Journal of Algebra 492 (2017) 52–56

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Noether Normalization theorem and dynamical Gröbner bases over Bezout domains of Krull dimension 1

Maroua Gamanda, Ihsen Yengui *

Département de Mathématiques, Faculté des Sciences de Sfax, Université de Sfax, 3000 Sfax, Tunisia

A R T I C L E   I N F O

Article history:
Received 11 February 2017
Available online 6 September 2017
Communicated by Michel Broué

MSC:
13Cxx
13Pxx
14Qxx

Keywords:
Noether Nomalization theorem
Monomial order
Dynamical Gröbner bases
Bezout domains
Prüfer domains

A B S T R A C T

We propose a new version of Noether normalization theorem over Bezout domains of Krull dimension one (the ring $\mathbb{Z}$ of integers as main example). We also show that one can avoid branching when computing dynamical Gröbner bases over a Bezout domain of Krull dimension one.

0. Introduction

We decided to write this paper after reading the nice short paper [1]. In that paper, Abhyankar and Kravitz offered a correction to *Commutative Algebra* [3] by Zariski and

* Corresponding author.
E-mail address: ihsen.yengui@fss.rnu.tn (I. Yengui).

http://dx.doi.org/10.1016/j.jalgebra.2017.09.002

Samuel by constructing two counterexamples for two erroneous theorems. Their first counterexample aroused our curiosity to have a "plausible" version of Noether normalization theorem over the integers (or, more generally, over a Bezout domain of Krull dimension one). Recall that Noether normalization theorem says that every finitely-generated $\mathbf{K}$-algebra over a field $\mathbf{K}$ is isomorphic with a module-finite extension of a polynomial ring $\mathbf{K}[z_1, \ldots, z_d]$. Note that Noether normalization theorem over an integral domain $\mathbf{A}$ given by Hochster in [5] is nothing but Noether normalization theorem over the quotient field $\mathbf{K}$ of $\mathbf{A}$ (it is immediate that, when normalizing in $\mathbf{K}$, we will make use of a finite number of denominators $c_1, \ldots, c_m \in \mathbf{A} \setminus \{0\}$ and, thus, we obtain a normalization in $\mathbf{A}[\frac{1}{c}]$ where $c = c_1 \cdots c_m$).

The second part to the paper is devoted to explain why when computing dynamical Gröbner bases (first introduced by the second author, see [4,9]) over $\mathbf{R}[X_1, \ldots, X_k]$, where $\mathbf{R}$ is a Bezout domain of Krull dimension 1, one can avoid branching.

1. Noether normalization over Bezout domains of Krull dimension 1

First, it is worth pointing out that, in this section, $\mathbb{Z}$ can be replaced by any Bezout domain of Krull dimension 1.

Definition 1. For $f \in \mathbb{Z}[X_1, \ldots, X_n] \setminus \{0\}$, we denote by $\mathrm{c}(f)$ the gcd of the nonzero coefficients of f. We convene that $\mathrm{c}(0) = 0$. If $\mathrm{c}(f) = 1$, we say that f is primitive.

For a finitely-generated ideal $I = \langle f_1, \ldots, f_s \rangle$ of $\mathbb{Z}[X_1, \ldots, X_n]$, we denote by

$$\mathrm{c}(I) := \gcd(\mathrm{c}(f_1), \ldots, \mathrm{c}(f_s)).$$

For a ring $\mathbf{A}$, we denote by $\mathbf{A}\langle X \rangle$ the localisation of the ring $\mathbf{A}[X]$ at monic polynomials. One can also define by induction the ring

$$\mathbf{A}\langle X_1, \ldots, X_n \rangle := (\mathbf{A}\langle X_1, \ldots, X_{n-1} \rangle)\langle X_n \rangle.$$

It is in fact the localisation of the multivariate polynomial ring $\mathbf{A}[X_1, \ldots, X_n]$ at the monoid

$$S_n = \{p \in \mathbf{A}[X_1, \ldots, X_n] \mid \mathrm{LC}(p) = 1\},$$

where $\mathrm{LC}(p)$ denotes the leading coefficient of p with respect to the lexicographic order on monomials with $X_1 < X_2 < \cdots < X_n$.

