

# Using Polynomial Structures in Reasoning with Reflexion

Theorema-Ultra-Omega '05 Workshop, Saarbrücken  
November 14-15, 2005

**Markus.Rosenkranz@oeaw.ac.at**

*Radon Institute for Computational and Applied Mathematics  
Austrian Academy of Sciences  
A-4040 Linz, Austria*

## Outline of the Talk

 [Reflexion](#): Just intuitive approach, no precise formulation of quote

→ Martin's talk.

- **Prelude: The Standard Polynomials**
- **Polynomials and Reflexion**
- **The General Notion of Polynomial**
- **The Rôle of Canonical Simplification**
- **Back to the Standard Polynomials**
- **Other Examples of Generalized Polynomials**
- **Postlude: The Green's Polynomials**

## The Standard Polynomials

Older texts:

"An **expression** of the form  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ , where  $n$  is a natural number, the coefficients  $a_r$  are arbitrary real numbers, and  $a_n \neq 0$ , is called a polynomial of degree  $n$ ."

W. Gellert, H. Kustner, M. Hellwich, H. Kastner  
(eds), *The VNR Concise Encyclopedia of Mathematics*,  
Van Nostrand Reinhold, New York, 1975, page 115.

Modern texts:

For any field  $K$ , the **monoid ring** over  $K$  for the monoid  $\mathbb{N}$  is denoted by  $K[x]$ ; its elements are called polynomials over  $K$ .

I. Becker, V. Weispfenning, *Gröbner Bases*,  
Springer, New York, 1993, page 64.

Multivariate polynomials:

- Take  $x_1, \dots, x_n$  instead of  $x$ .
- Take the monoid  $\mathbb{N}^n$  instead of  $\mathbb{N}$ .

Resumé: The "old approach" is outright nonsense!?

## Footnotes for Concrete Computations

Often assume that ring  $K[x]$  has additional **individual constants**:

- One for each coefficient in  $K$ , called its name.
- One for the algebraic generator  $x$ , called the indeterminate.

Concrete computation in  $K = \mathbb{Q}(\pi, i) \subseteq \mathbb{C}$ :

```
Expand [ (3πi x2 + 7.2) * (x - i) ]
```

```
-7.2 i + 7.2 x - 3 i x2 πi + 3 x3 πi
```

Input polynomials have indeterminate  $x$  and the names:

- Name  $3\pi i \in \mathbb{C}$ .
- Name  $7.2 \in \mathbb{C}$ .
- Name  $1 \in \mathbb{C}$  or unit  $1_{\mathbb{C}}$ .
- Name  $-i \in \mathbb{C}$  or  $-_{\mathbb{C}} i$  with  $i \in \mathbb{C}$ .

## The Idea of Reflexion

Intuition:

*The polynomials from  $K[x]$  are like “templates” for terms in the ring signature  $\langle +, -, * \rangle$  with “numbers” from  $K$  and a “variable”  $x$ .*

Hence proving/computing on the “meta level” of terms might be **reflected** in proving/computing on the “object level” of polynomials.

An example, in the usual formulation on the “object level”:

*For any field  $K$ , the polynomial ring  $K[x]$  is Euclidean.*

*This means essentially:*

$$\forall_{a, b \in K[x]} \exists!_{q, r \in K[x]} (a = qb + r \wedge \deg(r) < \deg(b) \iff b \neq 0)$$

The example, reflected on the “meta level”:

*Whenever we have terms  $\alpha, \beta$  such that  $\vdash \beta \neq 0$ ,*

*there are terms  $\theta, \rho$  such that  $\vdash \alpha = \theta\beta + \rho$  and  $\vdash \deg(\rho) < \deg(\beta)$ .*

*And if there are any other terms  $\theta', \rho'$  fulfilling the same requirements,*

*we have  $\vdash \theta' = \theta$  and  $\vdash \rho' = \rho$ .*

## A Result without Reflexion

Observation:

- The usage of reflexion is typically hidden in (computer) algebra textbooks.

- But in the majority of cases, one does not need reflexion.

Example of a “majority case” that uses Euclideanity:

- For any field  $K$ , the polynomial ring  $K[x]$  is a principal ideal domain.

