma(g)/g = \alpha^n$ for some $n \in \mathbb{N}^+$, then there exists $f \in F$ such that $\sigma(f)/f = \alpha$.

Example

$$Q(i, \textstyle\sum_{1 \leq j < i} \frac{1}{j}) \qquad \sigma(\textstyle\sum_{1 \leq j < i} \frac{1}{j}) = \sum_{1 \leq j < i+1} \frac{1}{j} = (\sum_{1 \leq j < i} \frac{1}{j}) + \frac{1}{i}$$

$$|$$

$$Q(i) \qquad \sigma(i) = i + 1$$

$$|$$

$$Q$$

Examples of algebraic extensions

Example

- $\mathbb{Q}((-1)^n) \simeq \mathbb{Q}[x]/\langle x^2 - 1 \rangle$ since $((-1)^n)^2 = 1$
  $x^2 - 1 = (x-1)(x+1)$ over $\mathbb{Q}[x]$.

Examples of algebraic extensions

Example

- $\mathbb{Q}((-1)^n) \simeq \mathbb{Q}[x]/\langle x^2 - 1\rangle$ since $((-1)^n)^2 = 1$
  $x^2 - 1 = (x-1)(x+1)$ over $\mathbb{Q}[x]$.
- $\mathbb{Q}(4^n)(2^n) \simeq \mathbb{Q}(4^n)[x]/\langle x^2 - 4^n\rangle$
  $x^2 - 4^n$ is irreducible over $\mathbb{Q}(4^n)$.

Examples of algebraic extensions

Example

- $\mathbb{Q}\left((-1)^n\right) \simeq \mathbb{Q}[x]/\langle x^2 - 1\rangle$ since $\left((-1)^n\right)^2 = 1$
  $x^2 - 1 = (x-1)(x+1)$ over $\mathbb{Q}[x]$.
- $\mathbb{Q}(4^n)\,(2^n) \simeq \mathbb{Q}(4^n)[x]/\langle x^2 - 4^n\rangle$
  $x^2 - 4^n$ is irreducible over $\mathbb{Q}(4^n)$.
- $\mathbb{Q}(8^n)\,(4^n) \simeq \mathbb{Q}(8^n)[x]/\langle x^3 - (8^n)^2\rangle$
  $x^3 - (8^n)^2$ is irreducible over $\mathbb{Q}(8^n)[x]$.

Examples of algebraic extensions

Example

- $\mathbb{Q}\left((-1)^n\right) \simeq \mathbb{Q}[x]/\langle x^2 - 1\rangle$ since $\left((-1)^n\right)^2 = 1$
  $x^2 - 1 = (x-1)(x+1)$ over $\mathbb{Q}[x]$.
- $\mathbb{Q}(4^n)\,(2^n) \simeq \mathbb{Q}(4^n)[x]/\langle x^2 - 4^n\rangle$
  $x^2 - 4^n$ is irreducible over $\mathbb{Q}(4^n)$.
- $\mathbb{Q}(8^n)\,(4^n) \simeq \mathbb{Q}(8^n)[x]/\langle x^3 - (8^n)^2\rangle$
  $x^3 - (8^n)^2$ is irreducible over $\mathbb{Q}(8^n)[x]$.
- $\mathbb{Q}(4^n, 9^n)(6^n) \simeq \mathbb{Q}(4^n, 9^n)[x]/\langle x^2 - 4^n 9^n\rangle$
  $x^2 - 4^n 9^n$ is irreducible over $\mathbb{Q}(4^n, 9^n)$.

D-rings

Definition

- R - ring
- σ - endomorphism of R

A $\sigma - \textit{derivation}$ is a map $\delta : R \to R$ satisfying

$$\delta(a+b) = \delta(a) + \delta(b) \quad \text{and} \quad \delta(ab) = \sigma(a)\delta(b) + \delta(a)b \tag{1}$$

for any $a, b \in R$. The triple (R, σ, δ) is called a D-ring.

Example (differential ring)

If $\sigma = 1_R$, δ is a derivation on R. In this case, (R, δ) is called a differential ring.

