The *Theorema* System

Wolfgang Windsteiger

RISC Institute
A-4232 Hagenberg, Austria
Wolfgang.Windsteiger@RISC.Uni-Linz.ac.at

Calculemus Autumn School, Pisa, September 27, 2002.

1 History

1.1 Initial Motivation

Initial motivation for development of *Theorema*:

Observation [Buchberger, ≈1990 or earlier]:

$$\boxed{\underset{\text{system}}{\nexists}\ \text{is-one-software}[\text{system}] \wedge \text{supports-all-of-algorithmic-mathematics}[\text{system}]}$$

where

$$\text{supports-all-of-algorithmic-mathematics}[s] :\Leftrightarrow$$

$$\bigwedge \begin{cases} \text{supports-defining-mathematical-concepts-in-a-natural-way}[s] \\ \text{supports-experimenting-by-large-nontrivial-computations}[s] \\ \text{supports-conjecturing-theorems}[s] \\ \text{supports-proving-theorems}[s] \\ \text{supports-gaining-insight-through-proving}[s] \\ \text{supports-turning-theorems-into-algorithms}[s] \\ \text{supports-publishing-mathematical-results}[s] \end{cases}$$

1.2 On the other hand ...

Fact 1:

$$\underset{\text{system}}{\exists} \; \bigwedge \begin{cases} \text{supports-defining-mathematical-concepts-in-a-natural-way}[\text{system}] \\ \text{supports-proving-theorems}[\text{system}] \\ \text{supports-gaining-insight-through-proving}[\text{system}] \end{cases}$$

Proof:

Take system:="the logic system used by human mathematicians",
e.g. system:="some version of predicate logic".

Fact 2:

$$\underset{\text{system}}{\exists} \; \bigwedge \begin{cases} \text{is-one-software}[\text{system}] \\ \text{supports-experimenting-by-large-nontrivial-computations}[\text{system}] \\ \text{supports-turning-theorems-into-algorithms}[\text{system}] \end{cases}$$

Proof:

Take system:="any available computer algebra system".

Fact 3:

$$\underset{\text{system}}{\exists} \; \bigwedge \begin{cases} \text{is-one-software}[\text{system}] \\ \text{supports-proving-theorems}[\text{system}] \end{cases}$$

Proof:

Take system:="any available theorem proving system".

Fact 4:

$$\underset{\text{system}}{\exists} \bigwedge \begin{cases} \text{is-one-software[system]} \\ \text{supports-publishing-mathematical-results[system]} \end{cases}$$

Proof:

Take system:="any mathematical typesetting system",
e.g. system:=$\LaTeX$.

1.3 Theorema

Implementation Design Specification

Find the most appropriate *programming language* or *software-system* for implementing one piece of software *system*, such that

$$\text{is-one-software[system]} \wedge \text{supports-all-of-algorithmic-mathematics[system]}$$

Implementation Design Decision Process (Buchberger and Co-Workers, ≈ 1990–1995)

Choose

- the Mathematica programming language (pattern matching),
- the Mathematica rewrite engine as the basis for the computation engine,
- the Mathematica Front End as user interface (configurable, extensible, programmable).

(see the early papers by Buchberger from that time!)

2 System Design

2.1 Language Layer Model

2.1.1 *Theorema* Expression Language

Formulating mathematical contents.
Higher order predicate logic, sets, tuples.
Syntax:
Internal representation as Mathematica data-structures.
External representation in "natural form" using typesetting features of the Mathematica Front End.
"Natural form" input supported by the Mathematica Front End.

⟨3, a, 2, N, 1, a⟩

⟨3, a, 2, N, 1, a⟩

{3, a, 2, N, 1, a}

{3, a, 2, N, 1, a}

$\{x^2 \mid x \in \mathbb{N}\}$ // FullForm

```
List[Alternatives[Power[x, 2], Element[x, \[DoubleStruckCapitalN]]]]
```

Fortunately configurable!

$\underset{x}{\forall} P[x] \bigwedge Q[f[x], y]$

```
Syntax::sntxi :  Incomplete expression; more input is needed.
```

$\underset{x}{\forall} P[x] \bigwedge Q[f[x], y]$

Fortunately extensible!