I. Becker, V. Weispfenning, *Gröbner Bases*, Springer, New York, 1993, page 82.

**Proof sketch:** Take any ideal  $I \subseteq K[x]$ . If  $I = 0$ , then  $I = 0 \cdot K[x]$  is principal. Otherwise take  $b \in I \setminus \{0\}$  with  $\deg(b)$  minimal and show  $I = b \cdot K[x]$ . Indeed, the inclusion  $\supseteq$  is obvious, so we must prove  $a \in I \Rightarrow a \in b \cdot K[x]$ . Now take  $a \in I$  and apply the **Euclidean algorithm** for obtaining  $q, r \in K[x]$  with  $a = qb + r$  and  $\deg(r) < \deg(b)$ . But then  $r = a - bq \in I$ , so  $r = 0$  by the minimality of the  $\deg(b)$  over  $b \in I \setminus \{0\}$ . Hence we have  $a = qb \in b \cdot K[x]$ , as required.  $\square$



7 of 19

## Working on the Term Structure: Integration of Elementary Functions

Distinguish:

**Integral Operator**  $\int(\dots) \leftrightarrow$  **Integral Quantifier**  $\int \dots dx$

Integral operator, say  $\int : C[0, 1] \rightarrow C^1[0, 1]$  is specified (non-uniquely!) by:

$$\forall_{f \in C[0,1]} \left( \int f \right)' = f$$

Integral quantifier via integral operator (syntactic abbreviation in FOL):

$$\int \tau dx \equiv \int (\lambda_x. \tau)$$

Why should we need an integral quantifier rather than operator?

- Input domain may be characterized syntactically (like Liouvillian fields or elementary functions) rather than abstractly (like  $C[0, 1]$  above).
- Integration algorithms may be more efficient if applied on terms.
- Integral tables are always written with integral quantifier.



8 of 19

## Using the Euclidean Algorithm on the Term Level

Example from an analysis book:

Let  $R = P/Q$  be a proper rational function, and assume the denominator polynomial has the product representation  $Q(z) = \prod_{i=1}^m (z - \zeta_i)^{\lambda_i}$ . Then  $R$  can be written in the form of a partial fraction decomposition  $R(z) = \sum_{i=1}^m \sum_{j=1}^{\lambda_i} \frac{a_{ij}}{(z - \zeta_i)^j}$  for suitable  $a_{ij} \in \mathbb{C}$ .

H. Heuser, *Analysis I*,  
Teubner, Stuttgart, 1990, page 401.

Corollary: We can integrate all **arithmetic terms**, i.e. all terms built

- over the signature  $\langle +, -, *, - \rangle$ ,
- with names from (a computable subfield of)  $\mathbb{C}$ ,
- and containing at most  $x$  as a variable.

Proof sketch: Every term may be rewritten as  $\alpha/\beta$  with  $\alpha$  and  $\beta$  being polynomial terms and  $\vdash \beta \neq 0$ . Using the **Euclidean algorithm**, we obtain terms  $\theta$  and  $\rho$  with  $\vdash \alpha/\beta = \theta + \rho/\beta$  such that  $\rho/\beta$  represents a proper rational function. Since  $\int$  is linear, the above result reduces the problem to the known integrals of polynomial terms and terms  $(z - \zeta_i)^j$ .  $\square$

9 of 19

## Reflexion Used in Solving

Find  $\xi, \eta \in \mathbb{C}$  such that (metavariables!):

$$\left. \begin{array}{l} \xi\eta^2 + 2\xi\eta + \xi^2 + 1 = 0 \\ \xi\eta + \eta^2 + 1 = 0 \end{array} \right\} \Pi[\xi, \eta]$$

The Buchberger algorithm **GroebnerBasis** :  $\mathbb{C}[x, y]^* \rightarrow \mathbb{C}[x, y]^*$  fulfills:

$$\forall_{f_1, \dots, f_n \in \mathbb{C}[x, y]} \mathcal{V}[\text{GroebnerBasis}[f_1, \dots, f_n]] = \mathcal{V}[f_1, \dots, f_n]$$

Here  $\mathcal{V} : \mathbb{C}[x, y]^* \rightarrow \mathbb{C}^2$  is the variety (common zeroes of a polynomial list).