Recall that if $\mathbf{R}$ is a Bezout domain of Krull dimension 1, then so is $\mathbf{R}\langle X_1, \ldots, X_n \rangle$ (see [7, Theorem 17] for a constructive proof). In particular, $\mathbb{Z}\langle X_1, \ldots, X_n \rangle$ is a Bezout domain of Krull dimension 1. Note that $\mathbf{R}\langle X \rangle$ cannot be a Prüfer domain (and, thus, cannot be a Bezout domain) if the Krull dimension of $\mathbf{R}$ is greater than one [6, Theorem 3.8].

The following result is the cornerstone of the Noether Normalization theorem over the integers we propose.

Theorem 2. *Let $I = \langle f_1, \dots, f_s \rangle$ be a finitely-generated nonzero ideal of $\mathbb{Z}[X_1, \dots, X_n]$ and let us fix the lexicographic monomial order on $\mathbb{Z}[X_1, \dots, X_n]$ with $X_1 < X_2 < \cdots < X_n$. Then there exist $b \in \mathbb{Z} \setminus \{0\}$, $g, g_1, \dots, g_s \in \mathbb{Z}[X_1, \dots, X_n]$ such that g is primitive, $\langle g_1, \dots, g_s \rangle$ contains a polynomial f whose leading coefficient is 1 (and, thus, f becomes monic at X_n after a change of variables "à la Nagata"), and*

$$I = b\, g\, \langle g_1, \dots, g_s \rangle.$$

Proof. Denoting by $\Delta := \gcd(f_1, \dots, f_s)$ in $\mathbb{Q}[X_1, \dots, X_n]$, we have $I = \langle f_1, \dots, f_s \rangle = \langle \Delta\, h_1, \dots, \Delta\, h_s \rangle$ for some coprime polynomials $h_1, \dots, h_s \in \mathbb{Q}[X_1, \dots, X_n]$. Multiplying I by α for an appropriate $\alpha \in \mathbb{Z} \setminus \{0\}$, we may suppose that $\Delta, h_1, \dots, h_s \in \mathbb{Z}[X_1, \dots, X_n]$. Denoting by $a = \mathrm{c}(f)\, \mathrm{c}(\langle h_1 h_1, \dots, h_s \rangle) \in \mathbb{Z} \setminus \{0\}$, we have

$$\alpha\, I = a\, g\, \langle g_1, \dots, g_s \rangle,$$

where $g, g_1, \dots, g_s \in \mathbb{Z}[X_1, \dots, X_n]$, $\gcd(g_1, \dots, g_s) = 1$ in $\mathbb{Q}[X_1, \dots, X_n]$, g is primitive, and at least one of the g_i's (say g_{i_0}) is primitive.

As α divides all the coefficients of $a\, g\, g_{i_0}$ and $g\, g_{i_0}$ is primitive, we infer that $\alpha \mid a$, and, thus, there exists $b \in \mathbb{Z} \setminus \{0\}$ such that

$$I = b\, g\, \langle g_1, \dots, g_s \rangle.$$

Also, since $\gcd(g_1, \dots, g_s) = 1$ in $\mathbb{Q}[X_1, \dots, X_n]$ and g_{i_0} is primitive, we deduce that $\gcd(g_1, \dots, g_s) = 1$ in $\mathbb{Z}[X_1, \dots, X_n]$. As $\mathbb{Z}\langle X_1, \dots, X_n \rangle$ is a Bezout domain (here we use the fact that $\mathbb{Z}$ is a Bezout domain of Krull dimension one), denoting by $J = \langle g_1, \dots, g_s \rangle$, we infer that

$$J \cap S_n \neq \emptyset. \qquad \square$$

We are now in a position to give our version of Noether Normalization theorem over the integers.

Theorem 3. *Let $\mathbf{R} = \mathbb{Z}[\theta_1, \dots, \theta_n]$ be a domain, finitely-generated over $\mathbb{Z}$, and let d be the Krull dimension of $\mathbf{R}$. Then, there exist an integer $\delta \in [\![0, d]\!]$, a subring $\mathbf{A}$ of $\mathbf{R}$ which is isomorphic to $\mathbb{Z}[X_1, \dots, X_{d-\delta}]/\langle h \rangle$ for some nonconstant irreducible polynomial $h \in \mathbb{Z}[X_1, \dots, X_{d-\delta}]$, and $z_1, \dots, z_\delta \in \mathbf{R}$ algebraically independent over $\mathbf{A}$, such that $\mathbf{R}$ is module-finite over $\mathbf{A}[z_1, \dots, z_\delta]$.*