$B * A$

$A\,B$

$5 * 2$

10

2^5

32

Fortunately programmable!

```
Needs["Theorema`"]
```

```
SetDelayed::write : Tag NotElement in NotElement[x$___] is Protected.
```

```
•[ 〈3, a, 2, N, 1, a〉 ]
```

```
〈3, a, 2, N, 1, a〉
```

```
•[ {3, a, 2, N, 1, a} ]
```

```
{3, a, 2, N, 1, a}
```

•[$\left\{x^2 \underset{x}{|} x \in \mathbb{N}\right\}$] // InputForm

```
™SetOf[•range[•simpleRange[•var[x]]],
 ™Element[•var[x], ™ℕ], ™Power[•var[x], 2]]
```

•[$\underset{x}{\forall} P[x] \bigwedge Q[f[x], y]$]

$\underset{x}{\forall} P[x] \bigwedge Q[f[x], y]$

```
•[ B∗A ]
```

```
B∗A
```

```
•[ 5∗2 ]
```

```
5∗2
```

•[2^5]

2^5

Semantics:

Algorithmic (executable) semantics is provided for the algorithmic part of the language.
Theorema semantics **can** be used in computations or in proofs.

2.1.2 *Theorema* Formal Text Language

Organization and structuring of mathematical items.

```
Definition["repeated operation on group", any[a, n],
  self[a, 0] := u                                  "base"
  (self[a, n] := a∘self[a, n − 1]) ⇐ is-natural[n]  "general" ]
```

```
Definition["reversed repeated operation", any[a, n], with[is-natural[n]],
  self-rev[n, a] := self[a, n]]
```

```
Definition["repeated operation on group"]
```

```
•def[repeated operation on group,
  •range[•simpleRange[a], •simpleRange[n]], True, •flist[•lf[base, self[a, 0] := u],
    •lf[general, (self[a, n] := a∘self[a, n − 1]) ⇐ IsNatural[n]]]]]
```

```
Axiom["unit element", any[a],
  a∘u = a   "right unit"
  u∘a = a   "left unit"  ]
```

```
Theory["group",
  Axiom["unit element"]
  Definition["repeated operation on group"]]
  Definition["reversed repeated operation"]
```

```
Built-in["multiplicative group",
  ^ → self]
```

```
Built-in["additive group",
  * → self-rev]
```

```
Theorem["Not over And", any[A, B],
  ¬ A ∨ ¬ B ⇒ ¬ (A ∧ B)]
```

2.1.3 *Theorema* User Language

Mathematical activities involving *Theorema* expressions and *Theorema* formal text entities
&
organizing the environment.

$$\text{Mathematical activity} := \begin{cases} \text{proving} & \rightarrow \ \text{Prove} \\ \text{computing} & \rightarrow \ \text{Compute} \\ \text{solving} & \rightarrow \ \text{Solve} \end{cases}$$

Uniform structure:

```
Prove[goal, using → KB, by → Method, built-in → additional knowledge]
```

```
Compute[expression, using → KB, by → Method, built-in → additional knowledge]
```

Computations using explicit knowledge:

```
Compute[self[a, 0]]
```

```
self[a, 0]
```

```
Compute[self[a, 0], using → Definition["repeated operation on group"]]
```

```
u
```

```
Compute[self[a, 5], using → Definition["repeated operation on group"]]
```

```
self[a, 5]
```

```
Compute[self[a, 5], using → Definition["repeated operation on group"],
  built-in → Built-in["Numbers"][is-natural]]
```

```
a∘self[a, 5 − 1]
```

```
Compute[self[a, 5], using → Definition["repeated operation on group"],
  built-in → Built-in["Numbers"][is-natural, −]]
```

```
a∘(a∘(a∘(a∘(a∘u))))
```

```
Compute[self[a, 5],
  using → ⟨Definition["repeated operation on group"], Axiom["unit element"]⟩,
  built-in → Built-in["Numbers"][is-natural, −]]
```

```
a∘(a∘(a∘(a∘a)))
```

```
Compute[self[a, 5], using → Theory["group"],
  built-in → Built-in["Numbers"][is-natural, −]]
```

```
a∘(a∘(a∘(a∘a)))
```

```
Use[⟨Theory["group"], Built-in["Numbers"][is-natural, −]⟩]
```

```
Compute[self[a, 5]]
```

```
a∘(a∘(a∘(a∘a)))
```

```
UseAlso[⟨Built-in["multiplicative group"], Built-in["additive group"]⟩]
```

```
Compute[2^5]
```

```
2∘(2∘(2∘(2∘2)))
```

```
Compute[5∗2]
```

```
2∘(2∘(2∘(2∘2)))
```

```
DoNotUse[⟨Built-in["multiplicative group"], Built-in["additive group"]⟩]
```

```
Compute[2^5,
  built-in → Built-in["Numbers"][^]]
```

```
32
```

```
Compute[2^500,
  built-in → Built-in["Numbers"][^]]
```

```
327339060789614187001318969682759915221664204604306478948329136809613∵
  379640467455488327009232590415715088668412756007100921725654588539З∵
  053328527589376
```

```
Use[]
```

```
Prove[Theorem["Not over And"], by → PredicateProver]
```

```
- ProofObject -
```

