the
abdus salam
international centre for theoretical physics

ICTP 40th Anniversary

SMR1576/3

Advanced School and Conference on Non-commutative Geometry

(9 - 27 August 2004)

An Introduction to the Commutative and Non-commutative Computer Algebra: Gröbner bases as a Tool for Homological Algebra

V. Levandovskyy, G. Pfister

Center for Computer Algebra
Fachbereich Mathematik
Universität Kaiserslautern
D-67653 Kaiserslautern
Germany

These are preliminary lecture notes, intended only for distribution to participants

An Introduction to the Commutative and Non–commutative Computer Algebra: Gröbner bases as a Tool for Homological Algebra

Viktor Levandovskyy, Gerhard Pfister
Center for Computer Algebra
Fachbereich Mathematik
Universität Kaiserslautern
D-67653 Germany

1 Introducing Gröbner-ready Algebras

1.1 Ordering on Monomials and Exponents

Let $\mathbf{N} = (\mathbb{N}^n, +)$ be an additive monoid with the neutral element $\mathbf{0} = (0, \ldots, 0)$.

Let $\mathbb{K}$ be a field and $\mathbf{R} = (\mathbb{K}[x_1, \ldots, x_n], +, \cdot)$ be a commutative polynomial ring in n variables.

As a $\mathbb{K}$–vectorspace, $\mathbf{R}$ is infinite–dimensional with the $\mathbb{K}$–basis $\{x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} \mid \alpha_k \geq 0\}$. Let us call an element of such $\mathbb{K}$–basis **a monomial** and use a shortcut $x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. We call such α **an exponent vector** of a monomial x^α.

Indeed, the set of monomials $\mathrm{Mon}(\mathbf{R})$ is in one–to–one correspondence with the set of n–tuples of natural numbers via

$$\mathrm{Mon}(\mathbf{R}) \ni \ x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} \longmapsto (\alpha_1, \alpha_2, \ldots, \alpha_n) = \alpha \ \in \mathbb{N}^n.$$

We can write every $f \in \mathbf{R}$ conveniently via $f = \sum_{\alpha \in \Lambda} c_\alpha x^\alpha$, where $c_\alpha \in \mathbb{K}$ and $\Lambda \subset \mathbb{N}^n$ is finite.

Now we have to order monomials, and we'll do it via their exponent vectors.

Definition 1.1. Let $\prec$ be a total ordering on $\mathbb{N}^n$.

1. An ordering $\prec$ is called **a well–ordering**, if $\forall \alpha \in \mathbb{N}^n$ there exist finitely many $\beta \in \mathbb{N}^n$, such that $b \prec a$. Then, 0 is the smallest element in $\mathbb{N}^n$ with respect to any well–ordering $\prec$.

2. An ordering $\prec$ on $\mathbb{N}^n$ induces an ordering $<$ on $\mathrm{Mon}(\mathbf{R})$ by
$$\forall\ \alpha, \beta \in \mathbb{N}^n,\ \alpha \prec \beta \Rightarrow x^\alpha < x^\beta.$$
$<$ is called **a monomial ordering** on R, if it is compatible with the multiplicative structure of R, that is
$\forall\ \alpha, \beta, \gamma \in \mathbb{N}^n$ such that $x^\alpha \prec x^\beta$ we have $x^{\alpha+\gamma} < x^{\beta+\gamma}$.

One of the most known orderings is the **lexicographical ordering**, which we denote by `lp`:

$x^\beta <_{\mathrm{lp}} x^\alpha \overset{\text{def}}{\iff}$ the first non–zero entry of $\alpha - \beta$ is positive.

For any monomial ordering $<$ there exists a (non–unique) matrix $A \in \mathrm{GL}(n, \mathbb{R})$ such that $\beta < \alpha$ if and only if $A \cdot \beta <_{\mathrm{lp}} A \cdot \alpha$.

In the sequel, we will give matrices for all ordering we mention.

$$\texttt{lp} \sim \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}, \texttt{Dp} \sim \begin{pmatrix} 1 & \dots & 1 & 1 \\ 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \end{pmatrix}, \texttt{Wp} \sim \begin{pmatrix} \omega_1 & \dots & \omega_{n-1} & \omega_n \\ 1 & \dots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \dots & 1 & 0 \end{pmatrix}$$

$$\texttt{dp} \sim \begin{pmatrix} 1 & 1 & .. & 1 \\ 0 & 0 & .. & -1 \\ \vdots & \vdots & \iddots & \vdots \\ 0 & -1 & .. & 0 \end{pmatrix}, \texttt{wp} \sim \begin{pmatrix} \omega_1 & \omega_2 & .. & \omega_n \\ 0 & 0 & .. & -1 \\ \vdots & \vdots & \iddots & \vdots \\ 0 & -1 & .. & 0 \end{pmatrix}.$$

Here, `dp` denotes a **degree reverse lexicographical ordering**, which could be also defined as

$x^\beta <_{\mathrm{dp}} x^\alpha \overset{\text{def}}{\iff} \deg x^\beta < \deg x^\alpha$ or $\deg x^\alpha = \deg x^\beta$ and the last non–zero entry of $\alpha - \beta$ is negative.

Definition 1.2. Let $<$ be a monomial ordering. Then, any $f \in \mathbf{R} \setminus \{0\}$ can be written uniquely as $f = c_\alpha x^\alpha + f'$, with $c_\alpha \in \mathbb{K} \setminus \{0\}$ and $x^{\alpha'} < x^\alpha$ for any non–zero term $c_{\alpha'} x^{\alpha'}$ of f'. We define

$\mathrm{lm}(f)$	$= x^\alpha$,	the **leading monomial** of f,
$\mathrm{lc}(f)$	$= c_\alpha$,	the **leading coefficient** of f,
$\mathrm{le}(f)$	$= \alpha$,	the **leading exponent** of f.

The mapping $\mathrm{le} : \mathbf{R} \longrightarrow \mathbb{N}^n$, $f \mapsto \mathrm{le}(f) = \alpha$, has the following property: $\forall\ f, g \in \mathbf{R} \quad \mathrm{le}(f \cdot g) = \mathrm{le}(f) + \mathrm{le}(g)$. Equivalently, in form of monomials, $\forall\ f, g \in \mathbf{R} \quad \mathrm{lm}(f \cdot g) = \mathrm{lm}(f) \cdot \mathrm{lm}(g)$. This property hold trivially for any commutative ring $\mathbf{R}$, but what are the other structures, behaving like this?

1.2 (Almost Commutative) Non–commutative Structures

Let us take the same vectorspace as of $\mathbf{R}$, $\{x^\alpha \mid \alpha \in \mathbb{N}^n\}$, and think about an algebra A with this vectorspace as its $\mathbb{K}$–basis but with a different multiplication.

How different this multiplication could be?

Suppose the property $\mathrm{le}(f \cdot g) = \mathrm{le}(f) + \mathrm{le}(g)$ holds for all $f, g \in A$. Especially, it holds on the generators x_i, that is $\mathrm{le}(x_j x_i) = \mathrm{le}(x_i) + \mathrm{le}(x_j) = \mathrm{le}(x_i x_j)$ for any $j \neq i$. So, the relation between x_j and x_i becomes $x_j x_i = c_{ij} \cdot x_i x_j + d_{ij}$ for some nonzero constant c_{ij} and polynomial d_{ij}, such that $\mathrm{le}(d_{ij}) \prec \mathrm{le}(x_i) + \mathrm{le}(x_j)$.

We have fixed our $\mathbb{K}$–basis and hence we have declared elements $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ to be monomials. Hence, an element $x_2 x_1$ is not a monomial anymore, since, due to non-commutative relations, it could be written in terms of monomials, that is $x_2 x_1 = c_{12} x_1 x_2 + d_{12}$.

So, we can proceed with the non-commutativity as follows: $\forall 1 \leq i < j \leq n$, $x_j x_i = c_{ij} x_i x_j + d_{ij}$. Note, that there are relations, which c_{ij} and d_{ij} should satisfy: these relations ensure that $\{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ is the $\mathbb{K}$–basis of A.

Definition 1.3. Let $\mathbb{K}$ be a field and $R = \mathbb{K}[x_1, \ldots, x_n]$ be a commutative polynomial ring in n variables. Suppose there is a well–ordering $<$ on R and two sets of data: $C = \{c_{ij}\} \subset \mathbb{K} \setminus \{0\}$ and $D = \{d_{ij}\} \subset R$ (here $1 \leq i < j \leq n$).

We can associate to the data $(R, <, C, D)$ a non–commutative algebra

$$A = \mathbb{K}\langle x_1, \ldots, x_n \mid \ \forall\, i < j \ \ x_j x_i = c_{ij} x_i x_j + d_{ij} \rangle.$$

A is called **a G–algebra** (in n variables), if the following conditions hold:

- $\forall\ i < j\ \ \mathrm{lm}(d_{ij}(\underline{x})) < x_i x_j$,
- $\forall\ 1 \leq i < j < k \leq n$,

$$c_{ik}c_{jk} \cdot d_{ij}x_k - x_k d_{ij} + c_{jk} \cdot x_j d_{ik} - c_{ij} \cdot d_{ik}x_j + d_{jk}x_i - c_{ij}c_{ik} \cdot x_i d_{jk} = 0$$

If all $d_{ij} = 0$, we call an algebra **quasi–commutative**.

If all $c_{ij} = 1$, we are dealing with an **algebra of Lie type**.

If all $c_{ij} = 1$ and $d_{ij} = 0$, algebra is commutative.

Theorem 1.4. Let A be a G–algebra. Then

1) A is left and right Noetherian,

2) A is an integral domain.

We regard a G–algebra (in n variables) as a generalization of a commutative polynomial ring in n variables. For any proper two–sided ideal $J \subset A$, we define a factor–algebra $B = A/J$. Algebras of this type are called GR–algebras, that is, Gröbner–ready algebras.

1.3 Properties of Leading Functions

Although R and A have similar properties (in particular, $\mathrm{Mon}(R) = \mathrm{Mon}(A)$), there are several crucial differences.

