Mathematisches Forschungsinstitut Oberwolfach

Report No. 50/2009

DOI: 10.4171/OWR/2009/50

Mini-Workshop: Formal Methods in Commutative Algebra: A View Toward Constructive Homological Algebra

Organised by
Thierry Coquand, Göteborg
Alban Quadrat, INRIA Sophia Antipolis
Ihsen Yengui, Sfax

November 8th – November 14th, 2009

Abstract. The purpose of the mini-workshop is to bring into the same place different mathematical communities that study constructive homological algebra and are motivated by different applications (e.g., constructive algebra, symbolic computation, proof theory, algebraic topology, mathematical systems theory, D-modules, dynamical systems theory) so that they can share their results, techniques, softwares and experiences. Through the development of a unified terminology, common mathematical problems, which naturally appear when making homological algebra constructive, were discussed.

Mathematics Subject Classification (2000): Primary 03F65; Secondary 13Pxx, 16Exx, 16Sxx, 18Gxx.

Introduction by the Organisers

The mini-workshop entitled *Formal Methods in Commutative Algebra: A View Toward Constructive Homological Algebra*, organised by Thierry Coquand (University of Göteborg), Alban Quadrat (INRIA Sophia Antipolis) and Ihsen Yengui (University of Sfax) was held from November 8th to November 14th, 2009. This meeting was attended by 14 participants coming from England, France, Germany, Spain, Sweden and Tunisia (one participant from Morocco was not able to come due to health problems).

Homological algebra is nowadays playing a significant role in different parts of pure mathematics (e.g., algebraic topology, algebraic geometry, sheaf theory, D-modules), mathematical physics and more surprisingly in different applied fields of mathematics (e.g., mathematical systems theory, control theory, dynamical systems). This can easily be explained by the fact that homological algebra develops universal, powerful and intrinsic mathematical methods which can be applied to a large part of mathematics especially where linear systems of equations over a ring are involved. However, the methods of homological algebra generally involve large and tricky computations which cannot be easily achieved by hand and thus require the use of computers. To do that, the mathematician first needs to make them constructive at least for his particular field of interest. Generally, this is not an easy task. But the fast development of computer algebra and proof-assisted systems gives our generation the nice opportunity to develop the first efficient softwares dedicated to homological algebra and its applications.

The purpose of the mini-workshop was firstly to bring into the same place different mathematical communities that share a common interest for the development of constructive homological algebra, its implementations in computer algebra and computer-assisted proof systems as well as for its applications in different mathematical fields (e.g., constructive algebra, symbolic computation, proof theory, algebraic topology, mathematical systems theory, D-modules, dynamical systems theory) so that these communities can exchange their knowledge, experiences, results and softwares.

Secondly, all along the three lectures, a unified terminology was developped, and common mathematical problems which naturally appear when making homological algebra constructive were discussed (e.g., when can we say that a homology can be computed? what kind of algebraic conditions does it require? which kind of results and techniques of homological algebra can be made constructive, how to implement them and in which languages?).

Finally, the last goal of this mini-workshop was to federate researchers interested in the constructive aspects of homological algebra, their implementations in computer algebra and proof assistant systems and their applications in different mathematical fields. We hope that this mini-worksop will be the starting point for the development of a new community, dedicated to these issues, who will exchange on regular basis through meetings, conferences, summer schools...

The mini-workshop was divided into three lectures on constructive algebra and constructive homological algebra:

(1) **Introduction to homological algebra**, M. Barakat, D. Robertz (6 hours)
(2) **Introduction to constructive algebra**, H. Lombardi (4 hours)
(3) **Constructive homological algebra**, F. Sergeraert (3 hours)

and into five specialized talks which studied different aspects of constructive homological algebra and their applications in mathematical fields:

(1) **Ring theory** (Serre-Auslander-Buchsbaum theorem, coherent rings, characterization of module properties)

(2) **Algebraic topology** (constructive algebraic topology, perturbation lemma, spectral sequences, exact couples)
(3) **Mathematical systems theory** (parametrizability, factorization, reduction and decomposition problems, Serre's reduction)
(4) **Noncommutative ring theory and algebraic D-modules** (Gelfand-Kirilov dimension, Cohen-Macaulay property, Auslander regularity for noncommutative G-algebra)
(5) **Dynamical systems** (conley index, spectral sequences)

Mini-Workshop: Formal Methods in Commutative Algebra: A View Toward Constructive Homological Algebra

Table of Contents

Abstracts

Spectral sequences and effective computations

Mohamed Barakat

1. Introduction

This extended abstract of a series of talks held during the MFO-mini-workshop "A View Toward Constructive Homological Algebra" is also meant to be a short guide to [1]. All modules are understood as modules over an associative ring with one.

An m-step filtration on a module C induces an m-step filtration on any of its subfactor modules. This easy consequence of the isomorphism theorems is detailed in Section 2 for the case of a 2-step filtration.

On the other hand, the modules C_n of an m-step filtered complex

$$\begin{tikzcd} C: & \cdots & C_{n-1} \arrow[l, "\partial_{n-1}"'] & C_n \arrow[l, "\partial_n"'] & C_{n+1} \arrow[l, "\partial_{n+1}"'] & \cdots \arrow[l, "\partial_{n+2}"'] \end{tikzcd}$$

are by definition m-step filtered. A complex is called filtered if the boundary maps ∂ respect the filtrations of its modules. For example, a 2-step filtered complex is thus nothing but a complex C together with a subcomplex $A \leq C$.

Combining the two remarks above it follows that the homologies

$$H_n(C) := Z_n(C)/B_n(C) := \ker \partial_n / \operatorname{im} \partial_{n+1}$$

as subfactor modules of the modules C_n of an m-step filtered complex C are again m-step filtered.

This provides a mechanism to construct filtrations on a given module W by realizing it as the homology $H_n(C) \cong W$ of some filtered complex C. Often enough this is the only known way to construct certain desired filtrations on W.

2. A generality on submodule lattices

Let C be a module, Z, B, and A submodules with $B \leq Z$. Then the submodule lattice of C is at most a **degeneration** of the one in Figure 1.

This lattice makes no statement about the "size" of B or Z compared to A, since, in general, neither B nor Z is in a $\leq$-relation with A. The **second**[1] **isomorphism theorem** can be applied ten times within this lattice, two for each of the five parallelograms. The submodule A leads to the **intermediate submodule** $A' := (A + B) \cap Z$ sitting between B and Z, which in general neither coincides with Z nor with B. Hence, a 2-step filtration $0 \leq A \leq C$ induces a 2-step filtration $0 \leq A'/B \leq Z/B$.

This can be generalized to objects and subobjects in abelian categories. Arguing in terms of subobject lattices is a manifestation of the isomorphism theorems, all being immediate corollaries of the homomorphism theorem (cf. [2]).

[1] Here we follow the numbering in Emmy Noether's fundamental paper [2].

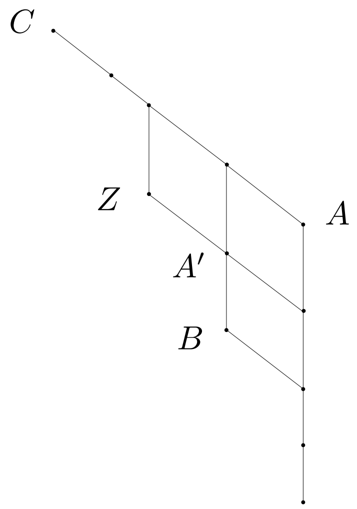


Figure 1. A general lattice with submodules $B \leq Z$ and A

3. Spectral sequences generalize long exact sequences

The main idea behind spectral sequences of filtered complexes can already be demonstrated in the case of a 2-step filtered complex $C \geq A$. A 2-step filtered complex C induces a short exact sequence of complexes $0 \leftarrow R \overset{\nu}{\leftarrow} C \overset{\iota}{\leftarrow} A \leftarrow 0$ with $R := C/A$.

The homologies of the three complexes (A, ∂_A), (C, ∂), and (R, ∂_R) fit together in a long exact (homology) sequence

$$\cdots \longleftarrow H_{n-1}(A) \xleftarrow{\partial_*} H_n(R) \xleftarrow{\nu_*} H_n(C) \xleftarrow{\iota_*} H_n(A) \xleftarrow{\partial_*} H_{n+1}(R) \longleftarrow \cdots ,$$

with so-called **connecting homomorphisms** ∂_* of degree -1. They detect the remaining off-diagonal information $\partial_{R \to A}$ of the boundary map ∂ which is not covered by ∂_A and ∂_R:

$$\partial = \begin{pmatrix} \partial_A & \partial_{R\to A} \\ 0 & \partial_R \end{pmatrix}.$$

A more provocative (inexact but suggestive) notation would be

$$\partial = \begin{pmatrix} \partial_A & \partial_* \\ 0 & \partial_R \end{pmatrix}.$$

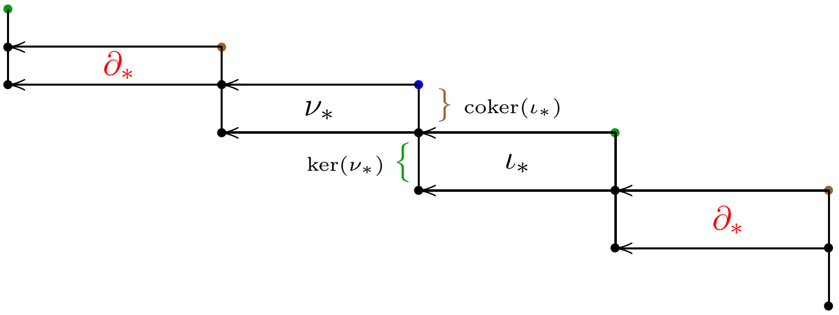
In other words, the degree 0 maps ∂_R and ∂_A capture the level preserving information in ∂, while the degree -1 connecting homomorphisms detect the remaining inter-level communication between R and A. In a 2-step filtered complex this covers all of ∂. Viewing things in this way it is now not surprising that for an m-step filtered complex one would in general still need degree -2 till degree $-m$ maps to get a full grasp on ∂.

As long exact sequences are more or less[2] tailored for the 2-step filtered complexes, they do not generalize to m-step filtrations whenever $m > 2$. The language of spectral sequences offers in this respect a better alternative.

[2] In fact, any module homomorphism induces a long exact sequence.

Before introducing the language of spectral sequences we first point out how the long exact sequence encodes the induced 2-step filtration on $H_n(C)$. This is indicated in the following diagram:

$$H_{n-1}(A) \xleftarrow{\partial_*} H_n(R) \xleftarrow{\nu_*} H_n(C) \xleftarrow{\iota_*} H_n(A) \xleftarrow{\partial_*} H_{n+1}(R) \tag{1}$$



Finally to motivate the transition to spectral sequences we note that the two graded parts

$$\operatorname{coker}(\iota_*) =: \operatorname{gr}_1 H_n(C) \qquad \text{and} \qquad \ker(\nu_*) =: \operatorname{gr}_0 H_n(C)$$

shown in (1) of the filtration of $H_n(C)$ both have an alternative description in terms of the connecting homomorphisms:

$$\operatorname{coker}(\iota_*) \cong \ker(\partial_*) \qquad \text{and} \qquad \ker(\nu_*) \cong \operatorname{coker}(\partial_*). \tag{2}$$

These natural isomorphisms are nothing but the statement of the homomorphism theorem applied to ι_* and ν_*.

Figure 2 shows the submodule lattice of C_n with all relevant submodules together with the submodule lattice of the filtered total homology $H_n(C)$ extracted to its left.