2.2 *Theorema* Proving Philosophy

- Multi-method system

"White-Box-Provers": Use inference rules similar to natural deduction rules. Proof generation and proof presentation is human-oriented.

  - ○ Propositional logic prover
  - ○ Predicate logic prover
  - ○ PCS prover (specialized for alternating quantifiers)
  - ○ Set theory prover
  - ○ Induction over natural numbers
  - ○ Induction over tuples
  - ○ Simplification prover
  - ○ …

"Black-Box-Provers": Transform proof problem and apply known techniques.

  - ○ Gröbner bases prover (geometry)
  - ○ Paule Schorn prover (identities involving $\sum$)
  - ○ Resolution prover
  - ○ Links to external systems (Otter, Vampire, Waldmeister, …)

- *Present* proofs in a human-like style.
- *Produce* proofs in a human-like style.

3 Some Examples

3.1 Set Theory

3.1.1 Pure Set Theory

Proposition["union powerset", any[A],
$\bigcup \mathcal{P}[A] = A$]

Prove[Proposition["union powerset"], by → SetTheoryPCSProver,
ProverOptions → {DisableProver → {STC}}]

- ProofObject -

Transform[%, TransformerOptions → {branches → Proved, steps → Useful}]

- ProofObject -

Proposition["intersection powerset",
$\bigcap \mathcal{P}[A] = \emptyset$]

Prove[Proposition["intersection powerset"], by → SetTheoryPCSProver,
transformBy → ProofSimplifier,
TransformerOptions → {branches → Proved, steps → Useful},
ProverOptions → {DisableProver → {STC}}]

- ProofObject -

Lemma["intersection indexed union",

$$\bigcup_{i \in \mathcal{I}} A_i \cap \bigcup_{j \in \mathcal{J}} B_j = \bigcup_{i \in \mathcal{I}} \left(\bigcup_{j \in \mathcal{J}} (A_i \cap B_j) \right)]$$

Prove[Lemma["intersection indexed union"],
by → SetTheoryPCSProver]

- ProofObject -

3.1.2 Mathematics Using Sets

Definition["reflexivity", any[~ , A],
is-reflexive$_A$[~] :⇔ $\underset{x \in A}{\forall}$ x ~ x]

Definition["class", any[x, A],
class$_A$[x] := {a ∈ A | a ~ x}]

Proposition["non−empty class", any[x ∈ A, A], with[is-reflexive$_A$[~]],
  class$_A$[x] ≠ ∅]

Proposition["in own class", any[x ∈ A, A], with[is-reflexive$_A$[~]],
  x ∈ class$_A$[x]]

```
IsSet[•[class_[___]]] := True;
Prove[Proposition["in own class"],
  by → SetTheoryPCSProver,
  using → ⟨Definition["reflexivity"], Definition["class"]⟩,
  ProverOptions → {GRWTarget → {"goal", "kb"}, ApplyBuiltIns → {"goal"}}]
```

- ProofObject -

```
Prove[Proposition["non−empty class"],
  by → SetTheoryPCSProver,
  using → ⟨Definition["reflexivity"], Definition["class"]⟩,
  ProverOptions → {GRWTarget → {"goal", "kb"},
      RWInsideQuantifiers → True, ApplyBuiltIns → {"goal"}}, SearchDepth → 40]
```

- ProofObject -

3.2 PCS

Definition["sum of sequences/functions", any[f, g, x],
  (f + g)[x] = f[x] + g[x]]

Definition["continuity", any[f, x],

$$\text{continuous}[f, x] :\Leftrightarrow \underset{\substack{\epsilon \\ \epsilon>0}}{\forall}\ \underset{\substack{\delta \\ \delta>0}}{\exists}\ \underset{\substack{y \\ |y-x|<\delta}}{\forall}\ |f[y] - f[x]| < \epsilon\Big]$$