Multiplicativity of lm:

In the commutative ring R, lm enjoys the following property:

$\forall\ f, g \in R\ \ \mathrm{lm}(f \cdot g) = \mathrm{lm}(f) \cdot \mathrm{lm}(g)$.

In a G–algebra A, a product of two monomials is, in general, a polynomial. But nevertheless, the weaker property holds:

$\forall\ f, g \in A\ \ \mathrm{lm}(f \cdot g) = \mathrm{lm}(\mathrm{lm}(f) \cdot \mathrm{lm}(g)) = \mathrm{lm}(g \cdot f)$.

Meanwhile, in terms of exponents both properties mean

$$\forall\ f, g \in A,\ \forall\ f, g \in R,\ \ \mathrm{le}(f \cdot g) = \mathrm{le}(f) + \mathrm{le}(g).$$

So, we are going to work rather with exponents than with monomials.

Non–additivity of lm:

If $\mathrm{lm}(g) = \mathrm{lm}(f)$, $\mathrm{lc}(f) = -\,\mathrm{lc}(g)$, $\mathrm{lm}(f+g) < \max_<(\mathrm{lm}(f), \mathrm{lm}(g))$.
For all other $f, g \in A$, $\mathrm{lm}(f+g) = \max_<(\mathrm{lm}(f), \mathrm{lm}(g))$.

Properties of lc:

For all $f, g \in A \quad \mathrm{lc}(f \cdot g) = \mathrm{lc}\big(\mathrm{lm}(f) \cdot \mathrm{lm}(g)\big) \cdot \mathrm{lc}(f) \cdot \mathrm{lc}(g)$.
However, in algebras of Lie type ($c_{ij} = 1, \forall j > i$), we have
$\mathrm{lc}(f \cdot g) = \mathrm{lc}(f) \cdot \mathrm{lc}(g)$.

2 Why Do We Need Non–commutative Algebras?

Let us illustrate the ubiquity of non–commutativity, say, in differential equations.

Let t be a variable and ∂ denotes the operator of a differentiation wrt t, $\frac{\partial}{\partial t}$ or $\frac{d}{dt}$, depending on the context.

For any function $f \in C^\infty(t)$, we introduce an operator F, $F(t) = f \cdot t$, that is F is an operator of left multiplication by f. We call f a **representative** of F. In general, operators F and ∂ do not commute, but still there is a relation between two actions.

Lemma 2.1. $\partial \circ F = F \circ \partial + \partial(f)$.

Proof. $\forall\ h \in C^\infty(t)$, we have the following:

$$(\partial \circ F)(h) = \partial(f \cdot h) = f \cdot \partial(h) + \partial(f) \cdot h = (F \circ \partial)(h) + \partial(f) \cdot (h),$$

hence $\partial \circ F = F \circ \partial + \partial(f)$. □

In the sequel, we will denote both operator and its representative by the same letter.

Example 2.2.

1. Taking t and $d = \frac{d}{dt}$ as variables, we obtain the algebra

$A_1 = \mathbb{K}\langle t, d \mid dt = td + 1\rangle$, *a first Weyl algebra* — a very famous object in mathematics. Note, that n–th Weyl algebra is defined to be $A_n = \mathbb{K}\langle x_1, \ldots, x_n, \partial_1, \ldots, \partial_n \mid \partial_i x_j = x_j \partial_i + \delta_{ij}\rangle$, where δ_{ij} is the Kronecker symbol ($\delta_{jj} = 1$ and $\delta_{ij} = 0$, $\forall\ i \neq j$). Here, ∂_i could be viewed as an operator of partial differentiation $\frac{\partial}{\partial x_i}$.

2. Let e denotes the operator $e^{\lambda t}$, where λ considered as a parameter. Then there is an *exponential algebra*

$$E = \mathbb{K}(\lambda)\langle e, \partial \mid \partial \cdot e = e \cdot \partial + \lambda e\rangle.$$

Both examples **1** and **2** are G–algebras for any degree well–ordering.

3. Let sin denotes the operator with the representative $sin(t)$, then $\partial \cdot sin = sin \cdot \partial + cos$ and hence we need the variable cos, corresponding to the operator $cos(t)$. Then, $\partial \cdot cos = cos \cdot \partial - sin$ and there is an algebra

$$T^0 = \mathbb{K}\langle sin, cos, \partial \mid \partial \cdot cos = cos \cdot \partial - sin, \partial \cdot sin = sin \cdot \partial + cos, cos \cdot sin = sin \cdot cos\rangle.$$

A direct computation shows that the element $c = sin^2 + cos^2$ commutes with ∂ (even more, it generates the *center* of T^0). Hence, we should take the factor–algebra by the the ideal, generated by $sin^2 + cos^2 - 1$. In such a way we obtain

a *trigonometric algebra* $T = T^0/\langle sin^2 + cos^2 - 1\rangle$.

This algebra is a GR–algebra for any degree well–ordering.

4. Consider the operator ln, assigned to the natural logarithm $\ln(t)$. Then, $\partial \cdot ln = ln \cdot \partial + t^{-1}$. Adding $s := t^{-1}$ as a variable, we obtain

a *logarithmic algebra*:

$$L = \mathbb{K}\langle s, ln, \partial \mid \partial \cdot s = s \cdot \partial - s^2, \partial \cdot ln = ln \cdot \partial + s, ln \cdot s = s \cdot ln\rangle.$$

Note, that in order to be a G–algebra, the monomial ordering $<$ should satisfy the property $s^2 < s\partial \Leftrightarrow s < \partial$.

3 Gröbner bases

Since a commutative ring R is a special case of a G–algebra A, we will say, when talking about R, "the case when A is commutative".

We will write all the multiplications from the algebra from the left, since it makes no difference in the commutative case, and we will work with left ideals in A. The whole theory could be also formulated for the right side just changing sides in the text below.

3.1 From Divisibility to Normal Form

Let A be a G–algebra in n variables.

Let us start with the divisibility of monomials.

Definition 3.1. Let $m_1 = x^\alpha$ and $m_2 = x^\beta$ be two monomials from A. We say that m_1 **divides** m_2 (and denote it by $m_1 \mid m_2$), if $\alpha_i \leq \beta_i \; \forall i = 1 \dots n$.

When A is commutative, there is $p \in \mathrm{Mon}(A)$ such that $m_2 = p \cdot m_1$. Otherwise, it means that m_2 is reducible by m_1, i.e. there exist $c \in \mathbb{K} \setminus \{0\}$, $p \in \mathrm{Mon}(A)$ and $r \in A$ such that $\mathrm{lm}(r) < m_1$ and $m_2 = c \cdot p \cdot m_1 + r$.

Example 3.2. Let us take two exponent vectors $\alpha = (1, 1)$ and $\beta = (1, 2)$ from $\mathbb{N}^2$. Then in any algebra in two generators, say, $\{x, \partial\}$, we have $m_1 := x\partial \mid x\partial^2 =: m_2$, but the division of one by another gives quite different answers in different algebras.

In the commutative polynomial ring $R = \mathbb{K}[x, \partial]$, we have $m_2 = \partial m_1$.

In the first quantized Weyl algebra $A_q = \mathbb{K}(q)\langle x, \partial \mid \partial x = q^2 x\partial + 1\rangle$, we obtain $m_2 = q^{-2} \cdot \partial \cdot m_1 - q^{-2}\partial$.

Definition 3.3. Let x^α and x^β be two monomials from A. For $\forall 1 \leq i \leq n$, set $\mu_i = \max(\alpha_i, \beta_i)$ and $\mu := \mu(\alpha, \beta) = (\mu_1, \dots, \mu_n) \in \mathbb{N}^n$.

The **(pseudo-)lcm** of x^α and x^β is defined to be $\mathrm{lcm}(x^\alpha, x^\beta) := x^{\mu(\alpha,\beta)}$.

It enjoys a nice property: $x^\alpha \mid x^{\mu(\alpha,\beta)}$ and $x^\beta \mid x^{\mu(\alpha,\beta)}$.

Why we use the name pseudo–lcm? Using the latter property, define an element $f(c) = x^{\mu(\alpha,\beta)-\alpha} \cdot x^\alpha - c \cdot x^{\mu(\alpha,\beta)-\beta} \cdot x^\beta$ for some $c \in \mathbb{K}$.

Let $c_0 := \frac{\mathrm{lc}(x^{\mu(\alpha,\beta)-\alpha} x^\beta)}{\mathrm{lc}(x^{\mu(\alpha,\beta)-\beta} x^\alpha)}$. Then, we see that c_0 is the unique number, such that $\mathrm{lm}(f(c_0)) < x^\mu$ (otherwise, for $c \neq c_0$, $\mathrm{lm}(f(c_0)) = x^\mu$).

In the commutative case, $c_0 = 1$, $f(c_0) = 0$ and hence $x^{\mu(\alpha,\beta)}$ is regarded as the generalization of the classical lcm function.

However, in the non–commutative case $f(c_0) \neq 0$ in general, but we will make a big use of the property $\mathrm{lm}(f(c_0)) < x^\mu$.

If A is a G–algebra of Lie type, $c_0 = 1$ and, in general, $f(c_0) \neq 0$.

If A is quasi–commutative, $f(c_0) = 0$ but, in general, $c_0 \neq 1$.

Definition 3.4. Our main objects are ideals in A and monoideals in $\mathbb{N}^n$.

- A subset $S \subseteq \mathbf{N} = (\mathbb{N}^n, +)$ is called a (additive) **monoideal**, if $\forall\, \alpha \in S,\ \forall\, \beta \in \mathbb{N}^n$ we have $\alpha + \beta \in S$.
- A subset $I \subseteq A = (A, +, \cdot)$ is called **a left ideal**, if $\forall f, g \in I$ we have $f + g \in I$ and $\forall f \in I,\ \forall a \in A$ we have $a \cdot f \in I$.

Noetherian property of A ensures that every ideal of A is finitely generated. Indeed, any monoideal of $\mathbb{N}^n$ is finitely generated, too, as famous Dixon's Lemma says.

Definition 3.5. Let S be any subset of A.

- We define $\mathcal{L}(S) \subseteq \mathbb{N}^n$ to be a monoideal, generated by the leading exponents of elements of S, that is $\mathcal{L}(S) = {}_{\mathbb{N}^n}\langle \alpha \mid \exists s \in S,\ \mathrm{le}(s) = \alpha \rangle$. We call $\mathcal{L}(S)$ a **monoideal of leading exponents**.

