GERANDO SUBCORPOS

Autor: Lucas Moraes Godoi[1] Orientador: Luiz Emílio Allem[2]

1 Licenciando em Matemática, Instituto de Matemática Pura e Aplicada - UFRGS
2 Professor da UFRGS no Instituto de Matemática Pura e Aplicada

Introdução

Este trabalho, originado a partir do artigo "Generating Subfields", de Mark van Hoeij, apresentará uma eficiente forma de gerar todos os subcorpos de um dado corpo de extensão finito e separável, a partir da interseção de um pequeno número de subcorpos.

Objetivos

Apresentar as definições e conceitos necessários para a demonstração do teorema, bem como exemplos aplicados.

Gerando Subcorpos

Dado um corpo de extensão K/k de grau n, estamos interessados em encontrar os subcorpos de K contendo k.
Seja K/k um corpo de extensão finito e separável de K sobre k de grau n, seja F um corpo contendo K, e $f = f_1 \ldots f_r$ fatoração de f sobre F, onde os $f_i \in F[x]$ são irredutíveis e mônicos, e $f_1 = x - \alpha$. Definimos os corpos $F_i := F[x]/< f_i >$, para $1 \leq i \leq r$. Denotamos elementos de K como $g(\alpha)$ onde g é um polinômio de grau $< n$, e definimos para $1 \leq i \leq r$ a aplicação

$$\phi_i : K \to F_i$$
$$g(\alpha) \longmapsto g(x) \bmod f_i$$

Segue que ϕ_1 é a aplicação id: $K \to F$, e definimos para $1 \leq i \leq r$:

$L_i := \text{Ker}\,(\phi_i - \text{id}) = \{g(\alpha) \in K$ tal que $g(x) \equiv g(\alpha) \bmod f_i\}$.

Os L_i são fechados sobre a multiplicação, e assim corpos, já que

$\phi_i(ab) = \phi_i(a)\,\phi_i(b), \forall a, b \in L_i$

Teorema

Se L é um subcorpo de K/k, então L é a interseção de L_i, $i \in I$, para algum $I \subseteq \{1, \ldots, r\}$.

Exemplo

Seja o polinômio $f(x) = x^{12} - 7$. Na sua fatoração no Maple®, encontramos $-(x^2 - \alpha x + \alpha^2)(x^2 + \alpha^2)(x^2 + \alpha x + \alpha^2)(x^4 - x^2\alpha^2 + \alpha^4)(x + \alpha)(-x + \alpha)$ onde α é raiz de f. Para obter L_3, verificamos que o resto da divisão de $h(x) := g(x) - g(\alpha)$ por $f_3 := x^2 + \alpha^2$ é

$(a_1 - \alpha^2 a_3 + \alpha^4 a_5 - \alpha^6 a_7 + \alpha^8 a_9 - \alpha^{10} a_{11})x - a_3\alpha^3 - a_5\alpha^5 - 2a_6\alpha^6 - a_7\alpha^7 - a_9\alpha^9 - 2a_{10}\alpha^{10} - a_{11}\alpha^{11} - a_1\alpha - 2a_2\alpha^2$, o que nos leva a um subcorpo de dimensão 3. A interseção de L_3 com L_6, onde $f_6 := x + \alpha$, deixa resto $(a_2 + \alpha^4 a_6 + \alpha^8 a_{10} - \alpha a_3 - \alpha^5 a_7 - \alpha^9 a_{11})x^2 + (a_1 - \alpha^2 a_3 + \alpha^4 a_5 - \alpha^6 a_7 + \alpha^8 a_9 - \alpha^{10} a_{11})x - 2a_3\alpha^3 - a_5\alpha^5 - a_6\alpha^5 - 2a_7\alpha^7 - a_9\alpha^9 - a_{10}\alpha^{10} - 2a_{11}\alpha^{11} - a_1\alpha - a_2\alpha^2$ nos leva a um subcorpo de dimensão 3.

Referências Bibliográficas

- LIDL, R., NIEDERREITER, H. **Finite Fields. Enciclopedia of Mathematics and Its Applications** Vol. 20. Cambridge, 1997.

- HERSTEIN, I. N. **Topics in Algebra**. 1964.

- GONÇALVES, A. **Introdução à Algebra**. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2001.

- ANDRADE, L. N. **Introdução à Computação Algébrica com o Maple**. Rio de Janeiro: SBM, 2004.