Lemma["distance of sum", any[x, y, z, t, δ, ϵ],
  $|(x + z) - (y + t)| < (\delta + \epsilon) \Leftarrow (|x - y| < \delta \wedge |z - t| < \epsilon)$]

Lemma["mininum, greater", any[m, M1, M2],
  min[M1, M2] > m ⇔ (M1 > m ∧ M2 > m)]

Lemma["mininum, less", any[m, M1, M2],
  (m < M1 ∧ m < M2) ⇔ m < min[M1, M2]]

Proposition["continuity", any[f, g, x],
  continuous[f, x] ∧ continuous[g, x] ⇒ continuous[f + g, x]]

```
Prove[Proposition["continuity"], using → ⟨Definition["continuity"],
      Lemma["distance of sum"], Definition["sum of sequences/functions"],
      Lemma["mininum, less"], Lemma["mininum, greater"]⟩,
  by →
    PCS]
```

- ProofObject -

3.3 Gröbner Bases

Formula["Geometry", any[x, y],

$$((x^3\,y^4 + 27\,xy^3 - 15\,x^3) = 0) \bigwedge \left(\left(\frac{1}{5}\,x^2\,y - 23\,x\,y + 17\right) = 0\right) \Rightarrow$$

$$\left(\left(\left(\left(17 + -23\,x\,y + \frac{x^2\,y}{5}\right)(15\,x\,y + x^2\,y^2) + (-15 + x\,y)(-15\,x^3 + 27\,xy^3 + x^3\,y^4)\right) = 0\right)\right]$$

Prove[Formula["Geometry"], by → GroebnerBasesProver]

- ProofObject -

3.4 Algorithmic Mathematics

A *complete implementation* of the Gröbner bases algorithm (⟶ Davenport course).

Definition["Exponent tuples", any[n],
PP[n] = Functor[ET, any[p1, p2],

$$\frac{\mathbb{s} = \langle\rangle}{}$$

$$\left(p1 \underset{ET}{<} p2\right) :\Leftrightarrow \underset{i=1,\ldots,n}{\exists} \left(p1_i < p2_i \bigwedge \underset{j=1,\ldots,i-1}{\forall} (p1_j = p2_j)\right)$$

$$p1 \underset{ET}{*} p2 := \left\langle p1_i + p2_i \underset{i=1,\ldots,n}{|} \right\rangle$$

$$p1 \underset{ET}{/} p2 := \left\langle p1_i - p2_i \underset{i=1,\ldots,n}{|} \right\rangle$$

$$\left(p1 \underset{ET}{|} p2\right) :\Leftrightarrow \underset{i=1,\ldots,n}{\forall} p1_i \leq p2_i$$

$$\underset{ET}{\mathrm{lcm}}[p1, p2] := \left\langle \begin{cases} p1_i & \Leftarrow \; p1_i \geq p2_i \\ p2_i & \Leftarrow \; \text{otherwise} \end{cases} \underset{i=1,\ldots,n}{\Bigg|} \right\rangle$$

]]

General::spell1 :
Possible spelling error: new symbol name "lcm" is similar to existing symbol "LCM".

$\langle 1,0,3\rangle$ stands for $x^1\,y^0\,z^3$.

(Lexicographic ordering, parametrized domain would allow the choice of term order.)