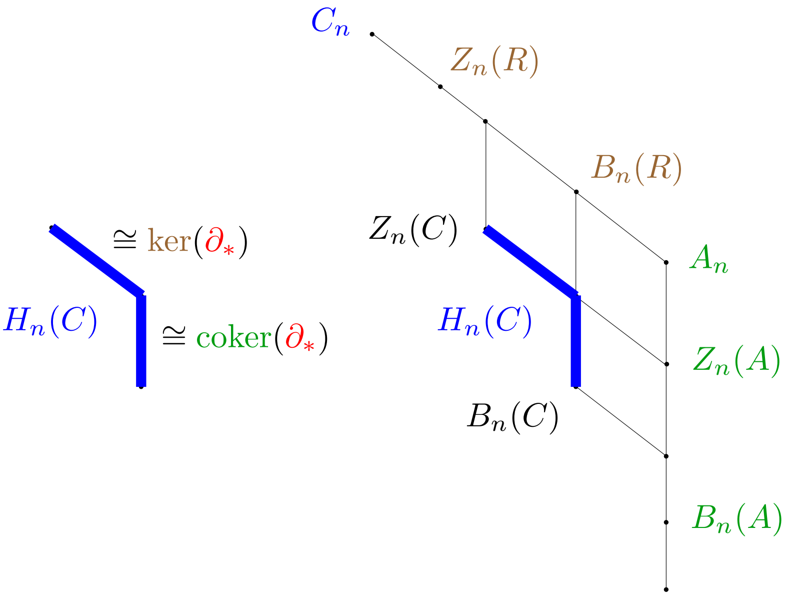
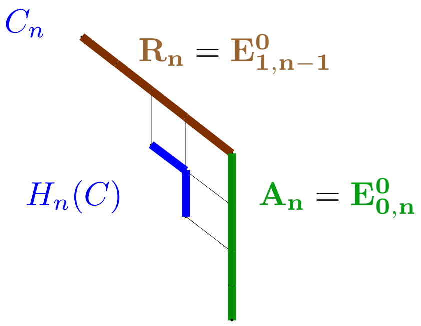


Figure 2. The 2-step filtration $0 \leq A \leq C$ and the induced 2-step filtration on $H_n(C)$

Part of the data we have in the context of long exact sequences can be organized in three successive "pages" E^0, E^1, and E^2. They describe the approximation of the graded parts of $H_n(C)$ in three steps:

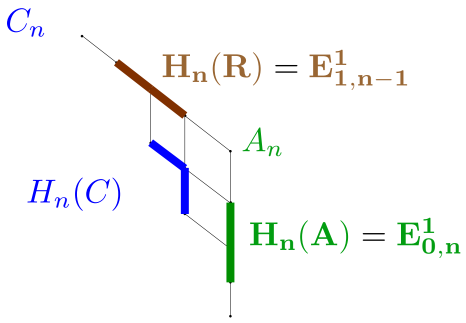
$$\begin{tikzcd}[row sep=large]
(A_n, R_n) & =: \arrow[d, squiggly] & (\mathrm{gr}_0\, C_n, \mathrm{gr}_1\, C_n) \\
(H_n(A), H_n(R)) & := \arrow[d, squiggly] & (Z_n(A)/B_n(A), Z_n(R)/B_n(R)) \\
(\mathrm{coker}(\partial_*), \ker(\partial_*)) & =: & (\mathrm{gr}_0\, H_n(C), \mathrm{gr}_1\, H_n(C)).
\end{tikzcd}$$

This approximation is achieved by successively taking deeper inter-level interaction into account. Since we are dealing with a 2-step filtration each page E^a has exactly two columns:



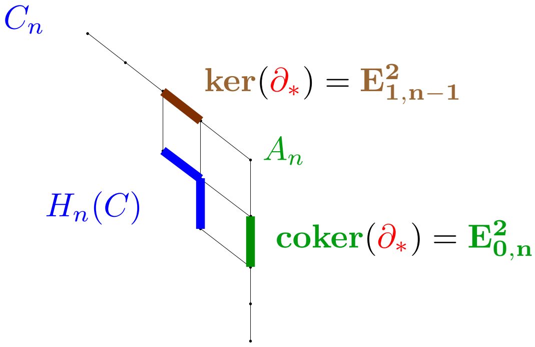
$$\begin{tikzcd}
A_{n+1} \arrow[d, "\partial_A"] \arrow[dr, dotted, no head] & R_{n+2} \arrow[d, "\partial_R"] & & E^0_{0,n-1} \arrow[d, "\partial_A"] \arrow[dr, dotted, no head] & E^0_{1,n-1} \arrow[d, "\partial_R"] \\
\mathbf{A_n} \arrow[d, "\partial_A"] \arrow[dr, dotted, no head] & R_{n+1} \arrow[d, "\partial_R"] & = & \mathbf{E^0_{0,n}} \arrow[d, "\partial_A"] \arrow[dr, dotted, no head] & E^0_{1,n} \arrow[d, "\partial_R"] \\
A_{n-1} \arrow[d, "\partial_A"] \arrow[dr, dotted, no head] & \mathbf{R_n} \arrow[d, "\partial_R"] & & E^0_{0,n-1} \arrow[d, "\partial_A"] \arrow[dr, dotted, no head] & \mathbf{E^0_{1,n-1}} \arrow[d, "\partial_R"] \\
A_{n-2} & R_{n-1} & & E^0_{0,n-2} & E^0_{1,n-2}
\end{tikzcd}$$

$$\begin{tikzcd}
{} \arrow[d, squiggly, "\text{take}"', "\text{homology}"] \\
{}
\end{tikzcd}$$


C_n
$\mathbf{H_n(R) = E^1_{1,n-1}}$
A_n
$H_n(C)$
$\mathbf{H_n(A) = E^1_{0,n}}$

$$\begin{tikzcd}
H_{n+1}(A) & H_{n+2}(R) \arrow[l, "\partial_*"'] & & E^1_{0,n-1} & E^1_{1,n-1} \arrow[l, "\partial_*"'] \\
\mathbf{H_n(A)} \arrow[ur, dash, dotted] & H_{n+1}(R) \arrow[l, "\partial_*"'] & = & \mathbf{E^1_{0,n}} \arrow[ur, dash, dotted] & E^1_{1,n} \arrow[l, "\partial_*"'] \\
H_{n-1}(A) \arrow[ur, dash, dotted] & \mathbf{H_n(R)} \arrow[l, "\partial_*"'] & & E^1_{0,n-1} \arrow[ur, dash, dotted] & \mathbf{E^1_{1,n-1}} \arrow[l, "\partial_*"'] \\
H_{n-2}(A) \arrow[ur, dash, dotted] & H_{n-1}(R) \arrow[l, "\partial_*"'] & & E^1_{0,n-2} \arrow[ur, dash, dotted] & E^1_{1,n-2} \arrow[l, "\partial_*"']
\end{tikzcd}$$

$$\begin{tikzcd}
{} \arrow[d, squiggly, "\text{take}"', "\text{homology}"] \\
{}
\end{tikzcd}$$


C_n
$\mathbf{ker}(\partial_*) = \mathbf{E^2_{1,n-1}}$
A_n
$H_n(C)$
$\mathbf{coker}(\partial_*) = \mathbf{E^2_{0,n}}$

$$\begin{tikzcd}
\operatorname{coker}(\partial_*) & \ker(\partial_*) & & E^2_{0,n-1} & E^2_{1,n-1} \\
\mathbf{coker}(\partial_*) \arrow[ur, dash, dotted] & \ker(\partial_*) & = & \mathbf{E^2_{0,n}} \arrow[ur, dash, dotted] & E^2_{1,n} \\
\operatorname{coker}(\partial_*) \arrow[ur, dash, dotted] & \mathbf{ker}(\partial_*) & & E^2_{0,n-1} \arrow[ur, dash, dotted] & \mathbf{E^2_{1,n-1}} \\
\operatorname{coker}(\partial_*) \arrow[ur, dash, dotted] & \ker(\partial_*) & & E^2_{0,n-2} \arrow[ur, dash, dotted] & E^2_{1,n-2}
\end{tikzcd}$$

This is the spectral sequence of a 2-filtered complex.

Figure 3 below shows how the objects $E^\infty_{0,n} = E^2_{0,n}$ and $E^\infty_{1,n-1} = E^2_{1,n-1}$ in the last page $E^\infty = E^2$ of the spectral sequence filter the total homology $H_n(C)$. The second isomorphism theorem is used to travel inside the subobject lattice of C_n. The diagram suggests the notion of **generalized embeddings** introduced in [1, Section 4].

References

[1] Mohamed Barakat, *Spectral Filtrations via Generalized Morphisms*, (submitted) (`http://arxiv.org/abs/0904.0240`).

[2] Emmy Noether, *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, Math. Ann. **96** (1927), no. 1, 26–61. MR MR1512304

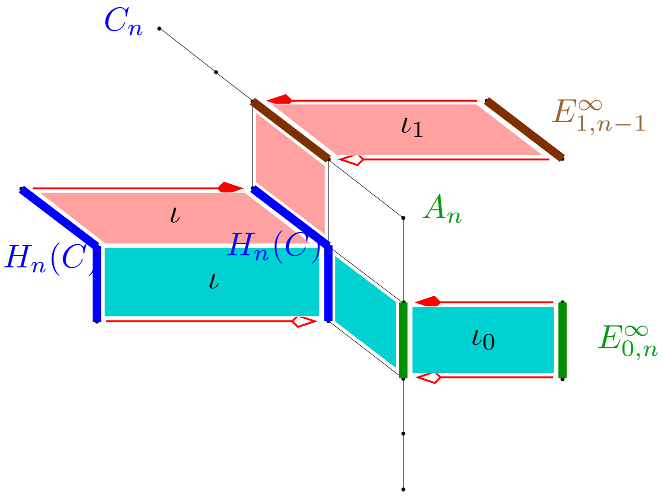


Figure 3. $\iota_0\iota^{-1}$ and $\iota_1\iota^{-1}$ filter $H_n(C)$

Constructive homological algebra

Francis Sergeraert
(joint work with Ana Romero and Julio Rubio)

Constructive homological algebra.

Talk 1: The Problem. The computability problem in Topological Algebra was born in 1953 when Jean-Pierre Serre proved most homology and homotopy groups of "reasonable" spaces are $\mathbb{Z}$-modules of finite type. The first positive result was obtained by Edgar Brown for the computability of the homotopy groups of finite simply connected simplicial sets, but his method is not concretely usable.

The main problem, practical and theoretical, is in the frequent appearance of objects *not of finite type*, mainly simplicial sets and chain complexes, objects which cannot be directly handled on a practical or theoretical machine. The standard tools to overcome such obstacles are exact and spectral sequences, but except in simple situations, these methods *are not* algorithms.

Functional programming is then a natural tool to process these infinite objects, at least if a finite set of data is finally sufficient to obtain the desired output of a computation.

The notion of SHP = *Solution for the Homological Problem* for a chain complex allows one to functionnally organize the workspace, describing how a finite set of data and a few functions *constructively* describe the homological nature of a chain complex, even if not of finite type.

If we consider the framework where the ground ring R is Cramer (= coherent + strongly discrete), that is, when the traditional computations around the Cramer systems in vector spaces can be processed, then an object of finite type is a module given through a finite presentation. It is natural to decide such a module is an *effective* R-module: the ordinary calculations of kernels and cokernels can be executed by a machine. However and unfortunately, this in general is not enough for the isomorphism problem between such modules, a serious gap in this area.

Finally the notions of *locally effective* and *fuzzy* R-modules are defined, allowing one to handle in a functional way various sorts of modules not of finite type. The standard decision problems for these modules in general cannot be solved.

Talk 2: Homological Perturbations. In general a SHP is made of "set-theoretic" maps, non-compatible with the module structures. This is a source of serious difficulties which can be frequently avoided when the theory of *Homological Perturbations* can be applied.

A *reduction* $\rho : \widehat{C}_* \Rrightarrow C_*$ is a strong chain equivalence between two chain complexes, expressing the big chain complex $\widehat{C}_*$ as the direct sum of the small one C_* and another one which is *explicitly* acyclic, thanks to a Hodge decomposition. Often, the big chain complex is only locally effective, while the small one is effective. The last one being effective, a SHP can be elementarily computed, and the reduction ρ then gives also a SHP for the big chain complex $\widehat{C}_*$.

Another property of these reductions is essential: if the differential of the big chain complex $\widehat{C}_*$ is *perturbed*, it is often possible to modify also the other data of the reductions to obtain an analogous reduction $\widehat{C}'_* \Rrightarrow C'_*$; it is the so called *Basic Perturbation Lemma* (BPL). It so happens a *fibration* is nothing but a *perturbed* product, a point which is the source of many applications of the BPL: Jean-Pierre Serre in the fifties proved many problems in Algebraic Topology can be reduced to problems about appropriate fibrations, and the BPL is then the ideal tool to transform the main spectral sequences, Serre and Eilenberg-Moore, into *algorithms* computing the desired homology groups.

A remarkable solution for the Adams' problem, due to Julio Rubio, is so obtained. If a simplicial set X is given *with effective homology* and is sufficiently reduced, then an *algorithm* produces a version *with effective homology* of the loop space ΩX. The data type of the output is the same as the data type of the input and the process can therefore be trivially iterated. The algorithm is implemented and computes some homology groups of loop spaces previously unreachable.

Talk 3: Using fuzzy modules. The BPL does not give a solution to make *effective* the spectral sequences not coming from a filtered chain complex, that is, when the spectral sequence is produced by an *exact couple.* Typical examples of such spectral sequences are the Bockstein and Bousfield-Kan spectral sequences, the last one describing the so rich, complex and interesting connection between homology and homotopy groups, leading to the famous Adams' spectral sequence.

An exact couple is a diagram:

$$\begin{tikzcd}
D \arrow[rr, "i"] & & D \arrow[dl, "j"] \\
& E \arrow[ul, "k"] &
\end{tikzcd}$$

where D and E are modules and the morphisms i, j and k are a circular exact sequence. A simple process produces a *derived* exact couple, and iterating this process often produces spectral sequences.

In the last talk it is proved that if D is a *fuzzy* module, if E is an *effective* module, and if the required exactness properties are *effective*, then an *algorithm* produces the derived exact couple, the last one satisfying the same effectiveness properties.

This gives *algorithms* computing for example the Bockstein and Bousfield-Kan spectral sequences. The particular case of the bicomplex spectral sequence is used to explain the method: then a solution for the SHP of every column is enough to make effective the initial exact couple. Iteratively applying the construction of the derived exact couple then computes the corresponding spectral sequence.

An *effective* version of the famous Bousfield-Kan spectral sequence is now the main goal to be reached following these lines. A quite fascinating workspace.

-o-o-o-o-o-o-

Constructive commutative algebra

Henri Lombardi

We will consider only commutative rings.

