Journal of Symbolic Computation 68 (2015) 316–325

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Triangular systems and a generalization of primitive polynomials

Gerhard Angermüller

ARTICLE INFO

Article history:
Received 17 July 2013
Accepted 29 June 2014
Available online 20 September 2014

Keywords:
Polynomial system
Primitive polynomial
Regular chain
Saturation ideal
Triangular set

ABSTRACT

A well-known generalization of the notion of primitive polynomials over factorial domains to arbitrary commutative rings is analyzed and applied to triangular systems. In particular, we clarify when a triangular system generates its saturation ideal, thus correcting a criterion published first in 2008.

© 2014 Elsevier Ltd. All rights reserved.

0. Introduction

In the first part of this note we analyze a well-known generalization to arbitrary commutative rings of the notion of primitive polynomials over factorial domains. The defining condition for this generalization has been used in Sharma (1981) for investigating principal ideals in a polynomial ring over a domain, but e.g. the application of this definition to questions on triangular systems in Lemaire et al. (2011) or Li (2010) shows that its relevance is not restricted to domains. As for domains the situation has been thoroughly investigated in the past decades with equivalent conditions (see e.g. Tang, 1972, Arnold and Sheldon, 1975 or Anderson and Zafrullah, 2007) we do not rule out rings with zero-divisors, thus using a similar approach as in Lemaire et al. (2011) or Li (2010). The characterization we give in Theorem 1 shows that the generalized notion we use here is for domains equivalent to *super-primitive* polynomials (cf. Tang, 1972), so we use the name *s-primitive* and call s-primitive polynomials *super-primitive* if the leading coefficient is a non-zero-divisor.

Main subject of this note is the use of super-primitive polynomials connected with triangular systems of multivariate polynomials, in particular with their saturation ideal (see e.g. Aubry et al., 1999 or Wang, 2000 for a detailed access to these notions). Polynomials with leading coefficient a non-zero-divisor play a prominent role in regular triangular systems and thus are essential

E-mail address: gerhard.angermueller@googlemail.com.

http://dx.doi.org/10.1016/j.jsc.2014.09.022
0747-7171/© 2014 Elsevier Ltd. All rights reserved.

for algorithms describing the zero-sets of multivariate polynomials. In Lemaire et al. (2011) (called "weakly primitive") s-primitive polynomials are shown to be very useful in the context of regular triangular systems. But the assertions made in Lemaire et al. (2011), Theorem 4.4 and Li (2010), Thm. 2.5 are not correct as we can show by an example. In Theorem 3 we prove a criterion for a triangular system to generate its saturation ideal. Our approach in this paper to triangular systems is quite general, valid for arbitrary commutative rings.

The content is organized as follows: after having defined and shown first properties of s-primitive polynomials, we collect some basic (and well-known) results to prepare the proofs in the subsequent chapters. In Section 1, s- and super-primitive polynomials are characterized, in Section 2 these results are applied to ideals in a polynomial ring and in Section 3 to triangular systems.

Notation. The basic concepts of Commutative Algebra used in this note are contained e.g. in Atiyah and Macdonald (1969) or Kaplansky (1974). If R is a commutative ring and M an R-module, an element x of R is called a *zero-divisor on* M, if x annihilates some non-zero element of M. An ideal I of a commutative ring R *has grade* 1, if it contains a non-zero-divisor x of R such that I consists only of zero-divisors on R/xR. An element q of a commutative ring R is called *irreducible*, if it is non-zero, not a unit and has no proper factors other than units; q is called *prime*, if qR is a non-zero prime ideal of R. A domain R is called a *factorial domain* (or a *UFD*), if any non-zero non-unit element of R can be expressed as a finite product of prime elements. For a polynomial $f \in R[X]$, $\deg f$ denotes the degree of f, $c(f)$ the ideal of R generated by the coefficients of f and $l(f)$ the leading coefficient of f; in particular $\deg 0 = -1$, $c(0) = 0$ and $l(0) = 0$. If I is an ideal of R, we denote for any $f \in R[X]$ the canonical image of f in $R/I[X]$ by the same symbol f. As in Tang (1972), Arnold and Sheldon (1975) or Anderson and Zafrullah (2007), $f \in R[X]$ is called *primitive* if $c(f)$ is not contained in any proper principal ideal of R.

