Journal of Algebra 499 (2018) 103–110

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

An elementary proof of Wiebe's Theorem

Thierry Coquand *, Claire Tête

ARTICLE INFO

Article history:
Received 26 January 2017
Available online 14 December 2017
Communicated by Michel Broué

Keywords:
Free resolutions
Wiebe's Theorem
Regular sequences
Resultant

ABSTRACT

This note has three contributions. The first one is to give elementary proofs about finite free resolution using only the notion of latent regular element (regular element which may be obtained after addition of indeterminates) and no notion from homological algebra. The second contribution is to use this to provide a simple proof of Wiebe's Theorem, a fundamental result in the theory of resultants [5]. Finally the third contribution is to explain how to "automatically" prove results or obtain counter-examples about regular sequences of a given length. We obtain in this way a new example of a local ring with a regular sequence b_1, b_2 such that b_2, b_1 is not regular.

Introduction

The work [3] presents simplified proofs of several results of Northcott's book [8] *Finite Free Resolutions*, using a homological definition of grade in term of Koszul complexes, and, in particular, the long exact sequence associated to a short exact sequence of complexes. It is mentioned there that all the results could be proved using a characterization of Northcott's definition of grade, which relies on Hochster's notion of latent nonzero divisor. The goal of the first part of this note is to show how to obtain such a character-

* Corresponding author.
E-mail address: Thierry.Coquand@cse.gu.se (T. Coquand).

https://doi.org/10.1016/j.jalgebra.2017.12.003

ization (Theorem 9), simplifying significantly the development in [8]. We illustrate this claim in the second part of this note, using Theorem 9 to provide a simple and elementary proof of Wiebe's Theorem, a fundamental result in the theory of the resultant [5]. A corollary of Wiebe's Theorem is a result about regular sequences. The last part is a logical analysis of such results, where we explain how to find in an automatic way a proof of statements about a regular sequence, for a fixed given length of the sequence.

1. Regular sequences

Let R be a commutative ring. If I is an ideal of R we write $I^\perp$ the *annihilator* of I, ideal of all x in R such that $xa = 0$ for all a in I. We say that I is *regular* if, and only if, $I^\perp$ is the ideal 0. We say that an element a of R is regular if the ideal $\langle a\rangle$ is regular.

A sequence $a_1, \ldots, a_n$ is called a *regular sequence* if a_1 is regular, a_2 is regular modulo $\langle a_1\rangle$, and a_3 regular modulo $\langle a_1, a_2\rangle$, ...

The property for an element to be regular, or for an ideal $\langle a_1, \ldots, a_n\rangle$ to be regular, is *invariant* under addition of indeterminates[1]: it holds in R if, and only if, it holds in an extension $R[u_1, \ldots, u_m]$ obtained from R by adding indeterminates $u_1, \ldots, u_m$.

Lemma 1. *If a, b are regular and $ay = bx$ then x belongs to $\langle a\rangle$ if, and only if, y belongs to $\langle b\rangle$.*

Proof. Indeed we have $x = az$ if, and only if, $ay = baz = bx$ if, and only if, $y = bz$ since a and b are regular. □

Corollary 2. *If a, b are regular then a is regular modulo $\langle b\rangle$ if, and only if, b is regular modulo $\langle a\rangle$; in particular, in this case, (a, b) is a regular sequence if, and only if, (b, a) is a regular sequence.*

Lemma 3. *If a, b are two regular elements of an ideal I then I is regular modulo $\langle a\rangle$ if, and only if, I is regular modulo $\langle b\rangle$.*

Proof. We assume that I is regular modulo $\langle b\rangle$ and let x in R be such that $xI \subseteq \langle a\rangle$. In particular $bx = ay$ for some y. Hence $bxI = ayI \subseteq \langle ab\rangle$. Since a is regular this implies $yI \subseteq \langle b\rangle$ and so y is in $\langle b\rangle$. By Lemma 1, x is in $\langle a\rangle$. □

If $f = a_1 m_1 + \cdots + a_l m_l$ is a polynomial on some indeterminates $u_1, \ldots, u_p$, where $m_1, \ldots, m_l$ are distinct monomials, then we denote by $c(f) = \langle a_1, \ldots, a_l\rangle$ the ideal of R generated by the coefficients of f. A *Kronecker polynomial* of an ideal I is any polynomial f such that $c(f) = I$.

Theorem 4 *(McCoy). The ideal $c(f)$ is regular if, and only if, f is regular in $R[u_1, \ldots, u_p]$.*

[1] More generally, it is invariant under any *faithfully flat* extension of R [7].