D-rings

Definition

- R - ring
- σ - endomorphism of R

A $\sigma-$ *derivation* is a map $\delta : R \to R$ satisfying

$$\delta(a+b) = \delta(a) + \delta(b) \quad \text{and} \quad \delta(ab) = \sigma(a)\delta(b) + \delta(a)b \tag{1}$$

for any $a, b \in R$. The triple (R, σ, δ) is called a D-ring.

Example (difference ring)

For any endomorphism σ of R, $\delta = 0$ is a σ-derivation. In this case, (k, σ) is called a difference ring.

D-rings

Definition

- R - ring
- σ - endomorphism of R

A $\sigma-$ *derivation* is a map $\delta : R \to R$ satisfying

$$\delta(a+b) = \delta(a) + \delta(b) \quad \text{and} \quad \delta(ab) = \sigma(a)\delta(b) + \delta(a)b \tag{1}$$

for any $a, b \in R$. The triple (R, σ, δ) is called a D-ring.

Example

If R is commutative, σ an endomorphism of R, and $\alpha \in R$, the map $\delta_\alpha = \alpha(\sigma - 1_R)$ given by $\delta(a) = \alpha(\sigma(a) - a)$ is a σ-derivation.

Example

- $R = \mathbb{Q}(x)$,
- $\sigma : x \mapsto x + 1$
- $\delta : x \mapsto 1$

Then,

$$\delta(x^2) = \delta(xx) = \sigma(x)\delta(x) + \delta(x)x = 2\delta(x)x + \delta(x) = 2x + 1$$

Extensions of D-rings

Definition

- (R, σ, δ) and (R', σ', δ') - D-rings

We say that (R', σ', δ') is a D-ring extension of (R, σ, δ) if R is a subring of R' and $\sigma'(a) = \sigma(a)$ and $\delta'(a) = \delta(a)$ for any $a \in R$.

Definition

- For a D-ring R and $a, b \in R$, we introduce the notation

$$V_{a,b}(R) = \{w \in R \text{ such that } \sigma(w) = aw + b\}$$

  to denote the solutions of the first order linear difference equation $\sigma(w) = aw + b$
- We call an element a of a D-ring R a *σ-radical over R* if there exists $z \in R^*$ such that $\sigma(z) = a^n z$ for an integer $n > 0$.

Lemma (Bronstein 2000, Lemma 13)

Let (k, σ, δ) be a D-field with σ an automorphism of k, K be a field and a D-field extension of k, and $t \in K^*$ be algebraic over k such that $\sigma(t) = at + b$ for $a, b \in k$. Then, $V_{a,b}(k)$ is not empty. Furthermore, if $b = 0$, then either $a = 0$ or a is a σ-radical over k.

Theorem

Let

- (R, σ, δ) *be a D-ring with* σ *an automorphism of R,*
- *S be a D-ring extension of R,*
- *and* $t \in S^*$ *be algebraic over R such that* $\sigma(t) = at + b$ *for* $a \in R^*$ *and* $b \in R$.

If

- $V_{a,b}(R)$ *has no nonzero elements and*
- $\mathrm{Const}_{\sigma,\delta}(R) = \mathrm{Const}_{\sigma,\delta}(S)$,

then

- $b = 0$,
- *a is a* σ*-radical over R and*
- *the minimal polynomial* $p \in R[X]$ *of t is of the form* $X^d - c$.

Proof

Following the proof of Theorem 2.3 in [Karr85], let $p(X) = X^d + \sum_{i=0}^{d-1} p_i X^i$ be the minimal polynomial of t over R where $d > 0$. We have

$$0 = \sigma(p(t)) = (at+b)^d + \sum_{i=0}^{d-1} \sigma(p_i)(at+b)^i.$$

Replacing t^d with $-\sum_{i=0}^{d-1} p_i t^i$ reveals

$$a^d \sum_{i=0}^{d-1} p_i t^i = \sum_{i=0}^{d-1} \binom{d}{i} (at)^i b^{d-i} + \sum_{i=0}^{d-1} \sigma(p_i)(at+b)^i \tag{2}$$

Comparing coefficients for t^{d-1}, we get the equality

$$a^d p_{d-1} = a^{d-1} b + \sigma(p_{d-1}) a^{d-1},$$

Then $w = -p_{d-1}/d \in V_{a,b}(R)$. Since $V_{a,b}(R)$ has no nonzero elements, we conclude $p_{d-1} = 0$. Replacing p_{d-1} by 0 in the last equality, we see that b is also 0.