Corollary: We have  $\vdash \Pi[\xi, \eta]$  iff  $\vdash \tilde{\Pi}[\xi, \eta]$ , where  $\tilde{\Pi}[\xi, \eta]$  is the polynomial equation system  $f_1 = \dots = f_n = 0$  from the output  $f_1, \dots, f_n$  of **GroebnerBasis**.

Computation:

```
GroebnerBasis[{\xi\eta^2 + 2 \xi\eta + \xi^2 + 1, \xi\eta + \eta^2 + 1}, {\xi, \eta}]
```

```
{-1 - \eta^2 + \eta^3 + \eta^4 + \eta^5, \eta^2 + \eta^3 + \eta^4 + \xi}
```



10 of 19

## The General Notion of Polynomial

Two natural questions:

- How can one justify this **reflection** of the “meta level” in the “object level”?
- Can one generalize this from ring terms to **other terms**?

Answer given by:

Given any **variety**  $\Sigma$ , a coefficient algebra  $\mathfrak{A}$  in  $\Sigma$ , and a set of **indeterminates**  $X$ , there is an algebra  $\mathfrak{A}[X]_{\Sigma}$  in  $\Sigma$ ; the elements of  $\mathfrak{A}[X]_{\Sigma}$  are called (generalized) **polynomials**.

H. Lausch, W. Nöbauer, *Algebra of Polynomials*,  
North-Holland, Amsterdam, Lemma 4.11, 1973(!),  
page 12.

Variety = Model class with functional signature and equational axioms.

Algebra=Model from a variety.

Let me call  $\mathfrak{A} \mapsto \mathfrak{A}[X]_{\Sigma}$  the **Lausch-Nöbauer functor**.



11 of 19

## A Rough Sketch of the Lausch-Nöbauer Functor

**Construction** analogous to functional part of Gödel’s completeness proof:

$$\mathfrak{A}[X]_{\Sigma} := \text{Term}(X, \text{Sgn}(\Sigma) \cup \text{Nm}(\mathfrak{A})) / \approx_{\Sigma, X}$$

$$t \approx_{\Sigma, \mathfrak{A}} t' \Leftrightarrow \text{Axm}(\Sigma) \cup \text{Op}(\mathfrak{A}) \vdash t = t'$$

Here we have used the following **abbreviations**:

**Sgn**( $\Sigma$ ) ... Signature of the variety  $\Sigma$   
**Nm**( $\mathfrak{A}$ ) ... Name signature for the algebra  $\mathfrak{A}$   
**Axm**( $\Sigma$ ) ... Axioms of the variety  $\Sigma$   
**Op**( $\mathfrak{A}$ ) ... Operation table for the algebra  $\mathfrak{A}$   
 $\vdash$  ... Equational provability

**Fundamental property** of the Lausch-Nöbauer functor:

Every extension  $\mathfrak{A}'$  of  $\mathfrak{A}$  generated by  $\{u_x \mid x \in X\}$  admits an epimorphism  $\text{ev} : \mathfrak{A}[X]_{\Sigma} \rightarrow \mathfrak{A}'$  with  $\text{ev}|_{\mathfrak{A}} = \text{Id}$  and  $\text{ev}(x) = u_x$  for all  $x \in X$ .

Lausch-Nöbauer, Lemma 4.43, page 15.



12 of 19

## The Standard Polynomials Revisited

Let  $\text{Ring}$  be the variety of unital commutative rings.

$\langle + : 2, 0 : 0, - : 1, * : 2, 1 : 0 \rangle$  } **Sgn**(**Ring**)

$x + (y + z) = (x + y) + z$   
 $x + 0 = 0$   
 $x + (-x) = 0$   
 $x + y = y + x$   
 $x * (y * z) = (x * y) * z$   
 $x * (y + z) = x * y + x * z$   
 $1 * x = x$   
 $x * y = x * y$

} **Axm**(**Ring**)

Let  $\mathbb{Q}_{\#}$  be the ring  $\mathbb{Q}$  together with all names and operation table:

$3.1 * 2 = 6.2, 0 = 0, 1 = 1, \dots$

Setting now  $X = \{x_1, \dots, x_n\}$ , we regain the standard polynomials:

$\mathbb{Q}_{\#}[X]_{\text{Ring}} \cong \mathbb{Q}[x_1, \dots, x_n]$



13 of 19

## The Rôle of Canonical Simplification for Symbolic Computation

Canonical simplifier  $x \mapsto \hat{x}$  with respect to a congruence  $\approx$  on a domain  $D$ :

$$\begin{aligned} \hat{x} &\approx x \\ x \approx y &\implies \hat{x} = \hat{y} \end{aligned}$$

General significance of canonical simplifiers:

Let  $f : D^n \rightarrow D$  be any operation that respects  $\approx$ , giving rise to the operation  $\bar{f} : \bar{D}^n \rightarrow \bar{D}$  on the quotient domain  $\bar{D} = D / \approx$ , defined by  $\bar{f}([x_1]_{\approx}, \dots, [x_n]_{\approx}) = [f(x_1, \dots, x_n)]_{\approx}$ .

Having a canonical simplifier  $x \mapsto \hat{x}$ , the quotient  $\bar{D}$  is isomorphic to  $\hat{D} = \{\hat{x} \mid x \in D\}$ , and  $\bar{f}$  can be realized isomorphically via  $\hat{f} : \hat{D}^n \rightarrow \hat{D}$ , defined by  $\hat{f}(\hat{x}_1, \dots, \hat{x}_n) = \hat{f}(x_1, \dots, x_n)$ .

If  $f$  and  $x \mapsto \hat{x}$  are **computable**, then  $\hat{f}$  is also.

B. Buchberger, R. Loos, *Computer Algebra: Symbolic and Algebraic Computation*,  
in B. Buchberger, G.E. Collins, R. Loos (eds), *Algebraic Simplification*, Springer, Wien, 1982.



14 of 19

## Canonical Simplification for the Standard Polynomials

Apply above result to  $\approx_{\Gamma, \mathbb{Q}_{\#}}$  and  $D = \mathbb{Q}_{\#}[\{x\}]_{\text{ring}}$ , and obtain for  $\hat{D}$  exactly...

The **terms**  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  with coefficients  $a_r \in \text{Nm}(\mathbb{Q}_{\#})$  and  $a_n \neq 0$  constitute the canonical forms for  $\approx_{\Gamma, \mathbb{Q}_{\#}}$ .

W. Gellert, H. Küstner, M. Hellwich, H. Kästner (eds), *The VNR Concise Encyclopedia of Mathematics*, Van Nostrand Reinhold, New York, 1975, page 115.

Operations like  $\hat{+}$  and  $\hat{\cdot}$  carried out as we learned it in high school:

Compute as if  $x$  were an “unknown” element of  $\mathbb{Q}$ , and simplify in the end.



15 of 19

## A Menagerie of Other Examples

(1) Group polynomials: Set  $\mathfrak{V} = \mathit{Grp}$  with, say,  $X = \{x, y\}$  and  $\mathfrak{A} = D_4$ .

$$xy^2x^{-3}SR^2y^{-1}Rx^{-2}SR \in (D_4[x, y]_{\mathit{Grp}})^\wedge$$

(2) Lattice polynomials: Analogously, set  $\mathfrak{V} = \mathit{Lat}$ , etc.

(3) Boolean polynomials: Analogously, set  $\mathfrak{V} = \mathit{Bool}$ , etc.

(4) Differential polynomials: Set  $\mathfrak{V} = \mathit{DiffRing}$  with,  $X = \{u\}$  and  $\mathfrak{A} = C^\infty(\mathbb{R})$ :

$$\sin u' + \exp u' u \in (C^\infty(\mathbb{R})[u]_{\mathit{DiffRing}})^\wedge$$

Variety  $\mathit{DiffRing}$  like  $\mathit{Ring}$ , but  $\langle \partial : 1 \rangle$  added to signature,

and  $\partial(f + g) = \partial f + \partial g$  and  $\partial(fg) = f \partial g + g \partial f$  to axioms.

Traditional description:

$$\left. \begin{array}{l} C^\infty(\mathbb{R})\{u\} = C^\infty(\mathbb{R})[u, u', u'', \dots] \\ \partial f = \partial f \\ \partial u^{(n)} = u^{(n+1)} \end{array} \right\} \rightarrow R\{u\} \cong C^\infty(\mathbb{R})[u]_{\mathit{DiffRing}}$$

## An Example from my own Research

(5) Integro-differential polynomials: Set  $\mathfrak{V} = \mathit{IntDiffRing}$ , else as before.

