Giesbrecht, Mark

Factoring in skew-polynomial rings over finite fields. (English) Zbl 0941.68160

J. Symb. Comput. 26, No. 4, 463-486 (1998).

The author considers two factorization problems in skew-polynomial rings $\mathbb{F}[x;\sigma]$ where $\mathbb{F}$ is a finite field, $\sigma:\mathbb{F}\to\mathbb{F}$ is a field automorphism and multiplication is defined by $xa=\sigma(a)x$ for all $a\in\mathbb{F}$. The first problem is the problem of complete factorization in $\mathbb{F}[x;\sigma]$, that is to write a non-constant $f\in\mathbb{F}[x;\sigma]$ as a product of irreducible elements of $\mathbb{F}[x;\sigma]$. The second problem is the bi-factorization problem, namely to determine for a given non-constant $f\in\mathbb{F}[x;\sigma]$ and a given natural number s if there exist elements g, $h\in\mathbb{F}[x;\sigma]$ such that $f=gh$ and $\deg(h)=s$ and to compute such polynomials g and h in case of existence. The complete factorization problem is reduced to the problem of determining whether a finite-dimensional associative algebra $\mathfrak{A}$ possesses non-trivial zero-divisors, and if so, finding non-zero $x,y\in\mathfrak{A}$ such that $xy=0$. Here the author describes a new fast algorithm. The bi-factorization problem is reduced to the complete factorization problem. Detailed descriptions of all algorithms and estimations of their complexity are given. The results on factorizations in a ring $\mathbb{F}[x;\sigma]$ are applied on functional decompositions of a special class of (ordinary) polynomials $f\in\mathbb{F}[x]$ possessing "wild" decompositions.

Reviewer: Friedrich Schwarz (Paderborn)

MSC:

16Z05	Computational aspects of associative rings (general theory)
16S36	Ordinary and skew polynomial rings and semigroup rings
68W30	Symbolic computation and algebraic computation

Keywords:
skew-polynomial rings; factorization; functional decomposition

Full Text: DOI