Finitely presented modules

A *finitely presented module* M is a module isomorphic to the cokernel of a linear map $\gamma : \mathbf{A}^m \longrightarrow \mathbf{A}^q$. The columns of the matrix $G \in \mathbf{A}^{q\times m}$ of γ form a generating system of the module of syzygies of the generating system $g_1, \ldots, g_q$ obtained as the image, under the surjective linear map $\pi : \mathbf{A}^q \to M$, of the canonical basis of $\mathbf{A}^q$. When we change the generating system it is possible to compute a presentation matrix for the new system by using the following trick. The structure of M remains unchanged if one applies to the presentation matrix G one of the following transformations.

— Insertion of a null column,

— Removal of a null column, except in case this leads to an empty matrix,

— Replacement of G, of size $q \times m$, by the matrix G' of size $(q+1) \times (m+1)$ obtained from G by adding a null row at the bottom and then a column to the right with 1 as entry in position $(q+1, m+1)$ (this means adding a vector to the list of generators, and giving a linear expression of the added vector in terms of previous generators):

$$G \;\mapsto\; G' \;=\; \begin{bmatrix} G & C \\ 0_{1,m} & 1 \end{bmatrix},$$

— The inverse operation of the previous one, except in case this leads to an empty matrix,

— Addition to a column of a linear combination of the others (this leaves unchanged the module of syzygies of the given generators),

— Addition to a row of a linear combination of the others (if we let L_i be the i-th row the replacing for instance L_1 $L_1 + \gamma L_2$ consists in replacing the generator g_2 by $g_2 - \gamma g_1$),
— Row or columns exchange

Theorem. *For given matrices $G \in \mathbf{A}^{q\times m}$ and $H \in \mathbf{A}^{r\times n}$ the following properties are equivalent.*
— *The cokernels of G and H are isomorphic.*
— *The two matrices of figure 1 are* elementarily equivalent*.*
— *The two matrices of figure 1 are* equivalent*.*

$$\begin{array}{c|c|c|c|c|} & m & r & q & n \\ \hline q & G & \mathit{0} & \mathit{0} & 0 \\ \hline r & 0 & \mathrm{I}_r & \mathit{0} & 0 \\ \hline \end{array} \qquad \begin{array}{c|c|c|c|c|} & m & r & q & n \\ \hline q & 0 & \mathit{0} & \mathrm{I}_q & 0 \\ \hline r & 0 & \mathit{0} & \mathit{0} & H \\ \hline \end{array}$$

Figure 1. The two matrices.

The category of finitely presented modules. The category of finitely presented modules over a ring $\mathbf{A}$ may be constructed from the one of finite rank free $\mathbf{A}$-modules by the following purely categorical process.
— A finitely presented module M is described by a triple $(\mathrm{K}_M, \mathrm{G}_M, \mathrm{A}_M)$, where A_M is a linear map between the finite rank free modules K_M and G_M. We have $M \simeq \operatorname{Coker} \mathrm{A}_M$ and the isomorphism is derived from a surjective linear map $\pi_M : \mathrm{G}_M \to M$ of kernel $\operatorname{Im} \mathrm{A}_M$. The matrix of A_M is a presentation of M.
— A linear map φ from the module M, given through $(\mathrm{K}_M, \mathrm{G}_M, \mathrm{A}_M)$, to the module N, given through $(\mathrm{K}_N, \mathrm{G}_N, \mathrm{A}_N)$, is described by two linear maps $\mathrm{K}_\varphi : \mathrm{K}_M \to \mathrm{K}_N$ and $\mathrm{G}_\varphi : \mathrm{G}_M \to \mathrm{G}_N$ subject to commutation relation $\mathrm{G}_\varphi \circ \mathrm{A}_M = \mathrm{A}_N \circ \mathrm{K}_\varphi$.

$$\begin{tikzcd} \mathrm{K}_M \arrow[r, "\mathrm{A}_M"] \arrow[d, "\mathrm{K}_\varphi"'] & \mathrm{G}_M \arrow[r, two heads, "\pi_M"] \arrow[d, "\mathrm{G}_\varphi"] & M \arrow[d, "\varphi"] \\ \mathrm{K}_N \arrow[r, "\mathrm{A}_N"'] & \mathrm{G}_N \arrow[r, two heads, "\pi_N"'] & N \end{tikzcd}$$

— The sum of two maps maps φ and ψ of M to N, given respectively by $(\mathrm{K}_\varphi, \mathrm{G}_\varphi)$ and $(\mathrm{K}_\psi, \mathrm{G}_\psi)$, is represented by $(\mathrm{K}_\varphi + \mathrm{K}_\psi, \mathrm{G}_\varphi + \mathrm{G}_\psi)$. In the same way, given $a \in \mathbf{A}$ the linear map map $a\varphi$ is represented by $(a\mathrm{K}_\varphi, a\mathrm{G}_\varphi)$.
— The representation of the composition of two linear maps is obtained by composing their representations.
— Finally, a linear map φ from M to N represented by $(\mathrm{K}_\varphi, \mathrm{G}_\varphi)$ is zero if and only if there exists $Z_\varphi : \mathrm{G}_M \to \mathrm{K}_N$ such that $\mathrm{A}_N \circ Z_\varphi = \mathrm{G}_\varphi$.

The above categorical construction shows that the questions concerning finitely presented modules may always be interpreted as questions concerning matrices, and very often reduce to linear system solving over the ring $\mathbf{A}$. For example, if one is given M, N and φ and looks for a linear map $\sigma : N \to M$ satisfying $\varphi \circ \sigma = \mathrm{Id}_N$, the question reduces to find $\mathrm{K}_\sigma : \mathrm{K}_N \to \mathrm{K}_M$, $\mathrm{G}_\sigma : \mathrm{G}_N \to \mathrm{G}_M$ and $Z : \mathrm{G}_N \to \mathrm{K}_N$ such that $\mathrm{G}_\sigma \circ \mathrm{A}_N = \mathrm{A}_M \circ \mathrm{K}_\sigma$ and $\mathrm{A}_N \circ Z = \mathrm{G}_\varphi \circ \mathrm{G}_\sigma - \mathrm{Id}_{\mathrm{G}_N}$. This is nothing but a linear system whose unknowns are the entries of the matrices of the linear maps G_σ, K_σ and Z.

Stability properties, coherence, discreteness. Finitely presented modules are stable by change of base ring and tensor products.

When the base ring is *coherent* (finitely generated ideals are finitely presented), finitely presented modules are coherent (finitely generated submodules are finitely presented) and stable for the Hom functor. Moreover one can compute a resolution by finite free modules for an arbitrary finitely presented module.

Theorem. *A module is coherent exactly when*
— the intersection of two arbitrary finitely generated submodules is finitely generated, and
— the annihilator of each element is a finitely generated ideal.

A set is said to be *discrete* when there is an equality test between the elements of the set, i.e. if $\forall x, y \in E$, $x = y$ or $x \neq y$. The real number field is *not* discrete. From a classical point of view, all sets are discrete.

A module M (or a ring) is said to be *strongly discrete* if for every fintely generated submodule N, the quotient module M/N is discrete. Over a strongly discrete ring, a finitely presented module is strongly discrete.

A *discrete field* $\mathbf{k}$ is a ring in which each element is zero or invertible. A discrete field $\mathbf{k}$ is a discrete set if and only if $1 =_{\mathbf{k}} 0$ or $1 \neq_{\mathbf{k}} 0$, if and only if $\mathbf{k} = \{0\}$ or not.

Fitting ideals. Let $G \in \mathbf{A}^{q\times m}$ be a presentation matrix of an $\mathbf{A}$-module M given by q generators. The *Fitting ideals of* M are the ideals $\mathcal{F}_{\mathbf{A},n}(M) = \mathcal{F}_n(M) := \mathcal{D}_{\mathbf{A},q-n}(G)$ $(n \in \mathbb{Z})$. They are well defined, i.e., they do not depend on the chosen presentation of M. We have the following chain of inclusions:

$$\langle 0 \rangle = \mathcal{F}_{-1}(M) \subseteq \mathcal{F}_0(M) \subseteq \cdots \subseteq \mathcal{F}_q(M) = \langle 1 \rangle\,.$$

Also $\mathrm{Ann}(M)^q \subseteq \mathcal{F}_0(M) \subseteq \mathrm{Ann}(M)$.

Theorem. *The following properties are equivalent.*
— The Fitting ideals of M are generated by idempotent elements.
— There exist a matrix H s.t. $GHG = G$.
— M is projective finitely generated, i.e., is isomorphic to a direct summand in a finite rank free module.

As a consequence, if $\mathbf{A}$ is strongly discrete, we have an effective procedure for deciding if a given finitely generated module is projective. For "fast" algorithms see [3].

Flatness and finite presentation. Theorem. *For a module M the following properties are equivalent.*
— M is flat.
— Any linear map $N \to M$ where N is finitely presented, factorizes through a finite rank free module.

Theorem. *Let M be a module and $X \in M^{n\times 1}$ a column vector whose coefficients $x_1, \ldots, x_n$ are a generating system for M. Then M is flat if and only if for each linear dependence relation $LX = 0$ ($L \in \mathbf{A}^{1\times n}$), there exist matrices $G, H \in \mathbb{M}_n(\mathbf{A})$ s.t. $H + G = \mathrm{I}_n$, $LG = 0$* and *$HX = 0$.*
In particular a module $M = \mathbf{A}y$ is flat if and only if

$$\forall a \in \mathbf{A},\ ay = 0 \ \Rightarrow\ \exists s \in \mathbf{A},\ \ as = 0,\ sy = y.$$

Theorem. *For a module M the following properties are equivalent.*
— M is finitely presented and flat.
— M is projective finitely generated.

By definition a ring is *local* if $x + y$ invertible implies x or y invertible.

Theorem. *Let M be a finitely generated flat module over a local ring $\mathbf{A}$. Assume that M is strongly discrete. Then M is free and a basis can be extracted from any generating system.*

By definition a ring $\mathbf{A}$ is *integral* (we say also that $\mathbf{A}$ is a domain) if each element is zero or regular. Constructively this notion is slightly stronger than the notion of *a ring without zero divisors*, that means $xy = 0$ implies $x = 0$ or $y = 0$.

Theorem. *Let $\mathbf{A}$ be a domain and $\mathbf{K}$ its total ring of fractions (which is a discrete field). Let M be a finitely generated flat module over $\mathbf{A}$. Assume that the finitely generated vector space $\mathbf{K} \otimes_{\mathbf{A}} M$ has a basis. Then M is projective finitely generated.*

Theorem. *For a ring $\mathbf{A}$ the following properties are equivalent.*
— Each principal ideal is generated by an idempotent.
— Each module is flat.
— $\mathbf{A}$ is von Neuman regular ($\forall x\ \exists y\ x^2y = x,\ y^2x = y$).

A bit more about coherence

From a constructive point of view, coherence is a crucial concept, more important than noetherianity. Here is a constructive definition (equivalent to the classical one in classical mathematics) for noetherianity.

Definition. *A module is said to be* Noetherian *if it satisfies the following* ascending chain condition*: any ascending sequence of finitely generated submodules has two consecutive equal terms. A ring $\mathbf{A}$ is called* Noetherian *if it is Noetherian as an $\mathbf{A}$-module.*

With this definition one has strong constructive results. E.g.,

Theorem. *If* $\mathbf{A}$ *is a coherent Noetherian ring then any finitely presented* $\mathbf{A}$*-module is coherent Noetherian.*

In classical mathematics, any Noetherian ring $\mathbf{A}$ is coherent since all submodules of $\mathbf{A}^n$ are finitely generated, and any finitely generated module is coherent for the same reason. From an algorithmic point of view, it seems however hopeless to find a constructive and satisfactory formulation of noetherianity that implies coherence.

We have the following constructive version of Hilbert Basis Theorem (see [5]):

Theorem. *If* $\mathbf{A}$ *is a coherent Noetherian ring then so is any finitely presented* $\mathbf{A}$*-algebra* $\mathbf{B}$*. Moreover if* $\mathbf{A}$ *is strongly discrete then so is* $\mathbf{B}$*.*

Definition.
— *A system of elements* $s_1, \ldots, s_n$ *in* $\mathbf{A}$ *is called* comaximal *if and only if* $\langle 1 \rangle = \langle s_1, \ldots, s_n \rangle$*.*
— *A system of monoids* $S_1, \ldots, S_n$ *of a ring* $\mathbf{A}$ *is called* comaximal *if for any* $s_1 \in S_1, \ldots, s_n \in S_n$ *the* s_i*'s are comaximal.*

Definition. *A ring* $\mathbf{A}$ *is said to be* arithmetical *if it satisfies one of the following equivalent properties.*
— *Each finitely generated ideal is* locally principal*, i.e., it becomes principal after localization at suitable comaximal elements.*
— *The intersection of two finitely generated ideals is finitely generated, and finitely generated ideals form a distributive lattice.*
— $\forall x, y,\ \exists u, v, s, t \quad sx = uy,\ ty = vx,\ s + t = 1.$

An arithmetical domain is called a *Prüfer domain.* It is easily seen that a Prüfer domain is coherent. Moreover it is strongly discrete if and only if the divisibility relation is explicite. Over a Prüfer domain each finitely generated ideal is projective. Also the kernel of a matrix is always a direct summand, so the kernel and the image of a matrix are projective finitely generated. The class of Prüfer domains seems important in applications, e.g. to control theory.

