Applications of Computer Algebra – ACA2018
Santiago de Compostela, June 18–22, 2018

Randomized Algorithms for Normal Basis in Characteristic Zero

Mark Giesbrecht[1], **Armin Jamshidpey**[1], **Éric Schost**[1]

For a finite Galois extension K/F with $G = \mathrm{Gal}(K/F)$, there exists an element $\alpha \in K$ such that its conjugates form an F-basis of K (as a vector space)[4, Theorem 6.13.1]. Having such a basis, which is known as normal basis, is useful for certain computational purposes.

There are efficient algorithms for constructing a normal basis in positive characteristics. For a deterministic algorithm see [1] and for randomized algorithms see [6] and [3]. In characteristic zero, deterministic algorithms are introduced in [2] and [5](for abelian extensions).

Our aim is to introduce randomized algorithms for constructing a normal basis in characteristic zero. We will present an algorithm for cyclic extensions and more generally abelian extensions. We also give a solution for Galois extensions with dihedral group as Galois group.

Keywords: Normal Basis, Cyclic Extension, Abelian Extension

References

[1] DANIEL AUGOT; PAUL CAMION, *Forme de Frobenius et vecteurs cycliques*. *C. R. Acad. Sci. Paris Sér. I Math.*, 318(2):183–188, 1994.

[2] KURT GIRSTMAIR, *An algorithm for the construction of a normal basis*. *J. Number Theory*, 78(1):36–45, 1999.

[3] ERICH KALTOFEN; VICTOR SHOUP. *Subquadratic-time factoring of polynomials over finite fields*. *Math. Comp.*, 67(223):1179–1197, 1998.

[4] SERGE LANG, *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[5] ALAIN POLI, *A deterministic construction for normal bases of abelian extensions*. *Comm. Algebra*, 22(12):4751–4757, 1994.

[6] JOACHIM VON ZUR GATHEN; MARK GIESBRECHT, *Constructing normal bases in finite fields*. *J. Symbolic Comput.*, 10(6):547–570, 1990.

[1]David R. Cheriton School of Computer Science
University of Waterloo
200 University Avenue West Waterloo, ON, Canada N2L 3G1
mwg@uwaterloo.ca
armin.jamshidpey@uwaterloo.ca
eschost@uwaterloo.ca