Available online at www.sciencedirect.com
SCIENCE DIRECT®

ELSEVIER

Journal of Symbolic Computation 39 (2005) 397–415

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Bezoutian and quotient ring structure

B. Mourrain

GALAAD, INRIA, BP 93, 06902 Sophia Antipolis, France

Received 16 September 2003; accepted 1 November 2004

Abstract

In this paper, we present different results related to bezoutian and residue theory. We consider, in particular, the problem of computing the structure of the quotient ring by an affine complete intersection, and an algorithm to obtain it, as conjectured in [Cardinal, J.-P., 1993. Dualité et algorithmes itératifs pour la résolution de systèmes polynomiaux. Ph.D. Thesis, Univ. de Rennes]. We analyze it in detail and prove the validity of the conjecture, for a modification of the initial method. Direct applications of the results in effective algebraic geometry are given.

Keywords: Bezoutian; Resultant; Residu; Quotient ring structure; Normal form; Multiplication matrix; Linear algebra; Polynomial system solving

1. Introduction

The bezoutian is a fundamental tool which, surprisingly, appears in many areas of constructive algebra.

It was introduced implicitly by E. Bézout (around 1756) and also studied by Euler, at the premise of resultant theory. Later on, this method was revisited and analyzed in detail by Cayley (1848), yielding an alternative approach to the well-known formulation of S. Sylvester for the resultant of two univariate polynomials. We also find the Bezoutian construction in the work of Dixon (1908) on resultants for bivariate polynomials.

E-mail address: mourrain@sophia.inria.fr.

0747-7171/$ - see front matter
doi:10.1016/j.jsc.2004.11.010

Indeed, the bezoutian plays a central role in elimination theory, as it can be observed in the work of Jouanolou (1991), where it is also named *Morley form*. It is involved in projective resultant constructions (Jouanolou, 1997; D'Andrea and Dickenstein, 2001) or toric resultants, Khetan (2002), and more recently in their generalization of resultants over parameterized varieties (Busé et al., 2000), or residual resultant (Busé et al., 2001; Busé, 2001). See also Kapur et al. (1994), Kapur and Saxena (1995), Kapur et al. (1996) and Kapur and Saxena (1997) for projection operators.

The bezoutian is naturally connected to the theory of residue, as we will see. In complex analysis, it appears explicitly in different contexts (eg. Griffiths and Harris, 1978, p. 657), involving the Cauchy formula and properness properties in order to obtain explicit representation formulae (Berenstein et al., 1993; Berenstein and Yger, 1991; Elkadi, 1993). This theory of residue has also an algebraic facet, which relies mainly on the works of Scheja and Storch (1975), and Kunz (1986), where the foundations of the algebraic theory of residues were settled. Some related works and algorithmic extensions were presented in Becker et al. (1996), Cardinal and Mourrain (1996) and Elkadi and Mourrain (1996). The algebraic approach of residue theory is also involved in works related to complexity analysis and polynomial representation formulae. See for instance Fitchas et al. (1993), Sabia and Solerno (1995), Krick and Pardo (1996), Giusti et al. (1996), Giusti et al. (1998), Krick et al. (2001), Cattani et al. (1996), Elkadi and Mourrain (2000), Mourrain (1996), Aizenberg and Kytmanov (1981) and Gonzalez-Vega (1997).

The problem we are concerned with in this paper is the computation of the structure of the quotient ring $\mathcal{A} = R/(f_1, \ldots, f_n)$ when $(f_1, \ldots, f_n)$ is an affine complete intersection. A new algorithm, contrasting with the classical Gröbner or triangular set approaches, was described in Cardinal (1993). It was conjectured that the matrices obtained at the end of this algorithm are the matrices of multiplication by the variables in a basis of $\mathcal{A}$. This was corroborated by the experimentations. Though this work induced an active focus of the community on the topic, the conjecture remained unsolved. The aim of the paper is to describe the problem and to specify it in detail, in order to give a positive answer to the conjecture, for a modification of the initial algorithm. We deduce some direct applications of this result in effective algebraic geometry.

The paper is organized as follows. In the next section, we give the definitions that are used through the paper. In Section 3, we recall the important algebraic properties of the bezoutian. In Section 4, we describe the algorithm, and in Section 5 we prove the conjecture under some hypothesis. In the last section, we give some direct applications.

2. Definitions

Let $\mathbb{K}$ be a field. Let $R = \mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[\boldsymbol{x}]$ be the ring of polynomials in the variables $\boldsymbol{x} = (x_1, \ldots, x_n)$ with coefficients in $\mathbb{K}$. By convention, we set $x_0 = 1$. For any $\alpha \in \mathbb{N}^n$, we denote by $\boldsymbol{x}^\alpha$ the monomial $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$. For any subset $\mathfrak{a}$ of R, we denote by $\langle \mathfrak{a} \rangle$ the vector space of R generated by $\mathfrak{a}$.

For any vector space $K \subset R$, we denote by K^+ the vector space $K^+ = K + x_1 K + \cdots + x_n K$. The notation $K^{[p]}$ means p iterations of the operator $+$, starting from K.