  By Dixon's Lemma, $\mathcal{L}(S)$ is finitely generated, that is there exist $\alpha_1, \ldots, \alpha_m \in \mathbb{N}^n$, such that $\mathcal{L}(S) = {}_{\mathbb{N}^n}\langle \alpha_1, \ldots, \alpha_m \rangle$.
- A **set of leading monomials of** S is defined to be $L(S) := \{x^\alpha \mid \alpha \in \mathcal{L}(S)\} \subseteq \mathrm{Mon}(A)$.

Definition 3.6. Let $<$ be a monomial ordering on A, $I \subset A$ be a left ideal and $G \subset I$ be a finite subset.

G is called a **Gröbner basis** of I if and only if $L(G) = L(I)$,
that is, for any $f \in I \setminus \{0\}$ there exists a $g \in G$ satisfying $\mathrm{lm}(g) \mid \mathrm{lm}(f)$.

In terms of exponents we can write it like this:

$$_{\mathbb{N}^n}\langle \mathcal{L}(G) \rangle = \mathcal{L}\big({}_A\langle G \rangle \big).$$

Remark 3.7. When $A = R$ is commutative, $L(I) = \{x^\alpha \mid \alpha \in \mathcal{L}(I)\} = \{\mathrm{lm}(f) \mid f \in I\}$ becomes a leading ideal of I. And the **Gröbner basis** property could be rewritten in a form $L({}_R\langle G \rangle) ={}_R \langle L(G) \rangle$, or just $L({}_R\langle g_1, \ldots, g_m \rangle) ={}_R \langle \mathrm{lm}(g_1), \ldots, \mathrm{lm}(g_m) \rangle$.

Note, that this direct approach does not work within the non–commutative case. Take the Weyl algebra $A = \mathbb{K}\langle x, \partial \mid \partial x = x\partial + 1 \rangle$ and the ideal $I ={}_A \langle x\partial + 1, x \rangle$. I is a proper ideal, equal to ${}_A\langle x \rangle$, hence $L(I) ={}_A \langle x \rangle$, but ${}_A\langle L(G) \rangle ={}_A \langle \{x\partial, x\} \rangle = A \cdot 1$.

A subset $S \subset A$ is called **minimal**, if $0 \notin S$ and $\mathrm{lm}(s) \notin L(S \smallsetminus \{s\})$ for all $s \in S$.

We say that $f \in A$ **reduced with respect to** $S \subset A$, if no monomial of f is contained in $L(S)$.

A subset $S \subset A$ is called **reduced**, if $0 \notin S$, and if for each $s \in S$, s is reduced with respect to $S \smallsetminus \{s\}$, and, moreover, $s - \mathrm{lc}(s)\,\mathrm{lm}(s)$ is reduced with respect to S. It means that for each $s \in S \subset A$, $\mathrm{lm}(s)$ does not divide any monomial of every element of S except itself.

Definition 3.8. Let $\mathcal{G}$ denote the set of all finite ordered subsets $G \subset A$.

1. A map $\mathrm{NF} : A \times \mathcal{G} \to A,\ (f, G) \mapsto \mathrm{NF}(f \mid G)$,
   is called a **(left) normal form** on A if, for all $f \in A$ and any $G \in \mathcal{G}$,

   (i) $\mathrm{NF}(0 \mid G) = 0$,
   (ii) $\mathrm{NF}(f \mid G) \neq 0 \ \Rightarrow\ \mathrm{lm}\big(\mathrm{NF}(f|G)\big) \notin L(G)$,
   (iii) $f - \mathrm{NF}(f \mid G) \in_A \langle G \rangle$.

   NF is called a **reduced normal form** if $\mathrm{NF}(f|G)$ is reduced with respect to G.

2. Let $G = \{g_1, \ldots, g_s\} \in \mathcal{G}$. A representation of $f \in_A \langle G \rangle$
   $$f = \sum_{i=1}^{s} a_i g_i, \quad a_i \in A,$$
   satisfying $\mathrm{lm}(f) \geq \mathrm{lm}(a_i g_i)$ for all $i = 1 \ldots s$ such that $a_i g_i \neq 0$ is called a **standard (left) representation** of f (with respect to G).

Lemma 3.9. Let $I \subset A$ be a left ideal, $G \subset I$ be a Gröbner basis of I and $\mathrm{NF}(\cdot \mid G)$ be a normal form on A with respect to G.

1. For any $f \in A$ we have $f \in I \Leftrightarrow \mathrm{NF}(f \mid G) = 0$.

2. If $J \subset A$ is a left ideal with $I \subset J$, then $L(I) = L(J)$ implies $I = J$. In particular, G generates I as a left ideal.

3. If $\mathrm{NF}(\cdot \mid G)$ is a reduced normal form, then it is unique.

Proof. 1. If $\mathrm{NF}(f|G) = 0$ then $f \in I$. If $\mathrm{NF}(f|G) \neq 0$, then $\mathrm{lm}\big(\mathrm{NF}(f|G)\big) \notin L(G) = L(I)$, hence $\mathrm{NF}(f|G) \notin I$, which implies $f \notin I$.

2. Let $f \in J$ and assume $\mathrm{NF}(f|G) \neq 0$. Then $\mathrm{lm}\big(\mathrm{NF}(f|G)\big) \notin L(G) = L(I) = L(J)$, which is a contradiction since $\mathrm{NF}(f|G) \in J$. Hence, $f \in I$ by 1).

3. Let $f \in A$ and assume that h, h' are two reduced normal forms of f with respect to G. Then $h - h' \in {}_A\langle G\rangle = I$. If $h - h' \neq 0$, then $\mathrm{lm}(h - h') \in L(I) = L(G)$, which contradicts the fact that $\mathrm{lm}(h - h')$ is a monomial of either h or h'.

□

3.2 Main Algorithms

Definition 3.10. Let $f, g \in A \smallsetminus \{0\}$ with $\mathrm{lm}(f) = x^\alpha$ and $\mathrm{lm}(g) = x^\beta$ respectively. Set $\gamma := \mu(\alpha, \beta)$ and define the **(left) s–polynomial** of f and g to be

$$\mathrm{LeftSpoly}(f, g) := x^{\gamma-\alpha} f - \frac{\mathrm{lc}(x^{\gamma-\alpha} f)}{\mathrm{lc}(x^{\gamma-\beta} g)} x^{\gamma-\beta} g.$$

Remark 3.11. It is easy to see that $\mathrm{lm}(\mathrm{LeftSpoly}(f, g)) < \mathrm{lm}(f \cdot g)$ holds. If $\mathrm{lm}(g) | \mathrm{lm}(f)$, say $\mathrm{lm}(g) = x^\beta$, $\mathrm{lm}(f) = x^\alpha$, then the s–polynomial is especially simple,

$$\mathrm{LeftSpoly}(f, g) = f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(x^{\alpha-\beta} g)} x^{\alpha-\beta} g,$$

and $\mathrm{lm}\big(\mathrm{LeftSpoly}(f, g)\big) < \mathrm{lm}(f)$.

If A is a G–algebra of Lie type, then

$$\mathrm{LeftSpoly}_{Lie}(f, g) := x^{\gamma-\alpha} f - \frac{\mathrm{lc}(f)}{\mathrm{lc}(g)} x^{\gamma-\beta} g,$$

and the formula coincides with the commutative one.

Now we write down both normal form algorithms. For any algorithm we will prove that its termination and correctness. For all algorithms below we assume that $<$ is a fixed monomial well–ordering on a G–algebra A.

Proof. (of 3.1) First of all, note that every specific choice of "any" in the algorithm may give us a different normal form function.

Let $h_0 := f$, and in the i–th step of the **while** loop we compute $h_i = \mathrm{spoly}(h_{i-1}, g)$. Since $\mathrm{lm}(h_i) = \mathrm{lm}(\mathrm{spoly}(h_{i-1}, g)) < \mathrm{lm}(h_{i-1})$ (by the property

Algorithm 3.1 LeftNF

Input : $f \in A,\ G \in \mathcal{G}$;
Output: $h \in A$, a left normal form of f with respect to G.

$h := f$;
while ($(h \neq 0)$ **and** $(G_h = \{g \in G : \ \mathrm{lm}(g) \mid \mathrm{lm}(h)\} \neq \emptyset)$) **do**
  choose any $g \in G_h$;
  $h := \mathrm{LeftSpoly}(h, g)$;
end while
return h;

of spoly), we obtain a set $\{\mathrm{lm}(h_i)\}$ of leading monomials of h_i, where $\forall i\ h_{i+1}$ has strictly smaller leading monomial than h_i. Since $<$ is a well–ordering, this set has a minimum, hence the algorithm terminates.

Suppose this minimum is reached at the step m. Let $h = h_m$, a_i are *terms* (monomials times coefficients) and $g_i \in G$. Making substitutions backwards, we obtain the following presentation

$$h = f - \sum_{i=1}^{m-1} a_i g_i,$$

satisfying $\mathrm{lm}(f) = \mathrm{lm}(a_1 g_1) > \mathrm{lm}(a_i g_i) > \mathrm{lm}(h_m), \quad \forall\ 1 \leq i \leq m$. By the construction, h is either zero or, if $h \neq 0$, then $\mathrm{lm}(h) \notin L(G)$. Hence the correctness follows. $\square$

Algorithm 3.2 redLeftNF

Input : $f \in A,\ G \in \mathcal{G}$;
Output: $h \in A$, a reduced left normal form of f with respect to G.

$h := 0,\ \ g := f$;
while $(g \neq 0)$ **do**
  $g := \mathrm{LeftNF}(g \mid G)$;
  $h := h + \mathrm{lc}(g)\,\mathrm{lm}(g)$;
  $g := g - \mathrm{lc}(g)\,\mathrm{lm}(g)$;
end while
return h;

Proof. (of 3.2) Since the *tail* of g, $g - \mathrm{lc}(g)\,\mathrm{lm}(g)$, has strictly smaller leading monomial than g and $<$ is a well–ordering, the algorithm terminates. The correctness of the algorithm follows from the correctness of LeftNF. $\square$

Algorithm 3.3 LeftGröbnerBasis

Input : $G \in \mathcal{G}$;
Output : $S \in \mathcal{G}$, a left Gröbner basis of the left ideal $I = {}_A\langle G\rangle \subset A$.