Definition["Monomials", any[K, n],

Mon[K, n] = Functor[M, any[c1, c2, p1, p2, m1, m2],

$$\begin{array}{l}
\mathbb{s} = \langle\rangle \\
\hline
\left(\langle \mathrm{c1}, \mathrm{p1}\rangle \underset{\mathrm{M}}{<} \langle \mathrm{c2}, \mathrm{p2}\rangle\right) :\Leftrightarrow \mathrm{p1} \underset{\mathrm{PP[n]}}{<} \mathrm{p2} \\
\langle \mathrm{c1}, \mathrm{p1}\rangle \underset{\mathrm{M}}{+} \langle \mathrm{c2}, \mathrm{p1}\rangle := \left\langle \mathrm{c1} \underset{\mathrm{K}}{+} \mathrm{c2}, \mathrm{p1}\right\rangle \\
\langle \mathrm{c1}, \mathrm{p1}\rangle \underset{\mathrm{M}}{-} \langle \mathrm{c2}, \mathrm{p1}\rangle := \left\langle \mathrm{c1} \underset{\mathrm{K}}{-} \mathrm{c2}, \mathrm{p1}\right\rangle \\
\underset{\mathrm{M}}{-}[\langle \mathrm{c1}, \mathrm{p1}\rangle] := \left\langle \underset{\mathrm{K}}{-}[\mathrm{c1}], \mathrm{p1}\right\rangle \\
\langle \mathrm{c1}, \mathrm{p1}\rangle \underset{\mathrm{M}}{*} \langle \mathrm{c2}, \mathrm{p2}\rangle := \left\langle \mathrm{c1} \underset{\mathrm{K}}{*} \mathrm{c2}, \mathrm{p1} \underset{\mathrm{PP[n]}}{*} \mathrm{p2}\right\rangle \\
\langle \mathrm{c1}, \mathrm{p1}\rangle \underset{\mathrm{M}}{/} \langle \mathrm{c2}, \mathrm{p2}\rangle := \left\langle \mathrm{c1} \underset{\mathrm{K}}{/} \mathrm{c2}, \mathrm{p1} \underset{\mathrm{PP[n]}}{/} \mathrm{p2}\right\rangle \\
\left(\langle \mathrm{c1}, \mathrm{p1}\rangle \underset{\mathrm{M}}{\mid} \langle \mathrm{c2}, \mathrm{p2}\rangle\right) :\Leftrightarrow \mathrm{p1} \underset{\mathrm{PP[n]}}{\mid} \mathrm{p2} \\
\underset{\mathrm{M}}{\mathrm{lcm}}[\langle \mathrm{c1}, \mathrm{p1}\rangle, \langle \mathrm{c2}, \mathrm{p2}\rangle] := \left\langle \mathrm{c1} \underset{\mathrm{K}}{*} \mathrm{c2}, \underset{\mathrm{PP[n]}}{\mathrm{lcm}}[\mathrm{p1}, \mathrm{p2}]\right\rangle \\
\underset{\mathrm{M}}{\text{is-zero}}[\langle \mathrm{c1}, \mathrm{p1}\rangle] :\Leftrightarrow \left(\mathrm{c1} = \underset{\mathrm{K}}{0}\right) \\
]]
\end{array}$$

$\langle 5, \langle 1, 0, 3\rangle\rangle$ stands for $5\, x\, z^3$.

Definition["Polynomials", any[M],
Poly[M] = Functor[P, any[c, p, r̄, m, m1, m2, $\overline{r1}$, $\overline{r2}$, p1, p2],

$$\mathbb{s} = \langle\rangle$$

$$\begin{array}{l}
\mathrm{lpp}[\langle\langle c, p\rangle, \bar{r}\rangle] := p \\
\mathrm{lcoef}[\langle\langle c, p\rangle, \bar{r}\rangle] := c \\
\mathrm{lmon}[\langle m, \bar{r}\rangle] := m \\
\mathrm{rp}[\langle m, \bar{r}\rangle] := \langle \bar{r}\rangle \\
\langle\rangle \underset{P}{+} p := p \\
p \underset{P}{+} \langle\rangle := p
\end{array}$$

$$\langle m1, \overline{r1}\rangle \underset{P}{+} \langle m2, \overline{r2}\rangle := \begin{cases} m2 \smile \left(\langle m1, \overline{r1}\rangle \underset{P}{+} \langle\overline{r2}\rangle\right) & \Leftarrow\ m1 \underset{M}{<} m2 \\ m1 \smile \left(\langle\overline{r1}\rangle \underset{P}{+} \langle m2, \overline{r2}\rangle\right) & \Leftarrow\ m2 \underset{M}{<} m1 \\ \mathrm{where}\Big[s = m1 \underset{M}{+} m2, & \Leftarrow\ \text{otherwise} \\ \quad \begin{cases} \langle\overline{r1}\rangle \underset{P}{+} \langle\overline{r2}\rangle & \Leftarrow\ \underset{M}{\text{is-zero}}[s] \\ s \smile \left(\langle\overline{r1}\rangle \underset{P}{+} \langle\overline{r2}\rangle\right) & \Leftarrow\ \text{otherwise} \end{cases} \Big] & \end{cases}$$

$$\begin{array}{l}
\underset{P}{-}[\langle\rangle] := \langle\rangle \\
\underset{P}{-}[p] := \left\langle \underset{M}{-}[p_i] \;\Big|_{i=1,\ldots,|p|} \right\rangle \\
\langle\rangle \underset{P}{-} p := \underset{P}{-}[p] \\
p \underset{P}{-} \langle\rangle := p
\end{array}$$