The following results are important and provable in classical mathematics, but we don't know any constructive proof. Perhaps some facts which are always true in classical mathematics have to be added to the hypotheses in order to get constructive theorems.

Theorem* *If* $\mathbf{A}$ *is a Prüfer domain, then* $\mathbf{A}[X_1, \ldots, X_n]$ *is a coherent ring.*

This is a particular case for a far more general result. A ring is called a *coherent regular ring* if each finitely generated ideal admits a finite projective resolution.

Theorem* *If* $\mathbf{A}$ *is a coherent regular ring, then so is* $\mathbf{A}[X_1, \ldots, X_n]$*.*

Local-global principles: concrete and abstract. Theorem. (basic concrete local-global principle)
Let $S_1, \ldots, S_n$ *be comaximal monoids of a ring* $\mathbf{A}$*,* B *a matrix in* $\mathbf{A}^{m \times p}$ *and* C *a column vector in* $\mathbf{A}^{m \times 1}$*. Then the following properties are equivalent.*
— *The linear system* $BX = C$ *has a solution in* $\mathbf{A}^p$*.*
— *For each* i *the linear system* $BX = C$ *has a solution in* $\mathbf{A}^p_{S_i}$*.*

Theorem. (basic abstract local-global principle)
Let $\mathbf{A}$ *be a ring,* B *a matrix in* $\mathbf{A}^{m\times p}$ *and* C *be a column vector in* $\mathbf{A}^{m\times 1}$*. Then the following properties are equivalent.*
— The linear system $BX = C$ *has a solution in* $\mathbf{A}^p$*.*
— For each prime ideal $\mathfrak{p}$ *the linear system* $BX = C$ *has a solution in* $\mathbf{A}^p_{\mathfrak{p}}$*.*

The abstract theorem has the advantage that it is not needed to find comaximal monoids. The inconvenient is that it does not give any algorithm for solving the given linear system. Moreover some concrete local-global principles are strong but there is no corresponding abstract local-global principle. E.g. the four first ones in the following list.

Theorem. (some concrete local-global principles for modules)
Let $S_1, \dots, S_n$ *be comaximal monoids of a ring* $\mathbf{A}$*, and* M*,* N*,* P *be* $\mathbf{A}$*-modules.*
— M *is finitely generated if and only if each* M_{S_i} *is finitely generated.*
— M *is finitely presented if and only if each* M_{S_i} *is finitely presented.*
— M *is projective finitely generated if and only if each* M_{S_i} *is projective finitely generated.*
— M *is coherent if and only if each* M_{S_i} *is coherent.*
— M *is flat if and only if each* M_{S_i} *is flat.*
— M *is Noetherian if and only if each* M_{S_i} *is Noetherian.*
— A sequence of linear maps $M \xrightarrow{\varphi} N \xrightarrow{\psi} P$ *is exact if and only if each sequence* $M_{S_i} \xrightarrow{\varphi_{S_i}} N_{S_i} \xrightarrow{\psi_{S_i}} P_{S_i}$ *is exact.*

Dynamical method (∼ lazzy evaluation)

The dynamical method has been introduced as a general tool for deciphering classical proofs without clear constructive counterpart.

This method is very similar to lazzy evaluation in Computer Algebra.

The method `D5` in Computer Algebra (see [2]) was invented in order to compute in a secure way inside the algebraic closure of a computable field without using factorization algorithms.

The fact that this method is very simple offers a strong contrast with the difficulties occurring when one wants to construct the algebraic closure of an arbitrary discrete field.

So the idea came that some abstract objects, as the algebraic closure of a field or the Zariski spectrum of a commutative ring, do have a constructive version if one allows dynamical objects rather that usual static objects.

A systematic use of these dynamical objects is made in recent papers which offer constructive understanding of e.g., algebraic closure, Zariski spectrum, Krull dimension and lead to constructive proofs of many important theorems which have previously only abstract proofs (see [4]).

References

[1] E. Bishop, D. Bridges, *Constructive Analysis*, Springer-Verlag, 1985.

[2] J. Della Dora, C. Dicrescenzo, D. Duval, *About a new method for computing in algebraic number fields*, In Caviness B.F. (Ed.) EUROCAL '85, Lecture Notes in Computer Science **204**, Springer, 1985, 289–290.

[3] G. Díaz-Toca, L. Gonzalez-Vega, H. Lombardi, C. Quitté, *Modules projectifs de type fini, applications linéaires croisées et inverses généralisés*, Journal of Algebra **303** (2006), 450–475.

[4] H. Lombardi, C. Quitté, *Algèbre Commutative, Méthodes Constructives*, to appear, available at `http://hlombardi.free.fr/publis/A---PTFCours.html`. An english version is to be published by Springer.

[5] R. Mines, F. Richman, W. Ruitenburg, *A Course in Constructive Algebra*, Universitext. Springer-Verlag, 1988.

The Auslander-Buchsbaum-Serre theorem

D. Robertz

The Auslander-Buchsbaum-Serre Theorem characterizes among the Noetherian commutative local rings the *regular* ones, i.e. those for which Krull dimension and embedding dimension coincide, as the ones whose global dimension is finite.

The geometric meaning of this notion of regularity is nonsingularity of the point corresponding to the maximal ideal of the local ring. More precisely, let V be an algebraic variety, which we assume irreducible for simplicity, and p a point of V. Then p is nonsingular if and only if the tangent space of V at p has the same dimension as V. If $\mathcal{O}$ is the coordinate ring of V, then the vector space dual of the tangent space of V at p is, up to isomorphism, given by $m_{p,V}/m_{p,V}^2$, where $m_{p,V}$ is the maximal ideal of the local ring $\mathcal{O}_{p,V}$ of V at p. By Nakayama's Lemma, a set of elements of $m_{p,V}$ is a minimal generating set for the ideal $m_{p,V}$ if their cosets modulo $m_{p,V}^2$ form a vector space basis of $m_{p,V}/m_{p,V}^2$. Therefore, p is nonsingular if and only if the Krull dimension of $\mathcal{O}_{p,V}$ equals its embedding dimension, which is defined to be the dimension of $m_{p,V}/m_{p,V}^2$.

The Koszul complex is a chain complex of free modules over the Noetherian commutative local ring R which is parametrized by a finite number of ring elements $g_1, \ldots, g_n$. Its homology detects the (common) length s of maximal regular sequences in the ideal I of R generated by $g_1, \ldots, g_n$, i.e. sequences of elements $r_1, \ldots, r_s$ in I such that multiplication by r_i on the module $R/(r_1, \ldots, r_{i-1})R$ is an injective map for every $i = 1, \ldots, s$ and such that no extension to a sequence of length $s + 1$ is possible satisfying the corresponding property. The number s is called the *depth* of I on R. More generally, if M is a finitely generated non-zero R-module, then the homology of the complex obtained by tensoring the Koszul complex for $g_1, \ldots, g_n$ with M detects the (common) length of maximal regular sequences on M in the ideal I, i.e. the depth of I on M. As it is an arithmetic measure of I and since in the case $s = n$, i.e. vanishing homology, the Koszul complex is a free resolution of R/I, these concepts are ubiquitous in commutative algebra, cf. e.g. [3].

The global dimension of R is the supremum of the projective dimensions of R-modules, i.e. the lengths of their shortest projective resolutions. By a result of Auslander, this supremum is the same if it is taken for all finitely generated R-modules.

Let m be the maximal ideal of the local ring R. For a finitely generated non-zero R-module M with finite projective dimension, the Auslander-Buchsbaum Formula states that its projective dimension is the difference of the depth of m on R and the depth of m on M.

A proof of the Auslander-Buchsbaum-Serre Theorem can be outlined as follows [3]: If R is regular, then it can be shown that R is an integral domain, from which one easily derives that m is minimally generated by a regular sequence $g_1, \dots, g_n$. The Koszul complex for $g_1, \dots, g_n$ is therefore a minimal free resolution of R/m. For a finitely generated R-module M, the homology $\mathrm{Tor}^R(M, R/m)$ arising from tensoring a free resolution of M with R/m characterizes the length of the resolution as the smallest non-negative integer i such that $\mathrm{Tor}^R_{i+1}(M, R/m)$ vanishes. Since this homology can also be computed by tensoring a free resolution of R/m by M, the projective dimension of R/m is shown to be an upper bound for the projective dimensions of finitely generated R-modules. Hence, the global dimension of R equals the length of the Koszul complex for $g_1, \dots, g_n$, which is n.

If R has finite global dimension, then it equals the projective dimension of R/m by the above argument involving $\mathrm{Tor}^R(M, R/m)$. However, it is not clear whether the Koszul complex for a minimal generating set $g_1, \dots, g_n$ of m is a free resolution of R/m. The Auslander-Buchsbaum Formula, applied to the R-module R/m, shows that the depth of m on R equals the projective dimension of R/m, which is finite. Since the Koszul complex for $g_1, \dots, g_n$ is a subcomplex of any minimal free resolution of R/m, the depth of m on R is therefore bounded below by n. Since the Krull dimension of R is an upper bound for this depth and the former is at most n by Krull's Principal Ideal Theorem, the equality of Krull dimension and embedding dimension of R is proved.

References

[1] G. Boffi, D. A. Buchsbaum, *Threading homology through algebra: selected patterns*, Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, Oxford, 2006.

[2] W. Bruns, J. Herzog, *Cohen-Macaulay rings*, *Cambridge Studies in Advanced Mathematics* **39**, Cambridge University Press, Cambridge, 1993.

[3] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry*, Graduate Texts in Mathematics, **150**, Springer-Verlag, New York, 1995.

[4] T. H. Gulliksen and G. Levin, *Homology of local rings*, Queen's Paper in Pure and Applied Mathematics **20**, Queen's University, Kingston, Ont., 1969.

[5] W. Krull, *Beiträge zur Arithmetik kommutativer Integritätsbereiche*, Math. Z., **42** (1937), 745–766.

[6] H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics **8**, Cambridge University Press, Cambridge, second edition, 1989.

[7] J. J. Rotman, *An introduction to homological algebra*, Universitext. Springer, New York, second edition, 2009.

Using constructive homological algebra for decomposing and reducing linear functional systems

Thomas Cluzeau
(joint work with Mohamed S. Boudellioua, Alban Quadrat)

The main purpose of this work is to show how symbolic computation methods can be used to simplify linear functional systems coming from mathematical physics, applied mathematics, engineering sciences and control theory. Simplifying a linear functional system is important problem which needs to be studied before investigating the structural properties and the existence of solutions of the system.

If D is an Ore algebra (i.e., a non-commutative polynomial ring of operators) and $R \in D^{q \times p}$ a matrix, then we can study the following four problems:

(1) **Factorization problem:** Find two matrices $L \in D^{q \times t}$ and $S \in D^{t \times p}$ such that $R = L\,S$.
(2) **Reduction problem:** Find two unimodular matrices $W \in \mathrm{GL}_p(D)$ and $V \in \mathrm{GL}_q(D)$ such that $V\,R\,W$ is a block-triangular matrix.
(3) **Decomposition problem:** Find two unimodular matrices $W \in \mathrm{GL}_p(D)$ and $V \in \mathrm{GL}_q(D)$ such that $V\,R\,W = \mathrm{diag}(Q_1, Q_2)$.
(4) **Serre's reduction problem:** Find two unimodular matrices $W \in \mathrm{GL}_p(D)$ and $V \in \mathrm{GL}_q(D)$ such that $V\,R\,W = \mathrm{diag}(I_{q-1}, Q)$.

We study these problems within a module theoretical framework. The techniques used are module theory and constructive homological algebra. All along the talk, the theoretical results are illustrated with explicit examples coming from mathematical physics, applied mathematics, engineering sciences or control theory. The different algorithms presented here have been implemented in two packages: OreMorphisms [1] and Serre[2] which are both built upon OreModules[3].