$S := G$;
$P := \{(f, g) \mid f, g \in S\} \subset S \times S$;
while ($P \neq \emptyset$) **do**
  choose $(f, g) \in P$;
  $P := P \setminus \{(f, g)\}$;
  $h :=$ LeftNF$\big($ LeftSpoly$(f, g) \mid S\big)$;
  if ($h \neq 0$) **then**
    $P := P \cup \{(h, f) \mid f \in S\}$;
    $S := S \cup h$;
  end if
end while
return S;

Proof. (of 3.3) **Termination:** By the property 3.9,1) we know that if $h \neq 0$ then $\mathrm{lm}(h) \notin L(S)$. Then, ${}_A\langle S\rangle \subset {}_A\langle\{S, h\}\rangle$ and we obtain a strictly increasing sequence of ideals of A. Since A is Noetherian, this sequence stabilizes. It means that, after finitely many steps, we always have LeftNF$\big($LeftSpoly$(f, g) \mid S)\big) = 0$ for all $(f, g) \in P$ and, after several more steps, the set P of pairs will become empty. Thus LeftGröbnerBasis terminates.

If LeftNF is a reduced normal form and if G is a reduced set, then S will be a reduced Gröbner basis. If G is not reduced, we may apply LeftNF afterwards to $(f, S \setminus \{f\})$ for all $f \in S$ in order to obtain a reduced Gröbner basis. □

The correctness is proved with the Left Buchberger's Criterion below.

Theorem 3.12. Let $I \subset A$ be a left ideal and $G = \{g_1, \ldots, g_s\} \subset I$. Let LeftNF$(\cdot \mid G)$ be a left normal form on A with respect to G. Then the following are equivalent:

1. G is a left Gröbner basis of I,
2. LeftNF$(f \mid G) = 0$ for all $f \in I$,
3. each $f \in I$ has a left standard representation with respect to G,
4. LeftNF$\big($LeftSpoly$(g_i, g_j) \mid G\big) = 0$ for $1 \leq i, j \leq s$.

Proof. The implication ($1 \Rightarrow 2$) follows from Lemma 3.9, ($2 \Rightarrow 3$) follows from the corresponding definitions. As for implication ($3 \Rightarrow 1$), we see that if f has a left standard representation with respect to G, then $\mathrm{lm}(f)$ must occur as the leading monomial of $a_i g_i$ for some i. It means that $\mathrm{lm}(g_i) \mid \mathrm{lm}(f)$, hence G is a left Gröbner basis of I.

To prove ($3 \Rightarrow 4$), we note first that $h = \mathrm{LeftNF}\big(\mathrm{LeftSpoly}(f_i, f_j) \mid G\big) \in I$ and hence, by 3, if $h \neq 0$, we have $\mathrm{lm}(h) \in L(G)$, what contradicts the property (iii) of NF. In the Lemma 3.9 we have already shown, that G generates I.

The implication ($4 \Rightarrow 1$) is an important criterion which allows checking and construction of Gröbner bases in a finite number of steps. This implication follows from the more general Theorem, which requires more technical details and therefore is omitted here. □

Definition 3.13. (Elimination ordering) Let A be a G–algebra in n variables, generated by $\{x_1, \dots, x_n\}$ such that $\{x_{r+1}, \dots, x_n\}$ generate an admissible sub–G–algebra $B \subset A$. A monomial ordering $<$ on A is **an elimination ordering for** $x_1, \dots, x_r$, if for $f \in A, \mathrm{lm}(f) \in B$ implies $f \in B$.

Note, that only with respect to the elimination ordering like in the definition we have $\mathrm{lm}(f) \in B \Leftrightarrow f \in B$.

Example 3.14. The classical elimination ordering in the commutative case is `lp` (lexicographical ordering). Since for many non–commutative G–algebras it is not an admissible ordering, an usual elimination ordering in the non–commutative setting is the block ordering of the form $(\mathtt{dp}(1..r),\mathtt{dp}(r+1..n))$, or the ordering with extra weights $(\mathtt{a}(w_1, \dots, w_r),<)$.

Let A, B be two ordering matrices. Then the block ordering $(<_A, <_B)$ is given by the matrix $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$.

A matrix for an ordering with extra weights look like follows:

$$(\mathtt{a}(\bar{\omega}),\mathtt{Dp}) \sim \begin{pmatrix} \omega_1 & \dots & \omega_r & 0 & \dots & 0 & 0 & 0 \\ 1 & \dots & 1 & 1 & \dots & 1 & 1 & 1 \\ 1 & \dots & 0 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 & 0 \end{pmatrix}.$$

However, for some algebras, like Weyl algebras, lexicographical ordering is admissible.

Lemma 3.15. Let $I \subseteq A$ be an ideal, $B = \langle x_{r+1}, \ldots, x_n \mid x_j x_i = c_{ij} x_i x_j + d_{ij} \rangle$ be an admissible subalgebra of A, and $<$ an elimination ordering for $x_1, \ldots, x_r$ on A . If $S = \{f_1, \ldots, f_m\}$ is a Gröbner basis of I, then $S \cap B$ is a Gröbner basis of $I \cap B$.

Proof. Take any $x^\alpha \in L(I)$, then there exists such $f \in I$, that $\mathrm{lm}(f) = x^\alpha$. Since $<$ is an elimination ordering for $x_1, \ldots, x_r$, from $\mathrm{lm}(f) \in B$ follows that $f \in B$. Hence,

$$L(I) \cap B = \{x^\alpha \mid \exists f \in I,\ \mathrm{lm}(f) = x^\alpha\} \cap B = \{x^\alpha \mid \exists f \in I \cap B,\ \mathrm{lm}(f) = x^\alpha\},$$

and the latter is just $L(I \cap B)$. Then, $L(S) \cap B = L(I) \cap B = L(I \cap B) = L(S \cap B)$, hence $S \cap B$ is a Gröbner basis of $I \cap B$ by the definition. $\square$

4 Examples

Consider the system of differential equations in some differential operator ∂, variable x and parameters a, b, written in the operator form:

$$\begin{aligned} x^2\partial + a \cdot x &= 0, \\ x\partial^2 + b \cdot \partial &= 0. \end{aligned}$$

We are going to see which role the parameters play, elaborate different cases and solve the system. We will use Gröbner bases and elimination for finding hidden equations (so-called *integrability conditions*) in the system and for simplifying systems of equations. Note, that Gröbner bases are useful for pre-processing of such systems of equations; we nevertheless need DE solvers for post-processing and solving.

1. PDE with constant coefficients.

If we consider this equation as the one in variables x, t with $\partial = \frac{\partial}{\partial t}$, the underlying algebra is commutative and is equal to $\mathbb{K}[x, \partial]$. The system corresponds to the ideal $I = \langle x^2\partial + ax, x\partial^2 + b\partial \rangle \subset \mathbb{K}[x, \partial]$.

For this, we are computing the reduced minimal Gröbner basis of the ideal I with respect to the ordering `Dp`.

```
option(redSB);  // compute minimal basis
option(redTail); // compute reduced basis
```

```
ring A  = (0,a,b),(x,d),Dp; // a,b are parameters
ideal I = x^2*d + a*x ,x*d^2 + b*d;
I = std(I);
I;

  I[1]=d
  I[2]=x
```

So, declaring a, b as parameters, we have assumed that they are generic, that is nonzero and algebraically independent. In this situation, we see that in this situation, the answer corresponds to the system of PDE's $\frac{\partial f}{\partial t} = 0, xf = 0$, which has only zero solution.

Now we would like to investigate the solutions of the system in the case of arbitrary a, b, declaring them as commutative variables.

```
ring V  = 0,(x,d,a,b),Dp; // a,b are variables
ideal I = x^2*d + a*x ,x*d^2 + b*d;
I = std(I);
I;

  I[1]=dab-db2
  I[2]=xa2-xab
  I[3]=xda-xdb
  I[4]=xd2+db
  I[5]=x2d+xa
```

So, the condensed form of the answer is

$\{x\partial^2 + b\partial,\ x^2\partial + ax,\ \ (a-b)b\partial, a(a-b)x,\ (a-b)x\partial\}$.

As we can see, there are three possible relations between a, b:

1.1. $a = 0, b \neq 0$. Then, we get just $\langle \partial \rangle$, that is an initial system is equivalent to the only one equation $\frac{\partial f}{\partial t} = 0$. Then, of course, each $f \in \mathbb{K}[x]$ is a solution.

1.2. $a \neq 0, b = 0$. Then, we get just $\langle x \rangle$, that is $xf = 0$, what is only satisfied by $f = 0$.

1.3. $a = b$. Then, we get ideal, which describes the system

$$\begin{array}{rcl} x\frac{\partial^2 f}{\partial t^2} + a\frac{\partial f}{\partial t} & = & 0 \\ x^2\frac{\partial f}{\partial t} + axf & = & 0. \end{array}$$

From the second equation follows, that $x\frac{\partial f}{\partial t}+af=0$ and the first equation is just a differentiation of it. So, all the solutions f satisfy this single equation, hence $f=ce^{-\frac{a}{x}t}, c\in\mathbb{K}$.

2. ODE with polynomial coefficients.

Let us treat the equation as the one in variable x with $\partial=\frac{d}{dx}$. Then, the underlying algebra becomes a non–commutative algebra $A=\mathbb{K}\langle x,\partial \mid \partial x = x\partial+1\rangle$ (the first Weyl algebra). The system corresponds to the left ideal $I=\langle x^2\partial+ax, x\partial^2+b\partial\rangle\subset A$.

At first, we computing the reduced minimal Gröbner basis of the ideal I as before, treating a,b as generic parameters.

```
option(redSB);  // compute minimal basis
option(redTail); // compute reduced basis
ring Ap  = (0,a,b),(x,d),Dp; // a,b are parameters
ncalgebra(1,1); // non-comm. initialization for Weyl algebra
ideal I = x^2*d + a*x ,x*d^2 + b*d;
I = std(I);
I;

  I[1]=1
```

Since this basis is just 1 (hence, the ideal coincide with the whole algebra), we conclude that for generic a,b the system is inconsistent and has no solutions. Moreover, there should be algebraic relations between a,b.