Proof (continued).

Looking back at equation (2) and comparing coefficients for t^i, we get

$$\sigma(p_i) = a^{d-i} p_i, \quad \text{for } 0 \leq i < d - 1.$$

Since t is nonzero, $p_j \neq 0$ for some $j < d$. For $j > 0$, $\sigma(t^{d-j}/p_{d-j}) = t^{d-j}/p_{d-j}$, so t^{d-j}/p_{d-j} is a new constant in R. Hence, for $0 < i < d$, $p_i = 0$. The equality $\sigma(p_0) = a^d p_0$ shows that a is a σ-radical over k. □

Remark

This theorem doesn't give any information about the purely differential case, since $V_{1,0}(R) = R$ and the statement doesn't apply.

Definition

- (R, σ, δ) - D-ring
- M - left R-module

A map $\theta : M \to M$ is called R-pseudo-linear (with respect to σ and δ) if

$$\theta(u + v) = \theta(u) + \theta(v) \qquad \text{and} \qquad \theta(au) = \sigma(a)\theta(u) + \delta(a)u$$

for any $a \in R$ and $u, v \in M$.
We write $End_{R,\sigma,\delta}(M)$ for the set of all R-pseudo-linear maps of M.

- (F, σ, δ) - D-field of characteristic 0
- (E, σ, δ) - algebraic extension of (F, σ, δ)
- $\theta : E \to E \in End_{F,\sigma,\delta}$ - an F-pseudo-linear map
- We are interested in solving

$$\theta(z) + fz = g$$

for $z \in E$ where $f, g \in E$ are given.

Example

In order to find a *simpler* expression for $\sum_{k=1}^{n}(-1)^k k$,, we need to solve the equation

$$\sigma(z) - z = (-1)^k k$$

in the difference field $\mathbb{Q}(k)((-1)^k)$, with $\sigma(k) = k + 1$ and $\sigma((-1)^k) = -(-1)^k$.

- We can view E as a finite dimensional algebra over F.
- Let $\mathbf{b} = (b_1, \ldots, b_n)$ be any basis of E over F.
- Write $u_{\mathbf{b}}$ for the column vector of the coordinates of u in the basis $\mathbf{b}$, i.e., $\mathbf{u}_b \in F^n$
- We want to solve

$$(\theta(z) + fz)_{\mathbf{b}} = g_{\mathbf{b}}.$$

Example

Let $\mathbf{b} = ((-1)^k, 1)$. We have $g = (-1)^k k$, then

$$g_{\mathbf{b}} = \begin{pmatrix} k \\ 0 \end{pmatrix}.$$

- Let $z \in E$. Write $z = z_1 b_1 + z_2 b_2 + \cdots + z_n b_n$ where $z_i \in F$ and $\mathbf{b} = (b_1, \ldots, b_n)$ is a basis of E over F.
- Then,

$$
\begin{aligned}
\theta(z) &= \theta(z_1 b_1) + \cdots + \theta(z_n b_n) \\
&= \sigma(z_1)\theta(b_1) + \delta(z_1) b_1 + \cdots + \sigma(z_n)\theta(b_n) + \delta(z_n) b_n \\
&= \sum_{i=1}^{n} \sigma(z_i)\theta(b_i) + \sum_{i=1}^{n} \delta(z_i) b_i
\end{aligned}
$$

- For an F-pseudo-linear map θ, define the matrix $\theta_{\mathbf{b}}$ as follows

$$\theta_{\mathbf{b}} = \begin{pmatrix} | & | & \cdots & | \\ (\theta(b_1))_{\mathbf{b}} & (\theta(b_2))_{\mathbf{b}} & \cdots & (\theta(b_n))_{\mathbf{b}} \\ | & | & \cdots & | \end{pmatrix}.$$

Example

In our example,

$$\sigma_{\mathbf{b}} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

- Recall,

$$\theta(z) = \sum_{i=1}^{n} \sigma(z_i)\theta(b_i) + \sum_{i=1}^{n} \delta(z_i) b_i$$