In what follows, we consider a linear functional system of the form $R\,y = 0$ where $R \in D^{q \times p}$ and D is an Ore algebra of functional operators for which Gröbner bases exist for all monomial orders and can be computed by Buchberger's algorithm. This is not too restrictive as it allows us to handle linear systems of partial differential equations, differential time-delay systems, difference equations... Note that the fact that Gröbner bases exist and can be computed is crucial for our algorithms. Following an important idea developed in algebraic analysis, we systematically associate the finitely presented left D-module $M = D^{1 \times p}/(D^{1 \times p}\,R)$ with the linear functional system $R\,y = 0$. Let $M = D^{1 \times p}/(D^{1 \times p}\,R)$ and $M' = D^{1 \times p'}/(D^{1 \times p'}\,R')$ be two finitely presented left D-modules. The existence of a left D-homomorphism $f : M \longrightarrow M'$ is then equivalent to the existence of two matrices $P \in D^{p \times p'}$ and $Q \in D^{q \times q'}$ satisfying $R\,P = Q\,R'$. In particular, we have $f(\pi(\lambda)) = \pi'(\lambda\,P)$ for all $\lambda \in D^{1 \times p}$, where π (resp. π') denotes the canonical projection from $D^{1 \times p}$

[1] freely available at `http://perso.ensil.unilim.fr/~cluzeau/OreMorphisms/` with a library of examples

[2] soon available with a library of examples

[3] `http://wwwb.math.rwth-aachen.de/OreModules/`

(resp. $D^{1\times p'}$) to M (resp. M'). Such a left D-homomorphism is defined up to a homotopy equivalence. The abelian group $\hom_D(M, M')$ can be written as

$$\hom_D(M, M') = E/(D^{p\times q'}\, R'),$$

where $E = \{P \in D^{p\times p'} \mid \exists\, Q \in D^{q\times q'} : \; R\,P = Q\,R'\}$. If $M' = M$, $\mathrm{end}_D(M)$ is then the quotient of the ring $E = \{P \in D^{p\times p} \mid \exists\, Q \in D^{q\times q} : R\,P = Q\,R\}$ by the two-sided ideal $D^{p\times q}\,R$, i.e., $\mathrm{end}_D(M)^{\mathrm{op}} \cong E/(D^{p\times q}\,R)$. Now, if D is a commutative ring, then $\hom_D(M, M')$ is a D-module and we can compute a family of generators with their relations whenever D is a noetherian ring. Using the Kronecker product $\otimes$, we can compute $\ker_D\left(.\begin{pmatrix} R^T \otimes I_{p'} \\ -I_q \otimes R' \end{pmatrix}\right)$ and we get a family $\{P_1, \ldots, P_r\}$ of generators of E. Then, we can reduce the rows of the P_i's with respect to a Gröbner basis of the rows of R' to get a family of generators $\{f_1, \ldots, f_r\}$ of $\hom_D(M, M')$. Using another syzygy computation, we can also compute the D-linear relations between generators $\sum_{j=1}^r X_{ij}\, f_j = 0$, $i = 1, \ldots, s$. In the case where $M = M'$, the table of multiplication of the generators f_j's, namely, $f_j \circ f_k = \sum_{l=1}^r \gamma_{jkl}\, f_l$, for j, $k = 1, \ldots, r$, can also be obtained. If we denote by $D\langle F_1, \ldots, F_r\rangle$ the free associated algebra generated by the symbols F_i's, then $\mathrm{end}_D(M) = D\langle F_1, \ldots, F_r\rangle/I$, where I is the following two-sided ideal:

$$I = \left\langle \sum_{j=1}^r X_{ij}\, F_j,\; i = 1, \ldots, s,\; F_j \circ F_k - \sum_{l=1}^r \gamma_{jkl}\, F_l,\; i, j = 1, \ldots, r \right\rangle.$$

If D is a non-commutative ring, then $\hom_D(M, M')$ is an abelian group and generally an infinite-dimensional k-vector space when D is a k-algebra. In this case, we can only find a k-basis of homomorphisms with fixed degrees in x_i and in ∂_j.

In a second part, we consider the factorization problem. If $f \in \hom_D(M, M')$, then we show that $\ker f = (D^{1\times t}\, S)/(D^{1\times q}\, R)$ where $S \in D^{t\times p}$ is defined by $\ker_D\left(.\begin{pmatrix} P \\ R' \end{pmatrix}\right) = D^{1\times t}\,(S \quad -T)$. Since $D^{1\times q}\,(R \quad -Q) \in \ker_D\left(.\begin{pmatrix} P \\ R' \end{pmatrix}\right)$, there exists $L \in D^{q\times t}$ such that $R = L\,S$. Hence, this method yields a non-trivial factorization of the matrix R when f is not injective.

In the third part of the talk, we consider the reduction problem. We show the following result: if $R \in D^{q\times p}$, $M = D^{1\times p}/(D^{1\times q}\, R)$ and $f \in \mathrm{end}_D(M)$ is defined by two matrices $P \in D^{p\times p}$ and $Q \in D^{q\times q}$ satisfying $R\,P = Q\,R$ and if the left D-modules $\ker_D(.P)$, $\mathrm{coim}_D(.P)$, $\ker_D(.Q)$, $\mathrm{coim}_D(.Q)$ are free, then there exist two matrices $U \in \mathrm{GL}_p(D)$ and $V \in \mathrm{GL}_q(D)$ such that the matrix $\overline{R} = V\,R\,U^{-1}$ is block-triangular. The matrices U and V can be obtained by means of basis computation of free modules which can be achieved by means of the packages OreModules[4], QuillenSuslin[5] and Stafford[6].

We then study the decomposition problem. To do that, we first need to search for idempotents of the endomorphism ring $\mathrm{end}_D(M)$ of M. A left D-endomorphism

[4] freely available at `http://wwwb.math.rwth-aachen.de/OreModules/index.html`

[5] `http://wwwb.math.rwth-aachen.de/QuillenSuslin/`

[6] freely available at `http://wwwb.math.rwth-aachen.de/OreModules/index.html`

f of $M = D^{1\times p}/(D^{1\times q}\, R)$, defined by the matrices $P \in D^{p\times p}$ and $Q \in D^{q\times q}$, is an idempotent, namely $f^2 = f$, if and only if there exist $Z \in D^{p\times q}$ and $Z' \in D^{q\times u}$ such that $P^2 = P + Z\, R$ and $Q^2 = Q + R\, Z + Z'\, R_2$, where $R_2 \in D^{t\times q}$ is such that $\ker_D(.R) = D^{1\times u}\, R_2$. Consequently, we can try to compute idempotents of $\mathrm{end}_D(M)$ when a family of endomorphisms of M is known. Idempotents are then used to decompose the solution space $\ker_{\mathcal{F}}(R.) = \{\eta \in \mathcal{F}^p \mid R\,\eta = 0\}$, where $\mathcal{F}$ is a left D-module. Let $f \in \mathrm{end}_D(M)$ be an idempotent defined by $P \in D^{p\times p}$ and $Q \in D^{q\times q}$, $\mathrm{coim} f = D^{1\times p}/(D^{1\times r}\, S)$, $R = L\, S$, $I_p - P = X\, S$ and $\ker_D(.S) = D^{1\times r_2}\, S_2$. Then, we have the decomposition of the solution space $\ker_{\mathcal{F}}(R.) = \ker_{\mathcal{F}}(S.) \oplus X\, \ker_{\mathcal{F}}((L^T \quad S_2^T)^T.)$. Furthermore, if the matrices P and Q satisfy the condition $P^2 = P$ and $Q^2 = Q$ and if the left D-modules $\ker_D(.P)$, $\mathrm{im}_D(.P)$, $\ker_D(.Q)$ and $\mathrm{im}_D(.Q)$ are free, then there exist two unimodular matrices $U \in \mathrm{GL}_p(D)$ and $V \in \mathrm{GL}_q(D)$ such that $\overline{R} = V\, R\, U^{-1}$ is a block-diagonal matrix, i.e., of the form $\mathrm{diag}(R_{11}, R_{22})$. Once again U and V are obtained by computing bases of free modules. In the case of a full row rank matrix R, i.e., $\ker_D(.R) = 0$, a way to get idempotent elements of $\mathrm{end}_D(M)$ defined by idempotent matrices P and Q, i.e., $P^2 = P$ and $Q^2 = Q$, is to find solutions $\Lambda \in D^{p\times q}$ of the algebraic Riccatti equation $\Lambda\, R\, \Lambda + (P - I_p)\, \Lambda + \Lambda\, Q + Z = 0$ and to define $\overline{P} = P + \Lambda\, R$ and $\overline{Q} = Q + R\, \Lambda$ which then satisfy $R\, \overline{P} = \overline{Q}\, R$, $\overline{P}^2 = \overline{P}$ and $\overline{Q}^2 = \overline{Q}$.

The last part of the talk concerns Serre's reduction which aims at reducing the number of equations and unknowns of a linear functional system. First, we explain the following result: let $R \in D^{q\times p}$ be a full row rank matrix and $\Lambda \in D^q$ such that there exists $U \in \mathrm{GL}_{p+1}(D)$ satisfying $(R \quad -\Lambda)\, U = (I_q \quad 0)$. Then, we have $M = D^{1\times p}/(D^{1\times q}\, R) \cong D^{1\times(p+1-q)}/(D\, Q_2)$, where Q_2 is the row vector formed by the $p+1-q$ last elements of the last row of U. In particular, this implies that the linear system $R\, y = 0$ is equivalent to a sole equation $Q_2\, z = 0$. If D is either a principal left ideal domain or a commutative polynomial ring with coefficients in a field or the Weyl algebra $A_n(k)$ or $B_n(k)$ (k is a field of characteristic 0) and $p - q \geq 1$, then the existence of a right-inverse of $(R \quad -\Lambda)$ over D is equivalent to the existence of the matrix U. Moreover, if $\Lambda \in D^q$ admits a left-inverse and if the left D-module $\ker_D(.Q_1)$ is free, where $Q_1 \in D^{p\times(p+1-q)}$ is the sub-matrix of U located above Q_2 in U, then there exist $W \in \mathrm{GL}_p(D)$ and $V \in \mathrm{GL}_q(D)$ such that $V\, R\, W = \mathrm{diag}(I_{q-1}, Q_2)$. The talk ends with recent results. Let D be the Weyl algebra $A_n(k)$ or $B_n(k)$, where k is a field of characteristic 0, $R \in D^{q\times p}$ a full row rank matrix, $M = D^{1\times p}/(D^{1\times q}\, R)$ and $\mathrm{ext}^1_D(M, D) = D^q/(R\, D^p)$. If $\mathrm{ext}^1_D(M, D)$ is a holonomic right D-module and $p - q \geq 1$, then there exists $Q_2 \in D^{1\times(p+1-q)}$ such that $M \cong D^{1\times(p+1-q)}/(D\, Q_2)$. Furthermore, if $q \geq 3$, then there exist two unimodular matrices U and V such that $V\, R\, U = \mathrm{diag}(I_{q-1}, Q_2)$.

References

[1] M. S. Boudellioua, A. Quadrat, *Reduction of linear systems based on Serre's theorem*, Proceedings of the 18th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2008), Virginia Tech, Blacksburg, Virginia (USA), 2008.

[2] M. S. Boudellioua, A. Quadrat, *Serre's reduction of linear functional linear systems*, INRIA Report, to appear, 2009.

[3] T. Cluzeau, A. Quadrat, *Using morphism computations for factoring and decomposing general linear functional systems*, Proceedings of the 17th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2006), Kyoto (Japan), 2006,

[4] T. Cluzeau, A. Quadrat, *Factoring and decomposing a class of linear functional systems*, Linear Algebra Appl., **428** (2008), 324–381.

[5] T. Cluzeau, A. Quadrat, *On the algebraic simplification of linear functional systems*, Topics in Time-Delay Systems: Analysis, Algorithms and Control, LNCIS **388**, Springer, 2009, 167–178.

[6] T. Cluzeau, A. Quadrat, OreMorphisms*: A homological algebraic package for factoring, reducing and decomposing linear functional system*, Topics in Time-Delay Systems: Analysis, Algorithms and Control, LNCIS **388**, Springer, 2009, 179–196.

[7] T. Cluzeau, A. Quadrat, *Serre's reduction of linear partial differential systems based on holonomy,* INRIA Report, to appear, 2009.

Parametrizing linear systems

D. Robertz
(joint work with Frédéric Chyzak, Alban Quadrat)

Given a system of (homogeneous) linear equations, an adequate way to represent the space of solutions is as the image of an operator to be constructed from the equations. In case the equations have coefficients in a field, Gaussian elimination achieves this objective. If the system is underdetermined, then the corresponding Gauss-reduced matrix singles out some variables of the system as parameters and specifies how all other variables are expressed (linearly) in terms of the parameters. This procedure can be viewed as identifying the kernel of the linear map induced by the system matrix as the image of another linear map. In particular, every tuple of values assigned to the parameters yields a solution, i.e. the parameters are not subject to any constraints.

More generally, if the equations have coefficients in a ring, that is not necessarily a (skew-) field, the question arises whether it is still possible to construct an operator which is defined over the same ring and whose image equals the space of solutions. For instance, a system of (homogeneous) linear partial differential equations may be written as an equation whose left hand side is a matrix differential operator applied to the vector of unknown functions and whose right hand side is zero. Is it possible to *parametrize* the system, i.e. to construct another matrix differential operator whose image equals the kernel of the given one? In general, the answer is negative. This question, and even a generalized one for the context of nonlinear differential equations, is known as *Monge's problem*; we refer to [7, 25, 8] for historical details. Important applications abound, e.g. in control theory [13, 14, 15, 16, 24, 26].

Ore algebras [4] form a suitable class of (not necessarily commutative) rings to address the parametrization problem. Types of linear systems which can be effectively dealt with by choosing an appropriate ring in this class include, e.g., time-varying systems of ordinary differential equations, differential time-delay systems, underdetermined systems of partial differential equations, multidimensional discrete systems, multidimensional convolutional codes, and many others. An Ore algebra is a certain iterated skew polynomial extension of a field or a commutative polynomial algebra. If this field or algebra is a Noetherian domain, then those Ore algebras which are relevant for parametrizing linear systems of the above types are Noetherian, have (left and right) quotient division rings [11], and even admit a Buchberger algorithm to compute Gröbner bases of their one-sided ideals [1, 9]. Prominent examples of Ore algebras are e.g. Weyl algebras and algebras of shift operators.