In order to find them, we declare a,b as variables, thus moving to the algebra $A\otimes_{\mathbb{K}}\mathbb{K}[a,b]$. Then, we compute the reduced Gröbner basis with respect to the *elimination ordering* for x,∂ (see 3.13) using the command `eliminate`.

```
ring A  = 0,(x,d),Dp;
ncalgebra(1,1); // non-comm. initialization for Weyl algebra
ring X = 0,(a,b),Dp; // a,b are variables
def V = A + X;   // V = A tensor X as algebra
setring V;
ideal I   = x^2*d + a*x ,x*d^2 + b*d;
ideal Rel = eliminate(I,x*d); //
Rel;

  Rel[1]=a2b-ab2-2a2+3ab-2a
```

Hence, the desired relation is $a(b-2)(a-b+1)=0$. Now we proceed with computations for each specific case.

2.1. $b=a+1$. We get just $\langle x\partial + a\rangle$, that corresponds to the equation $x\frac{\partial f}{\partial x}+af=0$, which parametric solutions are $\{cx^{-a}, c\in\mathbb{K}\}$.

2.2. $a=0, b=2$. We get a system $x\frac{\partial^2 f}{\partial t^2}+2\frac{\partial f}{\partial t}=0, x^2\frac{\partial f}{\partial t}=0$, whose only solutions are constants $\mathbb{K}$.

2.3. $a=0, b\notin\{1,2\}$. The ideal equals $\langle\partial\rangle$, hence there are only constant solutions.

2.4. $b=2, a\notin\{0,1\}$. The ideal equals $\langle x\rangle$, the only solution is zero.

3. ODE with rational coefficients.

As in the previous case, let $\partial=\frac{d}{dx}$, but let x be a rational function rather than polynomial. Then, we are dealing with the differential field $\mathbb{K}(x)$ and a non–commutative Ore algebra $B=\mathbb{K}(x)\langle\partial \mid \partial x = x\partial + 1\rangle$. The system corresponds to the ideal $I=\langle x^2\partial+ax, x\partial^2+b\partial\rangle\subset B$.

Unfortunately, computations in such Ore algebras are not yet implemented in Singular:Plural, so we will do computations by hand. Note, that the whole Gröbner bases theory could be generalized for such a case.

$f_1=x^2\partial+ax$, $f_2=x\partial^2+b\partial$. Since x is constant, we replace f_1 with $f_1'=x\partial+a$. Then, f_2 could be reduced with f_1' to $f_3=a(b-a+1)x$. In order for system to be consistent, f_3 should be zero, what provides a condition on parameters: $a(b-a+1)=0$.

3.1. $a=0$. Then $x\frac{\partial f}{\partial x}=0$ have only scalar solutions from $\mathbb{K}$.

3.2. $b=a-1, a\neq 0$. We have one equation, $x\frac{\partial f}{\partial x}+af=0$, whose solutions are $f\in\{cx^{-a}, c\in\mathbb{K}\}$.

5 Applications to Homological Algebra

5.1 Gröbner Bases for Modules

We are going to show, that all the results and algorithms could be easily transferred from the case of ideals to the submodules of free A–modules of finite rank (which appear either as themselves or as presentation matrices for finitely presented modules).

Let

$$e_i = (0, \ldots, 1_i, \ldots, 0) \text{ and } A^r = Ae_1 \oplus \ldots \oplus Ae_r$$

be a free A–module of rank r. We extend the notion of a monomial ordering from A to A^r. First of all, $\operatorname{Mon}(A^r) := \{x^\alpha e_i \mid \alpha \in \mathbb{N}^n, 1 \leq i \leq r\}$ and $x^\alpha e_i \in A^r$ is called a **monomial (involving component i)**.

Definition 5.1. Let $<$ be a monomial ordering on A. A **monomial** (**module**) **ordering** on A^r is a total ordering $<_m$ on the set of monomials $\operatorname{Mon}(A^r)$, satisfying for all $\alpha, \beta, \gamma \in \mathbb{N}^n$, $1 \leq i, j \leq r$

1. $x^\alpha e_i <_m x^\beta e_j \;\Rightarrow\; x^{\alpha+\gamma} e_i <_m x^{\beta+\gamma} e_j$,
2. $x^\alpha < x^\beta \;\Rightarrow\; x^\alpha e_i <_m x^\beta e_i$.

In addition to obvious generalizations of leading monomial/coefficient/exponent functions, for f, such that $\operatorname{lm}(f) = x^\alpha e_i$, we define i to be the **leading component** of f.

Every monomial ordering could be extended to the monomial module ordering in at least two following ways. We can order components either in ascending or in descending way (which we are going use below). Then,

$<_m$ is a position over term (**POT**) ordering, if

$$x^\alpha e_i <_{\mathrm{POT}} x^\beta e_j \;\stackrel{def}{\Leftrightarrow}\; i < j \text{ or, if } i = j,\;\; x^\alpha < x^\beta.$$

$<_m$ is a term over position (**TOP**) ordering, if

$$x^\alpha e_i <_{\mathrm{TOP}} x^\beta e_j \;\stackrel{def}{\Leftrightarrow}\; x^\alpha < x^\beta \text{ or, if } \alpha = \beta,\;\; i < j.$$

Let $f, g \in A^r \smallsetminus \{0\}$ with $\operatorname{lm}(f) = x^\alpha e_i$ and $\operatorname{lm}(g) = x^\beta e_j$. Setting $\gamma := \mu(\alpha, \beta)$, we define the **left s–polynomial** of f and g to be 0, if $i \neq j$ and

$$x^{\gamma-\alpha} f - \frac{\operatorname{lc}(x^{\gamma-\alpha} f)}{\operatorname{lc}(x^{\gamma-\beta} g)} x^{\gamma-\beta} g, \;\; \text{if } i = j.$$

Now the notions of normal form (3.8), Gröbner basis (3.6) and corresponding algorithms 3.1, 3.3 follow almost immediately together with lemma 3.9 and theorem 3.12.

In order to illustrate the principles of computing Gröbner bases and syzygies for submodules, we draw two matrices.

Suppose we are given $I = \{\bar{f}_1, \ldots, \bar{f}_k\} \subset A^r$ and let F be a matrix with $\bar{f}_i$ as columns. We append a $k \times k$ unit matrix to F, obtaining a matrix F'.

We put the result of the Gröbner basis computation of F' as of left module in the second matrix, sorting the columns in such a way, that the elements, having first r components zero, are moved to the left. (We denote $\bar{0} = (0, \ldots, 0)^T \in A^r$).

$$\begin{pmatrix} \bar{f}_1 & \ldots & \bar{f}_k \\ 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \xrightarrow{GB} \left(\begin{array}{ccc|ccc} \bar{0} & \ldots & \bar{0} & \bar{h}_1 & \ldots & \bar{h}_t \\ \hline & & & & & \\ & \mathbf{S} & & & \mathbf{T} & \\ & & & & & \end{array}\right)$$

Then,

$\{\bar{h}_1, \ldots, \bar{h}_t\}$ is a Gröbner basis of I (let H be a matrix with columns $\bar{h}_i$),

columns of $\mathbf{S}$ form a Gröbner basis of $\mathrm{Syz}(f_1, \ldots, f_k)$,

$\mathbf{T}$ is a left transition matrix between two bases of F, i.e. $H^t = \mathbf{T}^t F^t$.

Note, that the last equality is equivalent to $H = F\mathbf{T}$ only in the commutative case.

5.2 Maps induced by Hom

In the following three chapters we will describe how to compute Hom and Ext. For more details see [GP, BTV]. Let A be a $\mathbb{K}$–algebra and M, N be left A–modules. The $\mathrm{Hom}_A(M, N)$ has a canonical structure of right (resp. left) A–module if N (resp. M) is an A–bimodule. An A-bimodule M is said to be **centralizing**, if M is generated as a left A–module by its centralizer $\mathrm{Cen}_A(M) = \{m \in M \mid am = ma, a \in A\}$.
Next we want to compute $\mathrm{Hom}_A(\varphi, 1_{A^s})$ for a map $\varphi : A^n \to A^m$. We consider A^n and A^m as left modules and identify them with the corresponding row-spaces. Let $\varphi : A^n \to A^m$ be the left A–linear map defined by the $m \times n$–matrix $M = (M_{ij})$ with entries in A, $\varphi(x) = x \cdot M^t$. We want to compute the induced map

$$\varphi^* : \mathrm{Hom}_A(A^m, A^s) \to \mathrm{Hom}_A(A^n, A^s)$$

of right A–modules. To do so, we identify right modules $\mathrm{Hom}_A(A^n, A^s) = A^{sn}$ and $\mathrm{Hom}_A(A^m, A^s) = A^{ms}$, considered as column-spaces now. Let $\{e_1, \ldots, e_n\}$, $\{f_1, \ldots, f_m\}$, $\{h_1, \ldots, h_s\}$ denote the canonical bases of left A–modules A^n, A^m, and bimodule A^s, respectively. Then $\varphi(e_i) = \sum_{j=1}^m M_{ji} f_j$. Moreover, if $\{\sigma_{ij}\}$, $\{\kappa_{ij}\}$ are the bases of left modules $\mathrm{Hom}_A(A^m, A^s)$, respectively $\mathrm{Hom}_A(A^n, A^s)$, defined by $\sigma_{ij}(f_\ell) = \delta_{j\ell}h_i$,[1] respectively $\kappa_{ij}(e_\ell) = \delta_{j\ell}h_i$, then, since A^s is a centralizing bimodule,

$$\begin{aligned}\varphi^*(\sigma_{ij})(e_k) &= \sigma_{ij} \circ \varphi(e_k) = \sigma_{ij}\left(\sum_{\ell=1}^{m} M_{\ell k} f_\ell\right) = \sum_{\ell=1}^{m} M_{\ell k}\delta_{j\ell}h_i \\ &= M_{jk}h_i = \sum_{\ell=1}^{n} \delta_{\ell k}h_i M_{j\ell} = \sum_{\ell=1}^{n} \kappa_{i\ell}(e_k)M_{j\ell}\,.\end{aligned}$$