- Then,

$$\begin{aligned}(\theta(z))_{\mathbf{b}} &= \theta_{\mathbf{b}}(\sigma I)(z)_{\mathbf{b}} + (\delta I)(z)_{\mathbf{b}} \\ &= (\theta_{\mathbf{b}}(\sigma I) + (\delta I))\,(z)_{\mathbf{b}}\end{aligned}$$

- For any $u \in E$, define $M_{\mathbf{b}}(u)$ to be

$$M_{\mathbf{b}}(u) = \begin{pmatrix} | & | & \cdots & | \\ (ub_1)_{\mathbf{b}} & (ub_2)_{\mathbf{b}} & \cdots & (ub_n)_{\mathbf{b}} \\ | & | & \cdots & | \end{pmatrix}.$$

- Then for any $u, v \in E$

$$(uv)_{\mathbf{b}} = M_{\mathbf{b}}(u)(v)_{\mathbf{b}}.$$

Example

We have

$$M_{\mathbf{b}}(-1) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

- We have

$$\begin{aligned} g_{\mathbf{b}} &= (\theta(z) + fz)_{\mathbf{b}} \\ &= (\theta_{\mathbf{b}}(\sigma I) + (\delta I))\,(z)_{\mathbf{b}} + M_{\mathbf{b}}(f)(z)_{\mathbf{b}} \\ &= (\theta_{\mathbf{b}}(\sigma I) + (\delta I) + M_{\mathbf{b}}(f))\,(z)_{\mathbf{b}} \end{aligned}$$

Example

In the differential case, $\sigma = 1_F$, $\theta = \delta$, then we have

$$(\delta_{\mathbf{b}} + (\delta I) + M_{\mathbf{b}}(f))\,(z)_{\mathbf{b}} = g_{\mathbf{b}}.$$

Example

In the difference case, $\delta = 0_F$, $\theta = \sigma$, so we have

$$(\sigma_{\mathbf{b}}(\sigma I) + M_{\mathbf{b}}(f))\,(z)_{\mathbf{b}} = g_{\mathbf{b}}$$

Demo

Example

- Take $R = \mathbb{Q}(n)(e)$ with $\sigma(n) = n + 1$ and $\sigma(e) = -e$, where e behaves like $(-1)^n$.
- We want to extend $R = \mathbb{Q}(n)(e)$ from the previous example with a new indeterminate s such that $\sigma(s) = s - \frac{e}{n+1}$,
  i.e., s behaves like $\sum_{i=1}^{n} \frac{(-1)^i}{i}$.

Example

- $((-1)^n)^2 = 1$, so e satisfies the polynomial $x^2 - 1 \in \mathbb{Q}(n)[x]$.
- $x^2 - 1$ factors over $\mathbb{Q}(n)$

$$R \simeq \mathbb{Q}(n)[x]/\langle x^2 - 1\rangle \simeq \mathbb{Q}(n)[x]/\langle x - 1\rangle \oplus \mathbb{Q}(n)[x]/\langle x + 1\rangle$$

- $e_0 = \frac{e+1}{2}$ and $e_1 = \frac{-e+1}{2}$ are idempotent in R.
- Since $1 = e_0 + e_1$ and $e_0 e_1 = 0$, we also have the decomposition $R \simeq \mathbb{Q}(n)e_0 \oplus \mathbb{Q}(n)e_1$.

Theorem (Singer, van der Put, (1997))

Let (k, σ, δ) be a D-field with σ an automorphism of k, R be a finitely generated simple difference ring and a D-ring extension of k. There exist idempotents $e_0, \ldots, e_{d-1} \in R$ for $d > 0$ such that

1. $R = R_0 \oplus \cdots \oplus R_{d-1}$ *where* $R_i = e_i R$,
2. $\sigma(e_i) = e_{i+1 \pmod d}$ *so* σ *maps* R_i *isomorphically onto* $R_{i+1 \pmod d}$ *and* σ^d *leaves each* R_i *invariant.*
3. *For each* i, R_i *is a domain, a simple difference ring and a D-ring extension of* $e_i k$ *with respect to* σ^d.