Variety  $\mathit{IntDiffRing}$  like  $\mathit{DiffRing}$ , but  $\langle \int^* : 1, \int_* : 1 \rangle$  added to signature,

and the following axioms:

$$\begin{array}{ll} \int^* (f + g) = \int^* f + \int^* g & \int_* (f + g) = \int_* f + \int_* g \\ \partial(\int^* f) = f & \partial(\int_* f) = -f \\ \int^* fg = (\int^* g)f - \int^* (\int^* g)f' & \int_* fg = (\int_* g)f + \int_* (\int_* g)f' \end{array}$$

Typical integro-differential polynomial:

$$\int^* (\exp u^2) + \sin \left( \int_* (u) \right)^2$$

Extract subring of linear polynomials, write composition as multiplication

→ Green's polynomials → Green's system

$$\int_* (\partial^2 (\exp u)) + \sin \int^* (u) \rightarrow BD^2[\exp] + [\sin] A \in \mathbb{C} \langle A, B, D, [f] \rangle / \approx \rightarrow \dots^{\wedge}$$



17 of 19

## The Green's System I

```
System["Equalities Algebraic", any[f, g],
  [f] [g] = [f g]]
System["1. Equalities", any[f],
  DA = 1
  DB = -1
  D [f] = [f] D + [f']
  DL = 0
  DR = 0
  ]
System["3. Equalities", any[f],
  A [f] A = [∫* f] A - A [∫* f]
  A [f] B = [∫* f] B + A [∫* f]
  B [f] A = [∫* f] A + B [∫* f]
  B [f] B = [∫* f] B - B [∫* f]
  AA = [∫* 1] A - A [∫* 1]
  AB = [∫* 1] B + A [∫* 1]
  BA = [∫* 1] A + B [∫* 1]
  BB = [∫* 1] B - B [∫* 1]
  ]
```



18 of 19

## The Green's System II

System["2. Equalities", any[f], System["4. Equalities", any[f],

$$\begin{array}{l}
 LA = 0 \\
 RA = A + B \\
 LB = A + B \\
 RB = 0 \\
 \hline
 L[f] = f^{\leftarrow} L \\
 R[f] = f^{\rightarrow} R \\
 \hline
 LL = L \\
 LR = R \\
 RL = L \\
 RR = R
 \end{array}
 \quad ]
 \quad
 \begin{array}{l}
 A[f]D = -f^{\leftarrow} L + [f] - A[f'] \\
 B[f]D = f^{\rightarrow} R - [f] - B[f'] \\
 \hline
 AD = -L + 1 \\
 BD = R - 1 \\
 \hline
 A[f]L = [\int^* f] L \\
 B[f]L = [\int_* f] L \\
 A[f]R = [\int^* f] R \\
 B[f]R = [\int_* f] R \\
 \hline
 AL = [\int^* 1] L \\
 BL = [\int_* 1] L \\
 AR = [\int^* 1] R \\
 BR = [\int_* 1] R
 \end{array}
 ]$$



## The Use of Green's Polynomials: Solving Boundary Value Problems

Example (an ill-posed problem):

$$\begin{cases} -u'' = f \\ u'(0) = u'(1) = 0 \end{cases} \longrightarrow g(x, \xi) = \begin{cases} \frac{1}{3} - x - \frac{x^2 + \xi^2}{2} & \leftarrow 0 \leq \xi \leq x \leq 1 \\ \frac{1}{3} - \xi - \frac{x^2 + \xi^2}{2} & \leftarrow 0 \leq x \leq \xi \leq 1 \end{cases}$$

Operator formulation (with solution algorithm):

$$\begin{cases} -D^2 G = 1 \\ LDG = RDG = 0 \end{cases} \longrightarrow G = \frac{1}{3} A - [x] A - \frac{1}{2} [x^2] A - \frac{1}{2} A [x^2] \\ + \frac{1}{3} B - B [x] - \frac{1}{2} [x^2] B - \frac{1}{2} B [x^2]$$

Note the benefit of a good “datastructure”:

- Case distinction eliminated.
- Instead of two variables  $x, \xi$  only one.
- Direct representation of operators.
- Polynomials have (noncommutative) ring structure.
- Canonical simplifier  $\sim$  extraction of Green’s function.