This implies $\varphi^*(\sigma_{ab}) = \sum_{c=1}^{n} \kappa_{ac}M_{bc}$. To obtain the $sn \times sm$–matrix R defining φ^*, we order the basis elements σ_{ij} and κ_{ij} as follows

$$\begin{gathered}\{\sigma_{11}, \sigma_{12}, \dots, \sigma_{1m}, \sigma_{21}\,, \sigma_{22}, \dots\dots, \sigma_{s1}, \sigma_{s2}, \dots, \sigma_{sm}\}\,, \\ \{\kappa_{11}, \kappa_{12}, \dots, \kappa_{1n}, \kappa_{21}, \kappa_{22}, \dots\dots, \kappa_{s1}, \kappa_{s2}, \dots, \kappa_{sn}\}\,,\end{gathered}$$

and set, for $a, d = 1, \dots, s$, $b = 1, \dots, m$, $c = 1, \dots, n$,

$$i := (d-1)n + c, \quad j := (a-1)m + b\,.$$

Then

$$R_{ij} = \begin{cases} 0, & d \neq a, \\ M_{bc} & d = a\,. \end{cases}$$

We program this in a short procedure: given a matrix M, defining a left homomorphism $A^n \to A^m$, and an integer s, the procedure `contraHom` returns a matrix defining a right homomorphism $R : \mathrm{Hom}_A(A^m, A^s) \to \mathrm{Hom}_A(A^n, A^s)$.

```
proc contraHom(matrix M,int s)
{
   int n,m=ncols(M),nrows(M);
   int a,b,c;
   matrix R[s*n][s*m];
   for(b=1;b<=m;b++)
   {
      for(a=1;a<=s;a++)
      {
         for(c=1;c<=n;c++)
         {
            R[(a-1)*n+c,(a-1)*m+b]=M[b,c];
```

[1]Here $\delta_{j\ell}$ is the *Kronecker symbol* ($\delta_{j\ell} = 0$ if $j \neq \ell$ and $\delta_{jj} = 1$).

```
            }
        }
    }
    return(R);
}
```

Let us try an example.

```
ring A=0,(x,y,z),dp;
matrix M[3][3]=1,2,3,
               4,5,6,
               7,8,9;

print(contraHom(M,2));
//-> 1,4,7,0,0,0,
//-> 2,5,8,0,0,0,
//-> 3,6,9,0,0,0,
//-> 0,0,0,1,4,7,
//-> 0,0,0,2,5,8,
//-> 0,0,0,3,6,9
```

Note that for $s = 1$, the dual map, that is, the transposed matrix, is computed.

Similarly, we can compute the map of right A–modules

$$\varphi_* : \mathrm{Hom}_A(A^s, A^n) \to \mathrm{Hom}_A(A^s, A^m).$$

If $\{\sigma_{ij}\}$ and $\{\kappa_{ij}\}$ are defined as before as bases of $\mathrm{Hom}_A(A^s, A^n)$, respectively $\mathrm{Hom}_A(A^s, A^m)$, then one checks that $\varphi_*(\sigma_{ab}) = \sum_{c=1}^{m} M_{ca}\kappa_{cb}$.

We obtain the following procedure: given a right homomorphism $M : A^n \to A^m$ and s, `coHom` returns a right homomorphism $R : \mathrm{Hom}_A(A^s, A^n) \to \mathrm{Hom}_A(A^s, A^m)$.

```
proc coHom(matrix M,int s)
{
   int n,m=ncols(M),nrows(M);
   int a,b,c;
   matrix R[s*m][s*n];
   for(b=1;b<=s;b++)
   {
      for(a=1;a<=m;a++)
```

```
      {
         for(c=1;c<=n;c++)
         {
            R[(a-1)*s+b,(c-1)*s+b]=M[a,c];
         }
      }
   }
   return(R);
}
```

As an example, we use the matrix defined above.

```
print(coHom(M,2));
//-> 1,0,2,0,3,0,
//-> 0,1,0,2,0,3,
//-> 4,0,5,0,6,0,
//-> 0,4,0,5,0,6,
//-> 7,0,8,0,9,0,
//-> 0,7,0,8,0,9
```

5.3 Computation of Hom

Let M be a finitely generated left A–module with the presentation $A^m \xrightarrow{\varphi} A^n \to M \to 0$.

Let N be a finitely generated centralizing A–module $N = A^s/L$ for a suitable subbimodule $L \subset A^s$. Let $A^r \xrightarrow{\psi} A^s \to N \to 0$ be a presentation of N.

We obtain the following commutative diagram of right modules with exact rows and columns:

$$\begin{tikzcd}
\mathrm{Hom}_A(M,N) \arrow[r] & \mathrm{Hom}_A(A^n,N) \arrow[r, "\varphi_N^*"] & \mathrm{Hom}_A(A^m,N) \\
 & \mathrm{Hom}_A(A^n,A^s) \arrow[u] \arrow[r, "\varphi^*"] & \mathrm{Hom}_A(A^m,A^s) \arrow[u] \\
 & \mathrm{Hom}_A(A^n,A^r) \arrow[u, "j"'] \arrow[r] & \mathrm{Hom}_A(A^m,A^r)\,, \arrow[u, "i"']
\end{tikzcd}$$

In particular, $\varphi_N^*(\sigma) = \sigma \circ \varphi$, $\varphi^*(\sigma) = \sigma \circ \varphi$, $i(\sigma) = \psi \circ \sigma$, and $j(\sigma) = \psi \circ \sigma$. It is easy to see that

$$\mathrm{Hom}_A(M,N) = \mathrm{Ker}(\varphi_N^*) \cong \varphi^{*-1}\big(\mathrm{Im}(i)\big)\big/\,\mathrm{Im}(j)\,.$$

Using the SINGULAR built–in command `modulo`, which is explained below, we have (identifying, as before, $\mathrm{Hom}_A(A^n, A^s) = A^{sn}$ and $\mathrm{Hom}_A(A^m, A^s) = A^{ms}$)

$$D := \varphi^{*-1}\big(\mathrm{Im}(i)\big) = \mathrm{Ker}\big(A^{ns} \xrightarrow{\overline{\varphi^*}} A^{ms}/\,\mathrm{Im}(i)\big) = \ \mathtt{modulo}\,(\varphi^*, i)\,,$$

which is given by a $ns \times k$–matrix with entries in A, and we can compute $\mathrm{Hom}_A(M, N)$ as

$$\varphi^{*-1}\big(\mathrm{Im}(i)\big)/\,\mathrm{Im}(j) = A^k/\,\mathrm{Ker}\big(A^k \xrightarrow{\overline{D}} A^{ns}/\,\mathrm{Im}(j)\big) = A^k/\,\mathtt{modulo}\,(D, j)\,.$$

Finally, we obtain the following procedure with $F = \varphi^*$, $B = i$, $C = j$.

```
proc Hom(matrix M, matrix N)
{
  matrix F = contraHom(M,nrows(N));
  matrix B = coHom(N,ncols(M));
  matrix C = coHom(N,nrows(M));
  matrix D = modulo(F,B);
  matrix E = modulo(D,C);
  return(E);
}
```

Here is an example.

```
ring A=0,(x,y,z),dp;
matrix M[3][3]=1,2,3,
               4,5,6,
               7,8,9;
matrix N[2][2]=x,y,
               z,0;

print(Hom(M,N));      //a 6x6 matrix
//-> 0,0,0,0,y,x,
//-> 0,0,0,0,0,z,
//-> 1,0,0,0,0,0,
//-> 0,1,0,0,0,0,
//-> 0,0,1,0,0,0,
//-> 0,0,0,1,0,0
```

We explain the `modulo` command: let the matrices $M \in Mat(m \times n, A)$, respectively $N \in Mat(m \times s, A)$, represent linear maps

$$\begin{array}{ccc} A^n & \xrightarrow{M} & A^m \\ & & \uparrow{\scriptstyle N} \\ & & A^s \, . \end{array}$$

Then $\texttt{modulo}(M,N) = \operatorname{Ker}\big(A^n \xrightarrow{\overline{M}} A^m/\operatorname{Im}(N)\big)$, where $\overline{M}$ is the map induced by M; more precisely, $\texttt{modulo}(M,N)$ returns a set of vectors in A^n which generate $\operatorname{Ker}(\overline{M})$ [2]. Hence, `matrix(modulo(M,N))` is a presentation matrix for the quotient $(\operatorname{Im}(M) + \operatorname{Im}(N))/\operatorname{Im}(N)$.

5.4 Computation of Ext

The following lemma is the basis for computing $\operatorname{Ext}^i_A(M,N)$. Let M be a finitely generated left A–module and N a finitely generated centralizing A–module. Let
$\ldots \longrightarrow F_{i+1} \xrightarrow{\varphi_{i+1}} F_i \xrightarrow{\varphi_i} \ldots \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} M \longrightarrow 0$ be a free resolution of M and

$$G_1 \xrightarrow{\psi} G_0 \xrightarrow{\pi} N \longrightarrow 0$$

a presentation of N such that $\psi(G_1)$ is a bimodule. Then we obtain the following commutative diagram with exact columns and second and third row:

$$\begin{tikzcd}
 & 0 & 0 & 0 & \\
\cdots \arrow[r] & \operatorname{Hom}_A(F_{i-1},N) \arrow[r] \arrow[u] & \operatorname{Hom}_A(F_i,N) \arrow[r] \arrow[u] & \operatorname{Hom}_A(F_{i+1},N) \arrow[r] \arrow[u] & \cdots \\
\cdots \arrow[r] & \operatorname{Hom}_A(F_{i-1},G_0) \arrow[r, "\varphi_i^*"] \arrow[u] & \operatorname{Hom}_A(F_i,G_0) \arrow[r, "\varphi_{i+1}^*"] \arrow[u] & \operatorname{Hom}_A(F_{i+1},G_0) \arrow[r] \arrow[u] & \cdots \\
\cdots \arrow[r] & \operatorname{Hom}_A(F_{i-1},G_1) \arrow[r] \arrow[u] & \operatorname{Hom}_A(F_i,G_1) \arrow[r] \arrow[u, "\operatorname{Hom}_A(1_{F_i},\psi)"'] & \operatorname{Hom}_A(F_{i+1},G_1) \arrow[r] \arrow[u, "\operatorname{Hom}_A(1_{F_{i+1}},\psi)"'] & \cdots
\end{tikzcd}$$

Here we denote $\varphi_i^* = \operatorname{Hom}_A(\varphi_i, 1_{G_0})$.