In the following R denotes a commutative ring with unit and $Q(R)$ the *total ring of fractions of* R, i.e. the localization of R with respect to the multiplicative set of non-zero-divisors of R.

Definition. A polynomial $f = a_0 + \ldots + a_n X^n \in R[X]$ with $a_n \neq 0$ is called *s-primitive* (*in* $R[X]$), if for any $b \in R$ such that $ba_i \in a_n R$ for each $i = 0, \ldots, n-1$, one has $b \in a_n R$. f is called *super-primitive* (*in* $R[X]$), if f is s-primitive and a_n is not a zero-divisor in R.

Proposition 0. *Let* $f = a_0 + \ldots + a_n X^n \in R[X]$ *with* $a_n \neq 0$.

a) *If R is a factorial domain, then f is super-primitive (resp. s-primitive, resp. primitive) iff* $\gcd(a_0, \ldots, a_n) = 1$.
b) *f is s-primitive if $c(f) = R$; in particular, any monic polynomial is super-primitive.*
c) *f is s-primitive if a_j is not a zero-divisor in $R/a_n R$ for some $j \in \{0, \ldots, n-1\}$.*
d) *If $n = 0$, then f is super-primitive (resp. s-primitive, resp. primitive) iff a_0 is a unit of R.*
e) *If $n = 1$, then f is s-primitive iff a_0 is not a zero-divisor in $R/a_1 R$.*
f) *Let $R = \prod_{i \in I} R_i$ be a direct product of commutative rings R_i and $a_0 = (a_{0i})_{i \in I}, \ldots, a_n = (a_{ni})_{i \in I} \in R$ such that $a_{ni} \neq 0$ for each $i \in I$. Then f is s-primitive (resp. super-primitive) in $R[X]$ iff for each $i \in I$ $f_i(X) := a_{0i} + \ldots + a_{ni} X^n \in R_i[X]$ is s-primitive (resp. super-primitive) in $R_i[X]$.*
g) *If f is super-primitive, then f is primitive.*

Proof. a) If f is not s-primitive, then there is a $b \in R$ such that $ba_i \in a_n R$ for $i = 0, \ldots, n-1$ but $b \notin a_n R$. Then $b \gcd(a_0, \ldots, a_n) = \gcd(ba_0, \ldots, ba_n) \in a_n R$ and thus a prime factor of a_n divides $\gcd(a_0, \ldots, a_n)$, i.e. $\gcd(a_0, \ldots, a_n) \neq 1$.

If $\gcd(a_0, \ldots, a_n) \neq 1$, put $b := a_n / \gcd(a_0, \ldots, a_n)$. Then $b \notin a_n R$, but $ba_i = a_n a_i / \gcd(a_0, \ldots, a_n) \in a_n R$ for $i = 0, \ldots, n-1$, showing that f is not s-primitive.

The other assertions follow immediately from the definitions.

b) For $i = 0, \ldots, n$ choose b_i such that $a_0 b_0 + \ldots + a_n b_n = 1$ and let $b \in R$ be such that $ba_i \in a_n R$ for $i = 0, \ldots, n-1$. Then $b = b(a_0 b_0 + \ldots + a_n b_n) = ba_0 b_0 + \ldots + ba_n b_n \in a_n R$.

c) Let $b \in R$ be such that $ba_i \in a_n R$ for $i = 0, \ldots, n-1$. As a_j is not a zero-divisor in $R/a_n R$ for some $j \in \{0, \ldots, n-1\}$, $b \in a_n R$.

Download English Version:

https://daneshyari.com/en/article/401765

Download Persian Version:

https://daneshyari.com/article/401765

Daneshyari.com