$$\langle m1, \overline{r1}\rangle \underset{P}{-} \langle m2, \overline{r2}\rangle := \begin{cases} \underset{M}{-}[m2] \smile \left(\langle m1, \overline{r1}\rangle \underset{P}{-} \langle\overline{r2}\rangle\right) & \Leftarrow\ m1 \underset{M}{<} m2 \\ m1 \smile \left(\langle\overline{r1}\rangle \underset{P}{-} \langle m2, \overline{r2}\rangle\right) & \Leftarrow\ m2 \underset{M}{<} m1 \\ \mathrm{where}\Big[s = m1 \underset{M}{-} m2, & \Leftarrow\ \text{otherwise} \\ \quad \begin{cases} \langle\overline{r1}\rangle \underset{P}{-} \langle\overline{r2}\rangle & \Leftarrow\ \underset{M}{\text{is-zero}}[s] \\ s \smile \left(\langle\overline{r1}\rangle \underset{P}{-} \langle\overline{r2}\rangle\right) & \Leftarrow\ \text{otherwise} \end{cases} \Big] & \end{cases}$$

$$\begin{array}{l}
m \underset{P}{*} \langle\rangle := \langle\rangle \\
m \underset{P}{*} p := \left\langle m \underset{M}{*} p_i \;\Big|_{i=1,\ldots,|p|} \right\rangle
\end{array}$$

$$\underset{P}{\mathrm{normalized}}[p] := \mathrm{where}\Big[lc = \mathrm{lcoef}[p], \left\langle p_i \underset{M}{/} \left\langle lc, \left\langle 0 \;\Big|_{j=1,\ldots,|\mathrm{lpp}[p]|} \right\rangle\right\rangle \;\Bigg|_{i=1,\ldots,|p|} \right\rangle\Big]$$

]]

⟨⟨5, ⟨1, 0, 3⟩⟩, ⟨−4, ⟨0, 0, 2⟩⟩⟩ stands for $5\,x\,z^3 - 4\,z^2$. Monomials must be ordered appropriately. Arithmetic operations preserve the ordering.

Definition["Reduction domain", any[P, M],

ReductionDomain[P[M]] = Functor[R, any[p, S, All, r, $\overline{\text{S}}$],

$$\frac{\mathbb{s} = \langle\rangle}{\underset{\text{R}}{\text{partial-normal-form}}[\text{p, S}] := \underset{\text{R}}{\text{partial-normal-form}}[\text{p, S, S}]}$$

$$\underset{\text{R}}{\text{partial-normal-form}}[\text{p}, \langle\rangle, \text{All}] := \text{p}$$

$$\underset{\text{R}}{\text{partial-normal-form}}[\langle\rangle, \text{S, All}] := \langle\rangle$$

$$\underset{\text{R}}{\text{partial-normal-form}}[\text{p}, \langle \text{r}, \overline{\text{S}}\rangle, \text{All}] :=$$

$$\begin{cases} \underset{\text{R}}{\text{partial-normal-form}}\Big[\text{rp[p]} \underset{\text{P[M]}}{-} & \Leftarrow \ \text{lmon[r]} \underset{\text{M}}{|} \text{lmon[p]} \\ \quad \left(\left(\text{lmon[p]} \underset{\text{M}}{/} \text{lmon[r]}\right) \underset{\text{P[M]}}{*} \text{rp[r]}\right), \text{All}\Big] & \\ \underset{\text{R}}{\text{partial-normal-form}}[\text{p}, \langle\overline{\text{S}}\rangle, \text{All}] & \Leftarrow \ \text{otherwise} \end{cases}$$

$$\underset{\text{R}}{\text{complete-normal-form}}[\langle\rangle, \text{S}] := \langle\rangle$$

$$\underset{\text{R}}{\text{complete-normal-form}}[\text{p, S}] := \text{where}\Big[\text{pnf} = \underset{\text{R}}{\text{partial-normal-form}}[\text{p, S}],$$

$$\begin{cases} \langle\rangle & \Leftarrow \ \text{pnf} = \langle\rangle \\ \text{lmon[pnf]} \smile \underset{\text{R}}{\text{complete-normal-form}}[\text{rp[pnf], S}] & \Leftarrow \ \text{otherwise} \end{cases} \Big]$$

]]