[2] Using automatic type conversion, we can apply the `modulo`–command to modules as well as to matrices.

Lemma 5.2. With the above notations

$\mathrm{Ext}^i_A(M,N) = (\varphi^*_{i+1})^{-1}\,\mathrm{Im}(\mathrm{Hom}_A(1_{F_{i+1}},\psi))/\big(\mathrm{Im}(\mathrm{Hom}_A(1_{F_i},\psi)) + \mathrm{Im}(\varphi^*_i)\big)\,.$

Proof. The columns, the second and third row of the above diagram are exact. By definition,

$$\mathrm{Ext}^i_A(M,N) = \mathrm{Ker}(\mathrm{Hom}_A(\varphi_{i+1},1_N)/\,\mathrm{Im}(\mathrm{Hom}_A(\varphi_i,1_N)\,.$$

Now $\mathrm{Hom}_A(1_{F_i},\pi)$ maps $(\varphi^*_{i+1})^{-1}\big(\mathrm{Im}(\mathrm{Hom}_A(1_{F_{i+1}},\psi))\big)$ surjectively to $\mathrm{Ker}(\mathrm{Hom}_A(\varphi_{i+1},1_M))$. Therefore, we have a surjection

$$(\varphi^*_{i+1})^{-1}\big(\mathrm{Im}(\mathrm{Hom}_A(1_{F_{i+1}},\psi))\big) \longrightarrow \mathrm{Ext}^i_A(M,N)\,.$$

Obviously, $\mathrm{Im}(\mathrm{Hom}_A(1_{F_i},\psi)) + \mathrm{Im}(\varphi^*_i)$ is contained in the kernel of this surjection. An easy diagram chase shows that this is already the kernel. □

Using the lemma we write a procedure `Ext` to compute $\mathrm{Ext}^i_A(M,N)$ for finitely generated A–modules M and N, presented by the matrices `Ps` and `Ph`. We compute $\texttt{Im} := \mathrm{Im}(\mathrm{Hom}_A(1_{F_{i+1}},\psi))$, $\texttt{f} := \mathrm{Im}(\varphi^*_{i+1})$, $\texttt{Im2} := \mathrm{Im}(\varphi^*_i)$, $\texttt{Im1} := \mathrm{Im}(\mathrm{Hom}_A(1_{F_i},\psi))$, and obtain

$$\begin{aligned}\mathrm{Ext}^i_A(M,N) &= \mathrm{Ker}\left(\mathrm{Hom}_A(F_i,G_0) \xrightarrow{\overline{\varphi^*_{i+1}}} \mathrm{Hom}_A(F_{i+1},G_0)/\texttt{Im}\right)\Big/\big(\texttt{Im1}+\texttt{Im2}\big)\\ &= \texttt{modulo(f,Im)}/(\texttt{Im1}+\texttt{Im2})\,.\end{aligned}$$

```
proc Ext(int i, matrix Ps, matrix Ph)
{
  if(i==0) { return(module(Hom(Ps,Ph))); }
  list Phi   = mres(Ps,i+1);
  module Im  = coHom(Ph,ncols(Phi[i+1]));
  module f   = contraHom(matrix(Phi[i+1]),nrows(Ph));
  module Im1 = coHom(Ph,ncols(Phi[i]));
  module Im2 = contraHom(matrix(Phi[i]),nrows(Ph));
  module ker = modulo(f,Im);
  module ext = modulo(ker,Im1+Im2);
  ext        = prune(ext);
  return(ext);
}
```

Let us try an example:

```
ring R      = 0,(x,y),dp;
ideal I     = x2-y3;
qring S     = std(I);
module M    = [-x,y],[-y2,x];
module E1   = Ext(1,M,M);
print(E1);

 y,0,x,0,
 0,y,0,x
```

5.5 Computation of Tor

With the technology, elaborated in previous sections, we are able to compute also Tor.

The following proposition is the basis for computing $\mathrm{Tor}_i^A(M,N)$. Let

$$\ldots \longrightarrow F_{i+1} \xrightarrow{\varphi_{i+1}} F_i \xrightarrow{\varphi_i} \ldots \xrightarrow{\varphi_1} F_0 \xrightarrow{\varphi_0} N \longrightarrow 0$$

be a free resolution of the left A–module N and

$$G_1 \xrightarrow{\psi} G_0 \xrightarrow{\pi} M \longrightarrow 0$$

a presentation of the left A–module M. Then we obtain the following commutative diagram:

$$\begin{tikzcd}
 & 0 & 0 & 0 & \\
\cdots \arrow[r] & F_{i+1}\otimes_A M \arrow[u] \arrow[r] & F_i \otimes_A M \arrow[u] \arrow[r] & F_{i-1}\otimes_A M \arrow[u] \arrow[r] & \cdots \\
\cdots \arrow[r] & F_{i+1}\otimes_A G_0 \arrow[u] \arrow[r, "\varphi_{i+1}\otimes 1_{G_0}"] & F_i \otimes_A G_0 \arrow[u] \arrow[r, "\varphi_i\otimes 1_{G_0}"] & F_{i-1}\otimes_A G_0 \arrow[u] \arrow[r] & \cdots \\
\cdots \arrow[r] & F_{i+1}\otimes_A G_1 \arrow[u] \arrow[r] & F_i \otimes_A G_1 \arrow[u, "1_{F_i}\otimes\psi"'] \arrow[r] & F_{i-1}\otimes_A G_1 \arrow[u, "1_{F_{i-1}}\otimes\psi"'] \arrow[r] & \cdots
\end{tikzcd}$$

Proposition 5.3. With the above notations

$$\mathrm{Tor}_i^A(M,N) = (\varphi_i \otimes 1_{G_0})^{-1}\,\mathrm{Im}(1_{F_{i-1}}\otimes \psi)\big/\big(\mathrm{Im}(1_{F_i}\otimes\psi) + \mathrm{Im}(\varphi_{i+1}\otimes 1_{G_0})\big)\,.$$

Now we can write a procedure `Tor` to compute $\mathrm{Tor}_i^A(M,N)$ for finitely generated left A–modules M and N, presented by the matrices `Ps` and

Ph. We compute $\texttt{Im} := \mathrm{Im}(1_{F_{i-1}} \otimes \psi)$, $\texttt{f} := \mathrm{Im}(\varphi_i \otimes 1_{G_0})$, $\texttt{Im1} := \mathrm{Im}(1_{F_i} \otimes \psi)$, $\texttt{Im2} := \mathrm{Im}(\varphi_{i+1} \otimes 1_{G_0})$, and obtain

$$\begin{aligned}
\mathrm{Tor}_i^A(M,N) &= \mathrm{Ker}\left(F_i \otimes_A G_0 \xrightarrow{\overline{\varphi_i \otimes 1_{G_0}}} (F_{i-1} \otimes_A G_0)/\texttt{Im}\right) \Big/ \big(\texttt{Im1} + \texttt{Im2}\big) \\
&= \texttt{modulo(f,Im)}/(\texttt{Im1} + \texttt{Im2})\,.
\end{aligned}$$

```
proc tensorMaps(matrix M, matrix N)
{
   int r=ncols(M);
   int s=nrows(M);
   int p=ncols(N);
   int q=nrows(N);
   int a,b,c,d;
   matrix R[s*q][r*p];
   for(b=1;b<=p;b++)
   {
      for(d=1;d<=q;d++)
      {
         for(a=1;a<=r;a++)
         {
            for(c=1;c<=s;c++)
            {
               R[(c-1)*q+d,(a-1)*p+b]=M[c,a]*N[d,b];
            }
         }
      }
   }
   return(R);
}

LIB "matrix.lib";

proc tensorMod(matrix Phi, matrix Psi)
{
   int s = nrows(Phi);
   int q = nrows(Psi);
   matrix A = tensorMaps(unitmat(s),Psi);  //I_s tensor Psi
   matrix B = tensorMaps(Phi,unitmat(q));  //Phi tensor I_q
   matrix R = concat(A,B);                 //sum of A and B
   return(R);
```

```
}

proc Tor(int i, matrix Ps, matrix Ph)
{
  if(i==0){ return(module(tensorMod(Ps,Ph))); }
                               // the tensor product
  list Phi   = mres(Ph,i+1);     // a resolution of Ph
  module Im  = tensorMaps(unitmat(nrows(Phi[i])),Ps);
  module f   = tensorMaps(matrix(Phi[i]),unitmat(nrows(Ps)));
  module Im1 = tensorMaps(unitmat(ncols(Phi[i])),Ps);
  module Im2 = tensorMaps(matrix(Phi[i+1]),unitmat(nrows(Ps)));
  module ker = modulo(f,Im);
  module tor = modulo(ker,Im1+Im2);
  tor        = prune(tor);
  return(tor);
}
```

Now, let us consider an example.

```
ring A=0,(x,y),dp;
matrix Ps[1][2]=x2,y;
matrix Ph[1][1]=x;
print(Tor(1,Ps,Ph));

  y,x
```

5.6 Hochschild cohomology

As an application we are able now to compute the Hochschild cohomology (for definitions and details cf. [C, CE]). Let A be a $\mathbb{K}$–algebra and M an A-bimodule. Let $A^e = A \otimes_{\mathbb{K}} A^o$ be the enveloping algebra (note that A^o is the opposite algebra to A, i.e. A as $\mathbb{K}$–vectorspace and the multiplication $a * b = ba$).Then M has the structure of an left A^e–module.

A itself is considered as bimodule over A^e in the canonical way ($(a \otimes b^*)x = axb^*$ and $x(a \otimes b^*) = b^*xa$).