Proof. We proceed by induction on n. If $n = 0$ then $\mathbf{R} = \mathbb{Z}$. We may take $d = 1$, $\delta = 0$, $\mathbf{A} = \mathbb{Z}$, and $h = X_1$. Now suppose $n \geq 1$ and that we know the result for $\mathbb{Z}$-algebras generated by $n-1$ or fewer elements. If the θ_i's are algebraically independent over $\mathbb{Z}$ then we are done: we may take $d = n+1$, $\delta = n$, $\mathbf{A} = \mathbb{Z}$, $h = X_1$, and $z_i = \theta_i$ for $1 \leq i \leq n$. Therefore we may assume that $I := \{f \in \mathbb{Z}[X_1, \ldots, X_n] \mid f(\theta_1, \ldots, \theta_n) = 0\}$ is a nonzero ideal of $\mathbb{Z}[X_1, \ldots, X_n]$. By virtue of Theorem 2, fixing the lexicographic monomial order on $\mathbb{Z}[X_1, \ldots, X_n]$ with $X_1 < X_2 < \cdots < X_n$, there exist $b \in \mathbb{Z} \setminus \{0\}$, $g, g_1, \ldots, g_s \in \mathbb{Z}[X_1, \ldots, X_n]$ such that g is primitive, $\langle g_1, \ldots, g_s\rangle$ contains a polynomial f whose leading coefficient is 1, and

$$I = b\, g\, \langle g_1, \ldots, g_s\rangle.$$

As $\mathbf{R} = \mathbb{Z}[\theta_1, \ldots, \theta_n] \cong \mathbb{Z}[X_1, \ldots, X_n]/I$ is integral, the ideal I is prime, and necessarily either $I = \langle b\rangle$ with b a prime number, or $I = \langle g\rangle$ with g a nonconstant irreducible polynomial in $\mathbb{Z}[X_1, \ldots, X_n]$, or I contains a polynomial f whose leading coefficient is 1. The first case is impossible by definition of I. If the second case occurs, then we are done: we may take $d = n$, $\delta = 0$, $\mathbf{A} = \mathbf{R}$, and $h = g$.

Now, suppose that I contains a polynomial f whose leading coefficient is 1. By a change of variables "à la Nagata", we can suppose that I contains a monic polynomial at the variable X_n. Note that this change of variables amounts to choosing new generators $\theta'_1, \ldots, \theta'_n \in \mathbf{R}$ of $\mathbf{R}$ as $\mathbb{Z}$-algebra with

$$\theta'_1 = \theta_1 - \theta_n^N, \theta'_2 = \theta_2 - \theta_n^{N^2}, \ldots, \theta'_{n-1} = \theta_{n-1} - \theta_n^{N^{n-1}}, \theta'_n = \theta_n,$$

for some suitable $N \in \mathbb{N}$. As θ'_n is integral over $\mathbf{T} := \mathbb{Z}[\theta'_1, \ldots, \theta'_{n-1}]$, $\mathbf{R} = \mathbb{Z}[\theta'_1, \ldots, \theta'_n]$ is module-finite over $\mathbf{T}$. As $\mathbf{T}$ has $n-1$ generators over $\mathbb{Z}$, the desired result follows by the induction hypothesis. $\square$

Note that the first counterexample given in [1] corresponds to a polynomial ring over $\mathbb{Z}[\frac{1}{2}] \cong \mathbb{Z}[X]/\langle 2X-1\rangle$ and so it is covered by our Normalization Theorem 3.

2. Branching-free dynamical Gröbner bases over Bezout domains of Krull dimension 1

We propose in this section an important simplification of the dynamical method for the construction of dynamical Gröbner bases (see [4,9–11]) over a Bezout domain $\mathbf{R}$ of Krull dimension ≤ 1 (as examples $\mathbb{Z}$ and the ring of all algebraic integers; note that the last one in not a P.I.D). More precisely, we prove that, over any Bezout domain with Krull dimension ≤ 1, one can avoid branching when computing a dynamical Gröbner basis. Note that this is not possible for Prüfer domains of Krull dimension ≤ 1 which are not Bezout domains, or equivalently, which are not gcd-domains (for example, $\mathbb{Z}[\sqrt{-5}]$, see [4, 4. An example]). We suppose that the reader has a copy of [4] in hands. We start as if $\mathbf{R}$ were a valuation domain. Suppose that two incomparable (under division) elements a, b in $\mathbf{R}$ appear as leading coefficients, of f and g respectively, when computing an $S(f, g)$. A key fact is that writing $a = (a \wedge b)\, a'$, $b = (a \wedge b)\, b'$, with $a' \wedge b' = 1$, then