Definition["S-Polynomial", any[f, g, K, n],

S-Polynomial[f, g, K, n] :=

$$\text{where}\Big[\text{lmf} = \text{lmon[f]}, \text{lmg} = \text{lmon[g]}, \text{lcmmon} = \underset{\text{Mon[K,n]}}{\text{lcm}}[\text{lmf, lmg}],$$

$$\left(\left(\text{lcmmon} \underset{\text{Mon[K,n]}}{/} \text{lmon[f]}\right) \underset{\text{Poly[Mon[K,n]]}}{*} \text{f}\right) \underset{\text{Poly[Mon[K,n]]}}{-}$$

$$\left(\left(\text{lcmmon} \underset{\text{Mon[K,n]}}{/} \text{lmon[g]}\right) \underset{\text{Poly[Mon[K,n]]}}{*} \text{g}\right)\Big]\Big]$$

Definition["Polynomial pairs", any[P, p],

$$\text{all-pairs[P]} := \left\langle \left(\left\langle \text{P}_\text{i}, \text{P}_\text{j} \right\rangle \underset{\text{j=i+1,…,|P|}}{|} \right) \underset{\text{i=1,…,|P|}}{\Big|} \right\rangle \Big]$$

$$\text{new-pairs[p, P]} := \left\langle \left\langle \text{p}, \text{P}_\text{i} \right\rangle \underset{\text{i=1,…,|P|}}{|} \right\rangle$$

Algorithm["Gröbner Basis", any[F, K, n, P, p1, p2, r̄],

Gröbner-Basis[F, K, n] := Gröbner-Basis[F, all-pairs[F], K, n]
Gröbner-Basis[F, ⟨⟩, K, n] := F
Gröbner-Basis[F, ⟨⟨p1, p2⟩, r̄⟩, K, n] :=
where[sp = S-Polynomial[p1, p2, K, n],

$$\text{nf} = \underset{\text{ReductionDomain[Poly[Mon[K,n]]]}}{\text{complete-normal-form}}[\text{sp}, \text{F}],$$

$$\begin{cases} \text{Gröbner-Basis}[\text{F}, \langle\bar{\text{r}}\rangle, \text{K}, \text{n}] & \Leftarrow \text{nf} = \langle\rangle \\ \text{Gröbner-Basis}[\text{nf} \smile \text{F}, \text{new-pairs}[\text{nf}, \text{F}] \asymp \langle\bar{\text{r}}\rangle, \text{K}, \text{n}] & \Leftarrow \text{otherwise} \end{cases}\Big]\Big]$$

Algorithm["Reduced Gröbner Basis", any[F, G, K, n],

Deleted-Multiples[G, K, n] :=

$$\left\langle \underset{\text{Poly[Mon[K,n]]}}{\text{normalized}}[\text{G}_\text{i}] \;\Big|_{\text{i}=1,\ldots,|\text{G}|}\; \underset{\substack{\text{j}=1,\ldots,|\text{G}|\\ \text{j}\neq\text{i}}}{\forall} \neg\left(\text{lmon}[\text{G}_\text{j}] \underset{\text{Mon[K,n]}}{\mid} \text{lmon}[\text{G}_\text{i}]\right)\right\rangle$$

$$\text{Interreduced}[\text{G}, \text{K}, \text{n}] := \left\langle \underset{\text{ReductionDomain[Poly[Mon[K,n]]]}}{\text{complete-normal-form}}\left[\text{G}_\text{i}, \left\langle \text{G}_\text{j} \underset{\text{j}=1,\ldots,|\text{G}|}{\mid} \text{j} \neq \text{i}\right\rangle\right] \;\Big|_{\text{i}=1,\ldots,|\text{G}|} \right\rangle \Big]$$

Reduced-Gröbner-Basis[F, K, n] :=
Interreduced[Deleted-Multiples[Gröbner-Basis[F, K, n], K, n], K, n]

Use[⟨Algorithm["Reduced Gröbner Basis"], Algorithm["Gröbner Basis"],
Definition["Polynomial pairs"], Definition["S-Polynomial"],
Definition["Reduction domain"], Definition["Polynomials"],
Definition["Monomials"], Definition["Exponent tuples"],
Built-in["Quantifiers"], Built-in["Connectives"], Built-in["Tuples"],
Built-in["Sets"], Built-in["Numbers"], Built-in["Number Domains"]⟩]

Compute[
S-Polynomial[⟨⟨1, ⟨1, 0⟩⟩, ⟨1, ⟨0, 1⟩⟩, ⟨−1, ⟨0, 0⟩⟩⟩, ⟨⟨1, ⟨1, 1⟩⟩, ⟨−3, ⟨0, 0⟩⟩⟩, ℚ, 2]]