The algebraic approach to the parametrization problem for a linear system $R\,y = 0$ which is defined over a (Noetherian) Ore algebra D, as developed in [2], is outlined as follows: To $R\,y = 0$, where $R \in D^{q \times p}$, corresponds the left D-module $M := D^{1 \times p}/D^{1 \times q}R$. Linear equations that are equivalent to $R\,y = 0$ give rise to the same module M up to isomorphism. The entries of the unknown vector y are assumed to be elements of a left D-module $\mathcal{F}$. It is easy to check that the set of solutions to $R\,y = 0$ and $\hom_D(M, \mathcal{F})$ are isomorphic vector spaces [10]. Depending on the properties of $\mathcal{F}$, the duality defined by $\hom_D(-, \mathcal{F})$ allows to a certain extent to characterize structural information about the solutions in $\mathcal{F}^p$ in terms of properties of M. Suitable choices for $\mathcal{F}$ are injective cogenerators for the category of left D-modules, cf. e.g. [12] and the references therein. For instance, formal or convergent power series, smooth functions, (tempered) distributions and Sato's hyperfunctions, all defined over appropriate real or complex domains Ω, are injective cogenerators for the module category over commutative polynomial algebras whose generators act by partial differentiation.

There is a one-to-one correspondence between the torsion elements of M and the left D-linear combinations of the entries of y which have a non-zero annihilator in D. Therefore, non-trivial torsion elements give rise to constraints for possible parameters for the solution space. In fact, parametrizability of the linear system is equivalent to the triviality of the torsion submodule $t(M)$ of M. If a parametrization exists, then the algorithm which determines $t(M)$ constructs a parametrization at the same time. Methods from homological algebra allow to describe a hierarchy of parametrizability in terms of vanishing of certain $\mathrm{ext}^i_D(N, D)$, where $N := D^{q \times 1}/RD^{p \times 1}$ is the Auslander transposed module. For instance, $\mathrm{ext}^1_D(N, D) \cong t(M)$ is trivial if and only if M is torsion-free, i.e. the system is parametrizable; $\mathrm{ext}^i_D(N, D) = \{0\}$ for $i \in \{1, 2\}$ if and only if M is reflexive, i.e. a parametrization of the system is again parametrizable, etc. The de Rham complex is a well-known example which satisfies these conditions, if the differential forms are defined on a domain for which Poincaré's lemma applies.

Whereas in the case of linear equations with coefficients in a field it is always achieved that the solution set is parametrized by an injective linear map, the possibility to find an injective parametrization is not given in general. In system theoretic applications, linear and also nonlinear systems of differential equations whose solution sets have injective parametrizations in terms of arbitrary functions are nowadays said to be *flat* [6]. In the framework described above, a linear system $R\,y = 0$ is flat if and only if M is free. An algorithm which computes bases of free modules over the Weyl algebras, when the ground field is of characteristic zero, has recently been obtained in [19, 21] based on Stafford's theorems (see also [5] for an implementation of the Quillen-Suslin theorem, which is relevant for computing bases of free modules over commutative polynomial algebras).

The methods developed in [2] have been implemented in the Maple package `OreModules` [3], which is available online together with a library of examples with origin in control theory and mathematical physics.

References

[1] F. Chyzak, *Fonctions holonomes en calcul formel*, PhD thesis, Ecole Polytechnique, France, 1998.

[2] F. Chyzak, A. Quadrat, D. Robertz, *Effective algorithms for parametrizing linear control systems over Ore algebras*, Applicable Algebra in Engineering, Communication and Computing, **16** (2005), 319–376.

[3] F. Chyzak, A. Quadrat, D. Robertz, *OreModules: A symbolic package for the study of multidimensional linear systems*, in J. Chiasson and J.-J. Loiseau, editors, Applications of Time-Delay Systems, LNCIS **352**, Springer, 2007, 233–264. Cf. also `wwwb.math.rwth-aachen.de/OreModules`.

[4] F. Chyzak and B. Salvy, *Non-commutative elimination in Ore algebras proves multivariate identities*, J. Symbolic Comput., **26** (1998), 187–227.

[5] A. Fabiańska, A. Quadrat, "Applications of the Quillen-Suslin theorem in multidimensional systems theory", in the book *Gröbner Bases in Control Theory and Signal Processing*, H. Park and G. Regensburger (Eds.), Radon Series on Computation and Applied Mathematics **3**, de Gruyter publisher, 2007, 23–106.

[6] M. Fliess, J. Lévine, P. Martin, P. Rouchon, *Flatness and defect of nonlinear systems: introductory theory and examples*, Int. J. Control, **61** (1995), 1327–1361.

[7] E. Goursat, *Sur une généralisation du problème de Monge*, Ann. Fac. Sci. Toulouse Sci. Math. Sci. Phys., **22** (1930), 249–295.

[8] M. Janet, *P. Zervos et le problème de Monge*, Bull. Sci. Math., **95** (1971), 15–26.

[9] H. Kredel, *Solvable Polynomial Rings*, Shaker-Verlag, Aachen, 1993.

[10] B. Malgrange, *Systèmes différentiels à coefficients constants*, Séminaire Bourbaki, **246** (1963), 1–11.

[11] J. C. McConnell, J. C. Robson, with the cooperation of L. W. Small, *Noncommutative Noetherian rings*, Graduate Studies in Mathematics **30**, American Mathematical Society, Providence, RI, revised edition, 2001.

[12] U. Oberst, *Multidimensional constant linear systems*, Acta Appl. Math., **20** (1990), 1–175.

[13] J.-F. Pommaret, *Partial Differential Control Theory*, Mathematics and its Applications, 530, Kluwer Academic Publishers Group, Dordrecht, 2001.

[14] J. F. Pommaret, A. Quadrat, *Algebraic analysis of linear multidimensional control systems*, IMA J. Math. Control Inform., **16** (1999), 275–297.

[15] J. F. Pommaret, A. Quadrat, *Localization and parametrization of linear multidimensional control systems*, Systems Control Lett., **37** (1999), 247–260.

[16] A. Quadrat, *Analyse algébrique des systèmes de contrôle linéaires multidimensionnels*, PhD thesis, Ecole Nationale des Ponts et Chaussées, France, 1999.

[17] A. Quadrat, D. Robertz, *Parametrizing all solutions of uncontrollable multidimensional linear systems*, Proceedings of the 16th IFAC World Congress, Prague (Czech Republic), 2005.

[18] A. Quadrat, D. Robertz, *On the blowing-up of stably free behaviours*, in Proceedings of the 44th IEEE Conference on Decision and Control and European Control Conference ECC 2005, Seville (Spain), 2005, 1541–1546.

[19] A. Quadrat, D. Robertz, *Constructive computation of flat outputs of a class of multidimensional linear systems with variable coefficients*, Proceedings of the 17th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2006), Kyoto (Japan), 2006, 583–595.

[20] A. Quadrat, D. Robertz, *On the Monge problem and multidimensional optimal control*, Proceedings of the 17th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2006), Kyoto (Japan), 2006, 596–605.

[21] A. Quadrat, D. Robertz, *Computation of bases of free modules over the Weyl algebras*, Journal of Symbolic Computation, **42** (2007), 1113–1141.

[22] A. Quadrat, D. Robertz, *Baer's extension problem for multidimensional linear systems*, Proceedings of the 18th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2008), Virginia Tech, Blacksburg, Virginia (USA), 2008.

[23] D. Robertz, *Formal Computational Methods for Control Theory*, PhD thesis, RWTH Aachen, Germany, 2006, available at `http://darwin.bth.rwth-aachen.de/opus/volltexte/2006/1586`.

[24] J. Wood, *Modules and behaviours in* nD *systems theory*, Multidimens. Systems Signal Process., **11** (2000), 11–48.

[25] P. Zervos, *Le problème de Monge*, Mémorial des Sciences Mathématiques, fasc. **LIII**, 1932.

[26] E. Zerz, *Topics in Multidimensional Linear Systems Theory*, Lecture Notes in Control and Information Sciences **256**, Springer, 2000.

Constructive problems (and solutions) in homological algebra

Julio Rubio

One of the fundamental problems in Constructive Homological Algebra is the essential asymmetry existing between the concepts of *kernel* and *image*:

- The property $x \in Ker(f)$ is decidable
  (if the test to zero is decidable in the target module, and the homomorphism f is computable).
- The property $y \in Im(f)$ is undecidable.

In order to overcome this difficulty several strategies can be considered. For instance, we can work with *constructive morphisms.* A *constructive morphism* is a couple (f, s_f) where $f : A \to B$ is a homomorphism of $\mathbb{Z}$-modules, and $s_f : B \to A$ is a (computable) set-theoretic function such that $f s_f f = f$.

This concept generalises smoothly to other more general situations, where two categories are involved. For instance, f = ring homomorphism and s_f = group homomorphism; or f = chain complex morphism and s_f = morphism of graded modules. It can also be generalised to *reasonable* rings R (instead of $\mathbb{Z}$). More concretely, if R is a ring where a procedure to solve systems of linear equations is known, then any matrix defining a morphism between two finite type free R-modules induces a constructive morphism. Let us finally stress that if (f, s_f) is a constructive morphism, then $(s_f|_{Im(f)}, Ker(f))$ defines a *generalized map* in Barakat's sense (see [1]).

The interest of this notion is that it allows us to replace algorithms by closed formula in most of the elementary properties in Homological Algebra. As an example, in the statement of the *Five Lemma*:

$$\begin{tikzcd}
\cdots \arrow[r] & A_1 \arrow[r, "f_1"] \arrow[d, "\alpha_1"] & A_2 \arrow[r, "f_2"] \arrow[d, "\alpha_2"] & A_3 \arrow[r, "f_3"] \arrow[d, "\alpha_3"] & A_4 \arrow[r, "f_4"] \arrow[d, "\alpha_4"] & A_5 \arrow[r] \arrow[d, "\alpha_5"] & \cdots \\
\cdots \arrow[r] & B_1 \arrow[r, "f_1'"] & B_2 \arrow[r, "f_2'"] & B_3 \arrow[r, "f_3'"] & B_4 \arrow[r, "f_4'"] & B_5 \arrow[r] & \cdots
\end{tikzcd}$$

if we require in addition that the two rows are *constructively exact*, and the α_1, α_2, α_4, α_5 are *constructive* isomorphisms, then it is the same for α_3, with an explicit inverse given by: $\alpha_3^{-1} := f_2\alpha_2^{-1}s_2'(1 - \alpha_3 s_3 \alpha_4^{-1} f_3') + s_3\alpha_4^{-1}f_3'$ (explicit diagram chasing).

The drawbacks of this notion is that we do not kown if, beyond the finitely presented case, there exist enough constructive morphisms (they do not compose) and, overall, that we consider it is not powerful enough to undertake *actual* constructive problems in classical Homological Algebra. For instance, in the textbook by Hilton-Stammbach [3]:

- In page 23, the proof that free implies projective is not constructive, since it uses preimages of general morphisms.
- In pages 31-32, the proof that over a principal ideal domain, injective is equivalent to divisible, uses Zorn's lemma.
- In pages 37-38, the existence of the *injective envelope* uses twice Zorn's lemma (once to ensure the existence of a *maximal* essential extension, and a second time to prove this essential extension is injective).
- In pages 107 and 330, Whitehead problem is tackled with very complicated mathematics, related to foundations.

Nevertheless, there is another alternative approach to constructive Homological Algebra (and there *constructive* morphisms still play a role).

- A different approach:
  - Instead of rendering constructive "classical" homological algebra ...
  - to refound with new definitions ...
  - and then to develop in parallel to the classical view (without *deciphering* it).
  - Thus: results will be constructive by definition.
- An example: Sergeraert's effective homology.
- A case study: homology of groups (joint work with Ana Romero).

Sergeraert's effective homology theory has been introduced in [5], and materially realized in the Kenzo computer algebra system (see [2]). The application of effective homology and Kenzo to the computation of homology of groups has been documented in [4].

- *Conclusions:*
  - Refounding allows obtaining many constructive results ...
  - but very likely it does not allow solving the "classical" problems in constructive homological algebra, since ...

  - these problems do not appear in the new setting
    (for instance, injective modules seem to play no role in effective homology).
- *Open Questions:*
  - To find new basic definitions
  - allowing both tackling the problems of constructive homological algebra and recovering essential algorithmic results.
  - For instance: from basics, to infer the *necessity* of the *Basic Pertubation Lemma.*

References

[1] M. Barakat, *Spectral filtrations via generalized morphims.* `http://arxiv.org/abs/0904.0240v2`

[2] X. Dousson, F. Sergeraert, Y. Siret, *The Kenzo program*, Institut Fourier, Grenoble, 1999. `http://www-fourier.ujf-grenoble.fr/~sergerar/Kenzo/`

[3] P. J. Hilton, U. Stammbach, *A course in Homological Algebra*, Springer, 1997.

[4] A. Romero, G. Ellis, J. Rubio, *Interoperating between Computer Algebra Systems: Computing Homology of Groups with Kenzo and GAP*, Proceedings ISSAC 2009, ACM Press, 2009, 303–310.

[5] F. Sergeraert, *The computability problem in Algebraic Topology*, Advances in Mathematics, **124** (1994), 1–29.