a divides b in $\mathbf{R}[\frac{1}{a'}]$, b divides a in $\mathbf{R}[\frac{1}{b'}]$, and the two multiplicative subsets $a'^{\mathbb{N}}$ and $b'^{\mathbb{N}}$ are comaximal as $1 \in \langle a', b' \rangle$. Then $\mathbf{R}$ splits into $\mathbf{R}[\frac{1}{a'}]$ and $\mathbf{R}[\frac{1}{b'}]$ (see [9, Example 2.2]). Denoting by $\mathrm{mdeg}(f) = \alpha$, $\mathrm{mdeg}(g) = \beta$, and $\gamma = (\gamma_1, \ldots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$ for each i, $S(f, g)$ is computed as follows:

In the ring $\mathbf{R}[\frac{1}{b'}]$: $S(f, g) = \frac{X^\gamma}{X^\alpha} f - \frac{a'}{b'} \frac{X^\gamma}{X^\beta} g =: S_1$.

In the ring $\mathbf{R}[\frac{1}{a'}]$: $S(f, g) = \frac{b'}{a'} \frac{X^\gamma}{X^\alpha} f - \frac{X^\gamma}{X^\beta} g =: S_2$.

But, denoting by $S := b' \frac{X^\gamma}{X^\alpha} f - a' \frac{X^\gamma}{X^\beta} g$, we have:

$$S = b' S_1 = a' S_2.$$

As S is associated (i.e., equal up to a unit) to S_1 in $\mathbf{R}[\frac{1}{b'}]$ and to S_2 in $\mathbf{R}[\frac{1}{a'}]$, S can replace both of S_1 and S_2, and, thus, there was no need to open the two branches $\mathbf{R}[\frac{1}{a'}]$ and $\mathbf{R}[\frac{1}{b'}]$ (for $\mathbf{R} = \mathbb{Z}$, we retrieve the same construction as in [2,8]).

Note that the hypothesis "$\mathbf{R}$ has Krull dimension ≤ 1" ensures the termination of Buchberger's algorithm [11].

References

[1] S.-S. Abhyankar, B. Kravitz, Two counterexamples in normalization, Proc. Amer. Math. Soc. 135 (2007) 3521–3523.
[2] W.-W. Adams, P. Loustaunau, An Introduction to Gröbner Bases, Grad. Stud. Math., vol. 3, American Mathematical Society, Providence, RI, 1994.
[3] O. Zariski, P. Samuel, Commutative Algebra, vol. I, Springer-Verlag, New York, 1960.
[4] A. Hadj Kacem, I. Yengui, Dynamical Gröbner bases over Dedekind rings, J. Algebra 324 (2010) 12–24.
[5] M. Hochster, Noether normalization and Hilbert's Nullstellensatz, http://www.math.lsa.umich.edu/~hochster/615W10/supNoeth.pdf.
[6] L.R. Le Riche, The ring $\mathbf{R}\langle X \rangle$, J. Algebra 67 (1980) 327–341.
[7] H. Lombardi, C. Quitté, I. Yengui, Hidden constructions in abstract algebra (6) The theorem of Maroscia, Brewer and Costa, J. Pure Appl. Algebra 212 (2008) 1575–1582.
[8] F. Pauer, Gröbner bases with coefficients in rings, J. Symbolic Comput. 42 (2007) 1003–1011.
[9] I. Yengui, Dynamical Gröbner bases, J. Algebra 301 (2006) 447–458.
[10] I. Yengui, Corrigendum to "Dynamical Gröbner bases" [J. Algebra 301 (2) (2006) 447–458] and to "Dynamical Gröbner bases over Dedekind rings" [J. Algebra 324 (1) (2010) 12–24], J. Algebra 339 (2011) 370–375.
[11] I. Yengui, The Gröbner ring conjecture in the lexicographic order case, Math. Z. 276 (2014) 261–265.