⟨⟨1, ⟨0, 2⟩⟩, ⟨−1, ⟨0, 1⟩⟩, ⟨3, ⟨0, 0⟩⟩⟩

Compute[Gröbner-Basis[
⟨⟨⟨1, ⟨1, 0⟩⟩, ⟨1, ⟨0, 1⟩⟩, ⟨−1, ⟨0, 0⟩⟩⟩, ⟨⟨1, ⟨1, 1⟩⟩, ⟨−3, ⟨0, 0⟩⟩⟩⟩, ℚ, 2]]

⟨⟨⟨1, ⟨0, 2⟩⟩, ⟨−1, ⟨0, 1⟩⟩, ⟨3, ⟨0, 0⟩⟩⟩,
⟨⟨1, ⟨1, 0⟩⟩, ⟨1, ⟨0, 1⟩⟩, ⟨−1, ⟨0, 0⟩⟩⟩, ⟨⟨1, ⟨1, 1⟩⟩, ⟨−3, ⟨0, 0⟩⟩⟩⟩

GroebnerBasis[{x + y − 1, x y − 3}, {x, y}]

$\{(-3) + y + -y^2, (-1) + x + y\}$

Compute[Reduced-Gröbner-Basis[
⟨⟨⟨1, ⟨1, 0⟩⟩, ⟨1, ⟨0, 1⟩⟩, ⟨−1, ⟨0, 0⟩⟩⟩, ⟨⟨1, ⟨1, 1⟩⟩, ⟨−3, ⟨0, 0⟩⟩⟩⟩, ℚ, 2]]

⟨⟨⟨1, ⟨0, 2⟩⟩, ⟨−1, ⟨0, 1⟩⟩, ⟨3, ⟨0, 0⟩⟩⟩, ⟨⟨1, ⟨1, 0⟩⟩, ⟨1, ⟨0, 1⟩⟩, ⟨−1, ⟨0, 0⟩⟩⟩⟩

```
Compute[Reduced-Gröbner-Basis[
        ⟨⟨⟨3, ⟨1, 2⟩⟩, ⟨2, ⟨1, 1⟩⟩, ⟨1, ⟨1, 0⟩⟩, ⟨9, ⟨0, 2⟩⟩, ⟨5, ⟨0, 1⟩⟩, ⟨−3, ⟨0, 0⟩⟩⟩,
          ⟨⟨2, ⟨1, 3⟩⟩, ⟨−1, ⟨1, 1⟩⟩, ⟨−1, ⟨1, 0⟩⟩, ⟨6, ⟨0, 3⟩⟩,
            ⟨−2, ⟨0, 2⟩⟩, ⟨−3, ⟨0, 1⟩⟩, ⟨3, ⟨0, 0⟩⟩⟩,
          ⟨⟨1, ⟨1, 3⟩⟩, ⟨1, ⟨1, 2⟩⟩, ⟨3, ⟨0, 3⟩⟩, ⟨2, ⟨0, 2⟩⟩⟩⟩, ℚ, 2]] // Timing
```

$$\left\{14.48\ \text{Second}, \left\langle\left\langle\langle 1, \langle 0, 3\rangle\rangle, \left\langle\frac{-5}{2}, \langle 0, 2\rangle\right\rangle, \left\langle\frac{-5}{2}, \langle 0, 1\rangle\right\rangle\right\rangle,\right.\right.$$
$$\left.\left.\left\langle\langle 1, \langle 1, 0\rangle\rangle, \langle 1, \langle 0, 2\rangle\rangle, \left\langle\frac{-3}{2}, \langle 0, 1\rangle\right\rangle, \langle -3, \langle 0, 0\rangle\rangle\right\rangle\right\rangle\right\}$$

$$\begin{array}{l}\text{GroebnerBasis}[\\ \quad \{3\,x\,y^2 + 2\,x\,y + x + 9\,y^2 + 5\,y - 3,\ 2\,x\,y^3 - x\,y - x + 6\,y^3 - 2\,y^2 - 3\,y + 3,\\ \qquad x\,y^3 + x\,y^2 + 3\,y^3 + 2\,y^2\},\ \{x, y\}]\ //\ \text{Timing}\end{array}$$

$$\{0.02\ \text{Second}, \{-5\,y + -5\,y^2 + 2\,y^3,\ 6 + -2\,x + 3\,y + -2\,y^2\}\}$$

```
Use[]
```