A constructive analysis of Northcott's "Finite Free Resolutions"

Thierry Coquand

1. Introduction

Northcott [3] presents in an elementary way some fundamental results on finite free resolutions. However, on can argue that some arguments are not yet as elementary as they could be, since they require localization at arbitrary minimal primes, or at arbitrary minimal primes. The goal of this talk was to present some results in the first 6 chapters of Northcott's book where one can make the treatment even more elementary. We make use of several results contained in the forthcoming book [2] of H. Lombardi and C. Quitté.

2. Euler characteristic and prime ideals

One of the first use of prime ideals in Northcott's book is for justifying the definition of the Euler characteristic. If we have two finite free resolutions of the same module M

$$0 \to F_n \to \cdots \to F_0 \to M \to 0 \quad 0 \to G_m \to \cdots \to G_0 \to M \to 0$$

then $\Sigma(-1)^i rk(F_i) = \Sigma(-1)^j rk(G_j)$. This is proved in [3] using localisation at an arbitrary prime ideal. One has to assume that the ring is not trivial.

What is proved is elementary (in the logical sense of the term, this is a first-order statement): for instance it says that if we have two resolutions

$$0 \to R^3 \to R^2 \to M \to 0 \quad 0 \to R \to M \to 0$$

then $1 = 0$ in R. It is thus quite surprising to have to go via the existence of prime ideals to establish such a result.

There is a general method, developed in the reference [2] on several examples, to eliminate such "generic" use of prime ideals. In this case, there is a direct elementary proof which uses a variation of Schanuel's Lemma (exercise 5.4 of [2]): if we have two resolutions

$$0 \to K \to F_{l-1} \to \cdots \to F_0 \to M \to 0 \;\; 0 \to L \to G_{l-1} \to \cdots \to G_0 \to M \to 0$$

then the sums $K \oplus G_{l-1} \oplus G_{l-3} \oplus \cdots \oplus F_{l-2} \oplus F_{l-4} \oplus \dots$ and $L \oplus F_{l-1} \oplus F_{l-3} \oplus \cdots \oplus G_{l-2} \oplus G_{l-4} \oplus \dots$ are isomorphic. We notice that this more elementary proof eliminates also the hypothesis that the ring is not trivial.

Another proof that uses localisation at an arbitrary prime ideal is the one of Theorem 18, Chapter 4, that a matrix M presents a projective module iff for all i, the ideal $\Delta_i(M)$ generated by the minors $i \times i$ of M is generated by an idempotent element. There is an elementary version of this proof in [2].

3. Regular sequence

One goal of Northcott is to eliminate Noetherian hypotheses. There are similar motivations from a constructive point of view, since the Noetherian hypothesis is a logically complex notion. (Several examples of Noetherian elimination are presented in [2].) A key example is given by the notion of regular sequence, since this notion is presented usually using the Regular Element Theorem (a regular finitely generated ideal contains a regular element) which is, according to Kaplansky "a result that is among the most useful in the theory of commutative ring". How to avoid this result then?

Northcott presents a solution (based on an idea of Hochster) which is in the spirit of Kronecker. The main idea is to replace an *ideal* $\langle a_0, \dots, a_n \rangle$ by a *polynomial* $a_0 + a_1x + \cdots + a_nx^n$ or $a_0x_0 + \cdots + a_nx_n$. This idea plays a fundametal role in Kronecker's divisor theory [1]. The Regular Element Theorem is then replaced by the following resuly, known as McCoy's Lemma, which has a direct elementary proof: if the ideal $\langle a_0, \dots, a_n \rangle$ is regular then the element $a_0 + a_1x + \cdots + a_nx^n$ is regular. This holds without Noetherian hypothesis, and show that we have access in general to a regular element in a regular ideal, provided we allow the introduction of indeterminates. Northcott [3] shows how to develop a suitable theory, which is both elementary and without Noetherian hypothesis, of regular sequence based on this idea with an associate notion of grade of an ideal (with a version of the usual Auslander-Buchsbaum Theorem, which has an elementary proof).

4. Minimal prime

The proof of existence of minimal prime ideal requires Zorn's Lemma. It is thus very surprising that this is used to prove results having an elementary statement. An example is provided by Vasconcellos' Theorem.

Theorem: *Let I be a finitely generated ideal $\langle a_1, \ldots, a_n \rangle$ which admits a finite free resolution*

$$0 \to F_p \to F_{p-1} \to \cdots \to F_0 \to I \to 0$$

Each F_i is of the form R^{n_i} and we define $\mathsf{Char}_R(I)$ to be $n_0 - n_1 + n_2 - \ldots$. Then

- *If $\mathsf{Char}_R(I) = 0$ then $I = 0$ in R*
- *If $\mathsf{Char}_R(I) = 1$ then I is regular*
- *If $\mathsf{Char}_R(I) > 1$ then $1 = 0$ in R*

This corresponds to Theorem 12 of Chapter 4 [3] and the first point is proved there with localization at arbitrary minimal prime over the ideal $(0 : I)$.

We can eliminate the use of minimal prime ideals and obtain the following elementary proof. We remark that the statement is clear if $p = 0$. We prove then the statement by induction on p and on n_p. We can assume $n_p > 0$ and $n_{p-1} > 0$. The map $F_p \to F_{p-1}$ can be seen as a $n_p \times n_{p-1}$ matrix and since this map is injective the first column of this matrix defines a regular ideal $\langle c_1, \ldots, c_m \rangle$ with $m = n_{p-1}$.

The main remark is then that on each $R[1/c_j]$ the resolution can be simplified replacing n_p and n_{p-1} by $n_p - 1$ and $n_{p-1} - 1$. In this way, the characteristic is unchanged, and we get the result by induction.

The same induction principle can be used to prove that if we have a finite free resolution of $\langle a_1, \ldots, a_n \rangle$ of Euler characteristic 1 then $a_1, \ldots, a_n$ have a greatest common divisor which is a regular element, which is proved in [3] using minimal primes.

References

[1] H. Edwards, *Divisor Theory*, Boston, MA: Birkhäuser, 1989.

[2] H. Lombardi, C. Quitté, *Algèbre Commutative. Méthodes constructives (Modules projectifs de type fini)*, to appear and available from the home page of Henri Lombardi, 2009.

[3] D. G. Northcott, *Finite Free Resolutions*, Cambridge Tracts in Mathematics, 1976.

Gel'fand-Kirillov dimension, Cohen-Macaulay property and Auslander regularity of non-commutative G-algebras

Viktor Levandovskyy

Introduction

Considering important applications like systems and control theory, special functions, D-modules and so on, one has to work with modules over non-commutative algebras. There, even such a basic invariant as a dimension of a module is not easy to define. Indeed there are several essentially different definitions like generalized Krull dimension, Gel'fand-Kirillov dimension, flat and filter dimensions and so on. However, analyzing most ubiquitous operator algebras, it is possible to derive a fairly big class of them, sharing many properties with the polynomial commutative rings. This class is called the class of Gröbner-ready (GR) algebras, the analogues of polynomial rings in n variables are shortly called G-algebras. Over these algebras Gel'fand-Kirillov dimension is algorithmically computable and hence can be used in algebraic analysis and computer algebra. In this report we show, that surprizingly, every G-algebra enjoys important Cohen-Macaulay (with respect to Gel'fand-Kirillov dimension) and Auslander regular properties, which have strong implications in applications. In what follows, we denote by $\mathbb{K}$ a field.

1. G-algebras

Definition 1. *Let A be a quotient of the free associative algebra $\mathbb{K}\langle x_1, \ldots, x_n\rangle$ by the two-sided ideal I, generated by the finite set $\{x_j x_i - c_{ij} x_i x_j - d_{ij}\}$ for all $1 \le i < j \le n$, where $c_{ij} \in \mathbb{K}^*$ and d_{ij} are polynomials in $x_1, \ldots, x_n$. Without lost of generality* [6] *we can assume that d_{ij} are given in terms of standard monomials $x_1^{a_1} \ldots x_n^{a_n}$. A is called a G–*algebra [7, 6], *if*

- *for all $1 \le i < j < k \le n$ the expression $c_{ik}c_{jk} \cdot d_{ij}x_k - x_k d_{ij} + c_{jk} \cdot x_j d_{ik} - c_{ij} \cdot d_{ik}x_j + d_{jk}x_i - c_{ij}c_{ik} \cdot x_i d_{jk}$ reduces to zero modulo I and*
- *there exists a monomial ordering $\prec$ on $\mathbb{K}[x_1, \ldots, x_n]$, such that for each $i < j$, such that $d_{ij} \neq 0$, $\mathrm{lm}(d_{ij}) \prec x_i x_j$. Here,* lm *stands for the classical notion of leading monomial of a polynomial from $\mathbb{K}[x_1, \ldots, x_n]$, cf.* [4].

We call an ordering on a G-algebra **admissible**, if it satisfies second condition of the definition. A G-algebra A is Noetherian integral domain [7], hence there exists its total two-sided ring of fractions $\mathrm{Quot}(A)$, which is a division ring (skew field). A GR-algebra is a factor algebra of a G-algebra modulo a two-sided ideal.

Notable, the category of GR-algebras is nice in computations. In particular, it is possible to compute Gröbner bases of one- and two-sided ideals and submodules of a free module, hence homological computations (syzygy modules, free resolutions, module homomorphisms etc.) are possible as well. There is a system Singular:Plural [10, 6], which has a powerful implementation of many important algorithms for objects over any GR-algebra.

2. Cohen-Macaulay property and Auslander regularity

The notion of *dimension function* on an algebra is technical and can be found in e. g. [9].

Definition 2. *Let A be an associative $\mathbb{K}$-algebra and M be a left A-module.*

1. *The **grade** of M is defined to be $j(M) = \min\{i \mid \operatorname{Ext}^i_A(M, A) \neq 0\}$, or $j(M) = \infty$, if no such i exists or $M = \{0\}$.*
2. *A satisfies the **Auslander condition**, if for every fin. gen. A -module M, for all $i \geq 0$ and for all submodules $N \subseteq \operatorname{Ext}^i_A(M, A)$ the inequality $j(N) \geq i$ holds.*
3. *A is called an **Auslander-Gorenstein (AG)** algebra, if it is left and right Noetherian and the Auslander condition holds.*
4. *A is called an **Auslander regular (AR)** algebra, if it is Auslander-Gorenstein with $\operatorname{gl.dim}(A) < \infty$.*
5. *A is called a **Cohen-Macaulay (CM)** algebra wrt dimension function d, if for every fin. gen. nonzero A–module M, $j(M) + d(M) = d(A) < \infty$.*

3. Gel'fand-Kirillov dimension and its properties

Let R be an associative $\mathbb{K}$-algebra with generators $x_1, \ldots, x_m$. Assuming that each x_i has degree 1, we define an increasing degree filtration on R by:

$$F_k := \{f \in R \mid \deg f \leq k\} \quad k \geq 0.$$

Then we have $F_0 = \mathbb{K}$, $F_1 = \mathbb{K} \oplus \bigoplus_{i=1}^m \mathbb{K}x_i$ and so on. Here $V = \bigoplus_{i=1}^m \mathbb{K}x_i$ is called a *generating subspace* for R.

For any finitely generated left R-module M, there exists a finite dimensional subspace $M_0 \subset M$ (called a generating subspace for M), such that $RM_0 = M$. An ascending filtration $\{F_n, n \geq 0\}$ on R induces an ascending filtration on M, defined by $\{H_n := F_n M_0, n \geq 0\}$.

Definition 3. *Let $\{F_n, n \geq 0\}$ and $\{H_n, n \geq 0\}$ be filtrations on R and M as before. The **Gel'fand–Kirillov dimension** of M is defined to be*

$$\operatorname{GK.dim}(M) \; = \; \limsup_{n\to\infty} \log_n(\dim H_n).$$

$$\textit{In particular,}\ \operatorname{GK.dim}(R) \; = \; \operatorname{GK.dim}({}_R R) \; = \; \limsup_{n\to\infty} \log_n(\dim F_n).$$

Indeed, $\operatorname{GK.dim}(M)$ is independent of the choice of a generating subspace.

Note, that the Gel'fand-Kirillov dimension of a division ring does not need to be 0, we give that fact below. By a convention $\operatorname{GK.dim} \mathbb{Q} = 0$.

Let $\deg x_i = 1$, consider a filtration V up to degree d. We have:

$$V_d = \{f \mid \deg f = d\}, \quad V^d = \{f \mid \deg f \leq d\}.$$

Lemma 1. *Let A be a $\mathbb{K}$-algebra with PBW basis $\{x^\alpha \mid \alpha \in \mathbb{N}^n\}$ such A is a domain and there is a standard filtration. Then* $\operatorname{GK.dim}(A) = n + \operatorname{GK.dim}(\mathbb{K})$.

Proof. $\dim_{\mathbb{K}} V_d = \binom{d+n-1}{n-1}, \dim_{\mathbb{K}} V^d = \binom{d+n}{n}$. Thus $\binom{d+n}{n} = \frac{(d+n)\dots(d+1)}{n!} = \frac{d^n}{n!} +$ l.o.t, so we have $\mathrm{GK.}\dim(A) = \limsup_{d\to\infty} \log_d \binom{d+n}{n} = n$. □

In particular, any G-algebra in n variables over a field $\mathbb{K}$ has dimension $n + \mathrm{GK.}\dim \mathbb{K}$.