Remark

If $X^d - c$ splits over k, i.e., $X^d - c = \prod_{0 \le i < d}(x - \zeta_i)$ with $\zeta_i \in k$, we have

$$k[X]/\langle X^d - c\rangle \simeq \bigoplus_{0 \le i < d} k[X]/\langle X - \zeta_i\rangle.$$

The isomorphism is given by

$$\pi : k[X] \to \bigoplus_{0 \le i < d} k[X]/\langle X - \zeta_i\rangle \tag{3}$$

$$p \mapsto (p(\zeta_0), \ldots, p(\zeta_{d-1})) \tag{4}$$

Let $e_i = 1 \in K[X]/\langle X - \zeta_i\rangle$, then

$$\pi^{-1}(e_i) = \prod_{\substack{0 \le i < d \\ j \ne i}} \frac{x - e_j}{e_i - e_j}$$

Example

- Take $R = \mathbb{Q}(\zeta)(n)\,(e)$ with $\sigma(n) = n+1$ and $\sigma(e) = \zeta e$, where e behaves like $(\zeta)^n$ with ζ a 3rd root of unity.
- $((\zeta)^n)^3 = 1$, so e satisfies the polynomial $x^3 - 1 \in \mathbb{Q}(\zeta)(n)[x]$.
- $x^3 - 1$ factors over $\mathbb{Q}(\zeta)(n)$

$$\begin{aligned} R &\simeq \mathbb{Q}(\zeta)(n)[x]/\langle x^3 - 1\rangle \\ &\simeq \mathbb{Q}(\zeta)(n)[x]/\langle x - 1\rangle \oplus \mathbb{Q}(\zeta)(n)[x]/\langle x - \zeta\rangle \oplus \mathbb{Q}(\zeta)(n)[x]/\langle x - \zeta^2\rangle \end{aligned}$$

- $e_0 = \frac{e^2+e+1}{3}$, $e_1 = \frac{\zeta^2 e^2+\zeta e+1}{3}$ and $e_2 = \frac{\zeta e^2+\zeta^2 e+1}{3}$ are idempotent in R.

Extending algebraic extensions

Example

- We want to extend $R = \mathbb{Q}(n)(e)$ from the previous example with a new indeterminate s such that $\sigma(s) = s - \frac{e}{n+1}$,
  i.e., s behaves like $\sum_{i=1}^{n} \frac{(-1)^i}{i}$.
- Writing $s = s_0 e_0 + s_1 e_1$ and $e = e_0 - e_1$, we have

$$\begin{aligned} \sigma(s_0 e_0 + s_1 e_1) &= \sigma(s_0) e_1 + \sigma(s_1) e_0 \\ &= s_0 e_0 + s_1 e_1 + \frac{-e_0}{n+1} + \frac{e_1}{n+1} \end{aligned}$$

- Hence, we need to find an extension of $\mathbb{Q}(n)$, namely $\mathbb{Q}(n, h)$, where $\sigma(h) = ah + b$ for some $a, b \in \mathbb{Q}(n)$ and $s_0, s_1 \in \mathbb{Q}(n, h)$ such that $\sigma(s_0) = s_1 + \frac{1}{n+1}$ and $\sigma(s_1) = s_0 - \frac{1}{n+1}$.

Example (contd.)

- Take $\sigma(h) = -h - \frac{1}{n+1}$, $s_0 = -h$ and $s_1 = h$.
- Then

$$\begin{aligned} \sigma(s_0) &= \sigma(-h) = h + \frac{1}{n+1} \\ \sigma(s_1) &= \sigma(h) = -h - \frac{1}{n+1} \end{aligned}$$

Theorem

Let

- *Let* $R = K[x]/\langle x^d - c\rangle$ *and* (R, σ, δ) *be a D-ring,*
- *where* $x^d - c$ *splits over* $K[x]$ *and* $\sigma(x) = \zeta x$.
- *Let* $S = R[y]$ *be a D-ring extension of R, such that* $\sigma(y) = ay + b$ *for* $a \in R^*$ *and* $b \in R$.

Then

$$(S, \sigma) \simeq (K[\bar{y}][x]/\langle x^d - c\rangle, \tilde{\sigma})$$

where $\tilde{\sigma}(\bar{y}) = \zeta a(\zeta)\bar{y} + b(\zeta)$.

Demo

- q-identities which hold for roots of unity

Sage Days 24 at RISC,
Linz, Austria
July 17-22