Algoritmos para la determinación de los homomorfismos de inmersión de Campos de Galois

Algorithms for determination of the immersion homomorp- hisms of Galois Fields

Oristela Cuellar Justiz

Evaristo J. Madarro Capó

Guillermo Sosa Gómez

Gonzalo Palencia Fernández

Pablo Freyre Arrozarena

Universidad de las Ciencias Informáticas. La Habana. Cuba.

Universidad de La Habana. Cuba.

Universidad de Guadalajara. Jalisco. México. Universidad Central de Las Villas. Villa Clara.Cuba.

Universidad de La Habana, La Habana, Cuba.

Resumen

Los homomorfismos entre estructuras algebraicas son de mucha utilidad tanto en la matemática, como en la ciencia de la computación. En particular, los homorfismos entre campos de Galois son utilizados en la criptografía, en los llamados esquemas de cifrado homomórfico Zhang and Yue (2013), y en la teoría de códigos, por ejemplo, en la denominada decodificación local Grigorescu et˜al. (2006). Por lo que puede ser necesario conocer cuáles son las funciones que constituyen homomorfismos entre campos de Galois. En este trabajo se propone un algoritmo para la determinación de los homomorfismos de inmersión que existen entre los campos $GF(p^n)$ y $GF(p^m)$ cuando $n \mid m$.

Palabras claves: Homomorfismo, Inmersión, Campos de Galois

Abstract

Homomorphisms between algebraic structures are very useful in both mathematics and computer science. In particular, homomorphisms between Galois Fields are used in Cryptography, in the called homomorphic encryption schemes Zhang and Yue (2013), and in coding theory, for example, in the so-called local decoding Grigorescu et˜al. (2006). So it may be necessary to know what functions are homomorphisms between Galois Fields. In this work an algorithm for determining embedding homomorphisms between the $GF(p^n)$ and $GF(p^m)$ fields is proposed, when $n|m$.

Keywords: Homomorphisms, Immersion, Galois Fields