Example 1. *Let $T = \mathbb{K}\langle x_1, \dots, x_n\rangle$ be the free associative algebra. Then*

$$\dim_{\mathbb{K}} V_d = n^d, \quad \dim_{\mathbb{K}} V^d = \frac{n^{d+1}-1}{n-1}.$$

Note, that $\frac{n^{d+1}-1}{n-1} > n^d$. Since

$$\log_d n^d = d \log_d n = \frac{d}{\log_n d} \to \infty,\, d \to \infty,$$

it follows that $\mathrm{GK.}\dim(T) = \infty$.

Now, let us describe numerous properties of the Gel'fand-Kirillov dimension. **Subalgebras**. Let R be a $\mathbb{K}$-algebra. Then

(1) if S is a $\mathbb{K}$-subalgebra of R or a homomorphic image, then:

$$\mathrm{GK.}\dim S \leq \mathrm{GK.}\dim R.$$

(2) $\mathrm{GK.}\dim R = \sup\{\mathrm{GK.}\dim S \mid S \subset R \text{ an affine } \mathbb{K}\text{-subalgebra }\}$.

(3) For an R-module N, one has $\mathrm{GK.}\dim N = \sup\{\mathrm{GK.}\dim{}_S M \mid S \subset R$ an affine $\mathbb{K}$-subalgebra and M is a finitely generated S-submodule of $N\}$.

Lemma 2 (Elimination)**.** *Let $S \subset R$ be a subalgebra and $I \subset R$ a left ideal, such that $I \cap S = 0$. Then* $\mathrm{GK.}\dim S \leq \mathrm{GK.}\dim R/I$.

Lemma 3. *Here we address the case of commutative algebra.*

(i) *Let R be a commutative affine $\mathbb{K}$-algebra. Then (by Noether normalization) $\exists S = \mathbb{K}[x_1, \dots, x_t] \subseteq R$ and R is finitely generated S-module. Then* $\mathrm{GK.}\dim R = \mathrm{Kr.}\dim S = t$.

(ii) *If R is an integral domain,* $\mathrm{GK.}\dim R = \mathrm{tr.}\deg_{\mathbb{K}} \mathrm{Quot}(R)$.

Lemma 4 (Localization)**.** *Let R be an algebra and S a multiplicatively closed set of central regular elements of R. Then* $\mathrm{GK.}\dim S^{-1}R = \mathrm{GK.}\dim R$. *In particular, for a $\mathbb{K}$-algebra R and $f \in R[x]^*$ one has* $\mathrm{GK.}\dim R[x]_f = \mathrm{GK.}\dim R + 1$.

In general $\mathrm{GK.}\dim S^{-1}R \geq \mathrm{GK.}\dim R$ and very little is known! L. Makar-Limanov proved, that $\mathrm{GK.}\dim \mathrm{Quot}(A_1) = \infty$, since one can embed the free associative algebra in two variables into $\mathrm{Quot}(A_1)$.

More facts, more commutative rings.

(1) Curiosity: $\mathrm{GK.}\dim(R) \in \{0,1\} \cup [2, +\infty)$.

(2) For any $\mathbb{K}$-algebra R, $\mathrm{GK.}\dim R[x] = \mathrm{GK.}\dim R + 1$.

(3) $\mathrm{GK.}\dim \mathbb{K}[x_1, \dots, x_n]_{\mathfrak{p}} = n$ for $\mathfrak{p}$ prime.

(4) $\mathrm{GK.}\dim \mathbb{K}[[x_1, \dots, x_n]] = \mathrm{GK.}\dim \mathbb{K}\{x_1, \dots, x_n\} = \infty$.

Exactness. Let R be an affine algebra with finite standard fin.-dim. filtration, such that $\operatorname{Gr} R$ (that is an associated graded algebra of R) is left Noetherian. Then GK. dim is exact on short exact sequences of fin. gen. left R-modules. That is,

$$0 \to L \to M \to N \to 0 \ \Leftrightarrow \ \text{GK.}\dim M = \sup\{\text{GK.}\dim L, \text{GK.}\dim N\}$$

3.1. **Algorithmic computation.** There is an algorithm by Gomez-Torrecillaz et al. [1], which computes Gel'fand-Kirillov dimension for finitely presented modules over G-algebras (over ground field $\mathbb{K}$), hence over GR-algebras as well. Since the computation of a Krull dimension over a commutative polynomial ring is algorithmic, the algorithm can be formulated as follows.

```
GKdim($F$);
Let $A$ be a $G$-algebra in variables $x_1, \dots, x_n$.
    ○ Input:   Left generating set $F = \{f_1, \dots, f_m\} \subset A^r$
    ○ Output: $k \in \mathbb{N}$, $k = \text{GK.}\dim(A^r/_A\langle F\rangle) - \text{GK.}\dim(\mathbb{K})$.
    • $G$ =LeftGröbnerBasis($F$) $= \{g_1, \dots, g_t\}$ ;
    • $L = \{\operatorname{lm}(g_i) = x^{\alpha_i} e_s \mid 1 \leq i \leq t\}$;
    • return $\text{Kr.}\dim(\mathbb{K}[x_1, \dots, x_n]^r/\langle L\rangle)$;
```

This algorithm has been implemented in a Singular [5] library `gkdim.lib` [8] as the function `GKdim`.

4. CM and AR properties for G-algebras

Theorem 1 (Björk, Ekström, 1989). *Let R be a $\mathbb{K}$-algebra.*

(1) *If R is AG resp. Auslander regular, then for any ring automorphism σ on R and any σ-derivation δ, the skew polynomial ring $R[x; \sigma, \delta]$ is also AG resp. Auslander regular.*

(2) *Suppose that filtration is Zariskian. If $\operatorname{Gr} R$ is AG resp. Auslander regular, then so is R.*

Theorem 2 (V. Artamonov, Gomez-Torrecillaz and Lobillo [3]).
The algebra $\mathbb{K}_Q[x_1^{\pm 1}, \dots, x_n^{\pm 1}, x_{n+1}, \dots, x_{n+m}]$ is Auslander-regular and Cohen-Macaulay. Here, $Q = (q_{ij}) \in Mat_{n+m \times n+m}(\mathbb{K})$, such that $q_{ij}q_{ji} = 1$ and the relations on the algebra are $x_j x_i = q_{ij} x_i x_j$, $\forall 1 \leq i, j \leq n$.

Let Λ be a left Noetherian $\mathbb{K}$-subalgebra of a $\mathbb{K}$-algebra R, let $s \in \mathbb{Z}_+$and let $q_{ji} \in \Lambda$ for $1 \leqslant i < j \leqslant s$.

Theorem 3 (Gomez-Torrecillaz and Lobillo, [3]). *Let R be a $\mathbb{K}$-algebra, satisfying the following condition:*
$\exists\, x_1, \dots, x_s \in R$, an admissible ordering $\preceq'$ on $\mathbb{N}^s$, and finite subsets $\Gamma_{ji}, \Gamma_k \subseteq \mathbb{N}^s$ for $1 \leqslant i < j \leqslant s, 1 \leqslant k \leqslant s$ with $\max_{\preceq'} \Gamma_{ji} \prec' \epsilon_i + \epsilon_j$ and $\max_{\preceq'} \Gamma_k \prec' \epsilon_k$ such that $\{x^\alpha \mid \alpha \in \mathbb{N}^s\}$ is a basis of R as a left Λ-module and $x_j x_i = q_{ji} x_i x_j + \sum_{\alpha \in \Gamma_{ji}} c_\alpha x^\alpha$ and for all $a \in \Lambda$, $x_k a = a^{(k)} x_k + \sum_{\alpha \in \Gamma_i} c_\alpha x^\alpha$.
Suppose, in addition, that

(1) *The scalars $q_{ji} \in \mathbb{K}^*$ and the endomorphisms $\sigma_i : \Lambda \to \Lambda$ are automorphisms.*

(2) *Λ is generated as an algebra by elements $z_1, \ldots, z_t$ such that the standard filtration Λ_n obtained by giving degree 1 to each z_i satisfies that $gr(\Lambda) = \oplus_{n\geqslant 0}\Lambda_n/\Lambda_{n-1}$ is a finitely presented and Noetherian $\mathbb{K}$-algebra.*

(3) *$\sigma_i(\Lambda_1) \subseteq \Lambda_1$, for $i = 1, \ldots, s$.*

(4) *either $gr(\Lambda)$ or $\Lambda[y_1; \sigma_1] \cdots [y_s; \sigma_s]$ is an Auslander-regular and Cohen-Macaulay algebra.*

Then R is an Auslander-regular and Cohen-Macaulay algebra.

Corollary 1. *Let A be a G-algebra in n variables. Then A is an Auslander-regular and Cohen-Macaulay algebra.*

5. Application of CM+AR in module theory

Let A be a Cohen-Macaulay $\mathbb{K}$-algebra of finite Gel'fand-Kirillov dimension. Moreover, let M be a finitely generated left A-module and N be a transposed module to M. That is, N is a right A-module, presented by the transposed matrix of the presentation matrix of M, cf. [2]. We follow the dictionary of module properties of [2] and come with the following proposition. Suppose that $\mathrm{Hom}_A(N, A) = 0$, that is $j(N) \geq 1$, what is equivalent to $\mathrm{GK.dim}(N) \leq \mathrm{GK.dim}(A) - 1$.

Proposition 1. *In the situation as above, the following characterizations hold:*

(1) *M contains a torsion submodule if and only if $\mathrm{Ext}^1_A(N, A) \neq 0$ if and only if $j(N) = 1$ if and only if $\mathrm{GK.dim}(N) = \mathrm{GK.dim}(A) - 1$.*

(2) *M is a torsion-free left A-module if and only if $\mathrm{Ext}^1_A(N, A) = 0$ if and only if $j(N) \geq 2$ if and only if $\mathrm{GK.dim}(N) \leq \mathrm{GK.dim}(A) - 2$.*

(3) *M is a reflexive left A-module if and only if $\mathrm{Ext}^1_A(N, A) = \mathrm{Ext}^2_A(N, A) = 0$ if and only if $j(N) \geq 3$ if and only if $\mathrm{GK.dim}(N) \leq \mathrm{GK.dim}(A) - 3$.*

and so on.

Hence, the study of properties of finitely generated module over a Cohen-Macaulay algebra with finite Gel'fand-Kirillov dimension in the case when

$$\mathrm{Hom}_A(N, A) = 0$$

(which appears quite often) reduces to just one dimension computation instead of explicit computation of numerous extension modules.

Some open problems include the study of Cohen-Macaulay properties of localized algebras, like operator algebras with rational coefficients and of factor algebras of Cohen-Macaulay algebras modulo a two-sided ideal. Since the global homological dimension of a Cohen-Macaulay algebra needs to be finite, an algorithm for finding or even bounding the global dimension or an algorithm, which finds out, that the global dimension is infinite, is of big importance. Unfortunately, this seems to be a very tough problem in general.

References

[1] J. Bueso, J. Gómez–Torrecillas, A. Verschoren, *Algorithmic methods in non-commutative algebra. Applications to quantum groups*, Kluwer Academic Publishers, 2003.

[2] F. Chyzak, A. Quadrat, D. Robertz, *Effective algorithms for parametrizing linear control systems over Ore algebras*, Applicable Algebra in Engineering, Communication and Computing, **16** (2005), 319–376.

[3] J. Gómez-Torrecillas, F .J. Lobillo, *Auslander-regular and Cohen-Macaulay quantum groups*, J. Algebr. Represent. Theory **7** (2004), 35–42.

[4] G.-M. Greuel, G. Pfister, with contributions by O. Bachmann, C. Lossen and H. Schönemann, *A SINGULAR Introduction to Commutative Algebra*, Springer, 2002.

[5] G.-M. Greuel, G. Pfister, H. Schönemann, SINGULAR *3.0. A Computer Algebra System for Polynomial Computations*, Centre for Computer Algebra, University of Kaiserslautern, 2005, `http://www.singular.uni-kl.de`.

[6] V. Levandovskyy, *Non-commutative Computer Algebra for polynomial algebras: Gröbner bases, applications and implementation*, Doctoral Thesis, Universität Kaiserslautern, 2005, `http://kluedo.ub.uni-kl.de/volltexte/2005/1883/`.

[7] V. Levandovskyy, H. Schönemann, *Plural — a computer algebra system for noncommutative polynomial algebras*, Proc. of the International Symposium on Symbolic and Algebraic Computation (ISSAC'03), ACM Press, 2003, 176 – 183, `http://doi.acm.org/10.1145/860854.860895`.

[8] F. J. Lobillo, C. Rabelo, *A* SINGULAR *3.0 library for calculating the Gelfand-Kirillov dimension of modules gkdim.lib*, 2004.

[9] J. C. McConnell, J. C. Robson, with the cooperation of L. W. Small, *Noncommutative Noetherian rings*, Graduate Studies in Mathematics **30**, Providence, RI: American Mathematical Society (AMS), 2001.

[10] G. -M. Greuel, V. Levandovskyy, H. Schönemann, PLURAL. *A* SINGULAR *3.0 Subsystem for Computations with Non–commutative Polynomial Algebras*, Centre for Computer Algebra, University of Kaiserslautern, 2006, `http://www.singular.uni-kl.de`.

Reporter: Alban Quadrat