The Hochschild cohomology $H^n(A, M)$ is defined to be $\mathrm{Ext}^n_{A^e}(A, M)$.

Recall, that the Hochschild cohomology $H^n(A, M)$ can also be characterized as the cohomology of the following complex:
Let $C^n(A, M) = \{n\texttt{-linear maps } : A \to M\}$ with the differential ∂ defined

as follows. For $\phi \in C^n(A, M)$ define $\partial(\phi)(a_1, \dots, a_{n+1}) = a_1\phi(a_2, \dots, a_{n+1}) + \sum_{1\le i\le n}(-1)^i\phi(a_1, \dots, a_i a_{i+1}, \dots, a_{n+1}) + (-1)^{n+1}\phi(a_1, \dots, a_n)a_{n+1}$.
Let us consider the following example:

```
ring A          = 0,(x,y),dp;
ideal I         = x2-y3;
qring B         = std(I);
ring C          = 0,(x,y,z,w),dp;
ideal I         = x2-y3,z3-w2;
qring Be        = std(I);   //the enveloping algebra
matrix AA[1][2] = x-z,y-w;  //the presentation of B as Be-module
print(Ext(1,AA,AA));  //the presentation of the H^1(A,A)

   y-w,0,  x-z,0,
   0,  y-w,0,  x-z
```

The Hochschild cohomology is quite important for non–commutative algebras. Consider the universal enveloping algebra $U(\mathfrak{sl}_2) = \mathbb{K}\langle e, f, h \mid [e, f] = h,\ [h, e] = 2e,\ [h, f] = -2f\rangle$ over field $\mathbb{K}$ of char 0. The center Z of $U(\mathfrak{sl}_2)$ is generated by the Casimir element $z = 4ef + h^2 - 2h$. Let the two–sided ideal I be generated by z, then we compute $H^i(U(\mathfrak{sl}_2)/I)$.

```
ring A = 0, (e,f,h,H,F,E),Dp; // any degree ordering
matrix @D[6][6];
@D[1,2] = -h;   @D[1,3] = 2*e;   @D[2,3] = -2*f;
@D[4,5] = 2*F;  @D[4,6] = -2*E;  @D[5,6] = H;
ncalgebra(1,@D);            // U(sl_2) * U(sl2)^o
poly z = 4*e*f+h^2-2*h;     // generator of the center
poly zo = 4*F*E+H^2+2*H;    // the same, opposed
ideal Qe = z,zo;
qring B = twostd(Qe);      // (U/I)^e = (U/I) * (U/I)^o
matrix M[1][3] = E,F,H;    // presentation of U/I as (U/I)^e - mod
module X0 = Ext(0,M,M);     print(X0);

  E,F,H

module X1 = Ext(1,M,M);     print(X1);

  0
```

```
module X2 = Ext(2,M,M);    print(X2);

 2HFE,2HE2,4E,2HF2,2HFE+2H2,4F,2H2F+4HF,2H2E-4HE,4H

print(std(ideal(X2)));  //  X2 simplified:

  E,F,H
```

We organize obtained results in the following list:

$$H^i(U(\mathfrak{sl}_2)/I) = \begin{cases} \mathbb{K}, & i = 0, \\ 0, & i = 1, \\ \mathbb{K}, & i = 2. \end{cases}$$

Moreover, we know that $H^2(U(\mathfrak{sl}_2)/I) \simeq \mathrm{Tor}_1^Z(\mathbb{K}, \mathbb{K})$ as Z/I–modules. We can check it directly by computing the latter Tor:

```
ring Z = 0,(z),dp; // center of U(sl_2)
matrix I[1][1]=z;
module T = Tor(1,I,I);
print(T);

  z
```

So, $\mathrm{Tor}_1^Z(\mathbb{K}, \mathbb{K}) = \mathbb{K}$ in this situation.

5.7 Tate resolution

Here we want to describe how non-commutative algebra can be used to solve problems in algebraic geometry (for details see [EGSS]).

Let V be an $n+1$-dimensional $\mathbb{K}$-vectorspace and $W = V^*$ its dual. Let $\{x_0, \dots, x_n\}$ be a basis of W , $S = Sym(W) = \mathbb{K}[x_0, \dots, x_n]$ the symmetric algebra and $E = \Lambda(V)$ the exterior algebra.
Let $M = \oplus M_i$ be a finitely generated S–module and define complexes
$F(M) : \cdots \to M_i \otimes_{\mathbb{K}} E \xrightarrow{\phi_i} M_{i+1} \otimes_{\mathbb{K}} E \to \cdots$
$\phi_i(m \otimes 1) = \sum x_j m \otimes x_j^*$
$R(M) : \cdots \to \mathrm{Hom}_{\mathbb{K}}(E, M_i)\} \xrightarrow{\phi_i^*} \mathrm{Hom}_{\mathbb{K}}(E, M_{i+1}) \to \cdots$
$\phi_i^*(\alpha)(e) = \sum_j x_j \alpha(x_j^* \wedge e)$

Recall, that the Castelnuovo–Mumford regularity is defined as follows: Let $S = \mathbb{K}[x_0, \ldots, x_n]$ and $M = \oplus M_i$ be a finitely generated graded S–module.Then $M_{\geq r} = \underset{i \geq r}{\oplus} M_i$ is generated in degree r and has a linear free resolution for large r. The least integer r with this property is the Castelnuovo–Mumford regularity.

Theorem 5.4. (Eisenbud, Fløstad, Schreyer). $R(M_{>r})$ is exact, r= Castelnuovo–Mumford regularity of M.

The Tate resolution $T(M)$ is defined by

$$T^{>r}(M) = R(M_{>r})$$

and a minimal projective resolution of the kernel of

$$\mathrm{Hom}_{\mathbb{K}}(E, M_{r+1}) \to \mathrm{Hom}_{\mathbb{K}}(E, M_{r+2}).$$

Theorem 5.5. (Eisenbud, Fløstad, Schreyer). Let $S = \mathbb{K}[x_0, \ldots, x_n]$ and M be a finitely generated graded S–module. Then

$$T^i(M) = \underset{j}{\oplus} H^j(\widetilde{M}(i-j)) \otimes \mathrm{Hom}_{\mathbb{K}}(E, \mathbb{K})$$

Note: Each cohomology group of each twist of the sheaf $\widetilde{M}$ occurs exactly once in a term of $T(M)$.

The following Singular procedures compute the sheaf cohomology:

```
LIB "matrix.lib";

proc jacobM(matrix M)
{
   int n    = nvars(basering);
   int a    = nrows(M);
   int b    = ncols(M);
   matrix B = transpose(diff(M,var(1)));
   int i,j;
   for(i=2; i<=n; i++)
   {
     B = concat(B,transpose(diff(M,var(i))));
   }
   return(transpose(B));
```

```
}

proc max(int i,int j)
{
  if(i>j) { return(i); }
  return(j);
}

proc truncate(module M, int d, int r)
{
//---truncates the module (cokernel of the presentation M)
//---whith the gen(j) of degree d at degree r
//---computes the corresponding presentation matrix

   int i;
   int n = nrows(M);
   module L;
   for(i=1; i<=n; i++)
   {
     L = L + maxideal(r-d)*gen(i);
   }
   module Mstd = std(M);
   L = reduce(L,Mstd);
   L = modulo(L+Mstd,Mstd);
   L = prune(L);
   return(L);
}

proc sheafCoh(module M, int d, int l, int h)
{
//--- d is the degree of gen(j) for M
//--- l low degree
//--- h high degree

  def R     = basering;
  int reg   = regularity(mres(M,0))-1;
  int bound = max(reg+1,h-1);
  module MT = truncate(M,d,bound);
  int m     = nrows(MT);
  MT        = transpose(jacobM(MT));
  MT        = syz(MT);
```

```
  int n     = nvars(basering);
  matrix ML[n][1]=maxideal(1);
  matrix S  = transpose(outer(ML,unitmat(m)));
  matrix SS = transpose(S*MT);
//--- to the exterior algebra
  execute("ring AR="+charstr(R)+",("+varstr(R)+"),dp;");
  ncalgebra(-1,0); // now ring AR is anticommutative
  int in = 1;
  ideal aus;
  for (in=1; in<=n; in++)   { aus[in] = var(in)^2; }
  aus     = twostd(aus);
  qring S = aus; // S is an exterior algebra
  option(redSB);
  option(redTail);
  matrix EM = imap(R,SS);
//--- here we are with our matrix
  int bound1    = max(1,bound-l+1);
  resolution RE = mres(EM,bound1+1);
  print(betti(RE),"betti");
  setring R;
  option(noredSB);
  option(noredTail);
}
```

Let us consider the following example:

```
   ring R=0,(x,y,z,u),dp;
   resolution T1 = mres(maxideal(1),0);
   module      M = T1[3];
   sheafCoh(M,1,-6,2);

       0    1    2    3    4    5    6    7    8    9
-----------------------------------------------------
 0:    20   6    -    -    -    -    -    -    -    -
 1:     -   -    1    -    -    -    -    -    -    -
 2:     -   -    -    -    -    -    -    -    -    -
 3:     -   -    -    4   15   36   70  120  189  280
-----------------------------------------------------
total: 20   6    1    4   15   36   70  120  189  280
```

References

[MR] J.C. McConnell, J.C. Robson, *Noncommutative Noetherian Rings,* Graduate Studies in Math. 30 AMS, 2000.

[H] Huishi Li, *Noncommutative Groebner Bases and Filter-Graded Transfer*, Springer, SLN 1795.

[C] A. Connes, *Non-commutative differential geometry*, Publ. Math. IHES 62 (1985).

[BTV] J.L. Bueso, J.G. Torrecillas, A. Verschoren, *Algorithmic methodes in non-commutative Algebra*, Kluwer Acad. Press 2003.

[EGSS] D. Eisenbud, D.R. Grayson, M. Stillman, B. Sturmfels, *Computations in Algebraic Geometry with Macaulay 2*, Springer, 2002.

[GP] G.-M. Greuel, G. Pfister,*A SINGULAR Introduction to Commutative Algebra*, Springer, 2002.

[CE] H. Cartan, S. Eilenberg,*Homological Algebra*, London, 1956.