Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, Vol. 3, N. 1, 2015.
Trabalho apresentado no XXXV CNMAC, Natal-RN, 2014.

Uma nova representação para Subcorpos de uma dada Extensão de Corpos

Mark van Hoeij
Departament of Mathematics, Florida State University
Florida, EUA
E-mail: hoeij@math.fsu.edu

Jonas Szutkoski **Luis Emilio Allem** **Vilmar Trevisan**
UFRGS - Departamento de Matemática Pura e Aplicada
91509-900, Campus do Vale, Porto Alegre, RS
jonas.szutkoski@ufrgs.br emilio.allem@ufrgs.br trevisan@mat.ufrgs.br

RESUMO

Seja $k \subseteq K$ uma extensão finita e separável de corpos de grau n e fixe $\alpha \in K$ um elemento primitivo de K sobre k, isto é, $K = k(\alpha)$. Além disso, seja $f \in k[x]$ o polinômio minimal de α sobre k. Estamos interessados em calcular todos os corpos L tais que $k \subseteq L \subseteq K$.

Seja $\tilde{K}$ um corpo contendo K e seja $f = f_1 f_2 \cdots f_r$ a fatoração de f sobre $\tilde{K}[x]$, onde cada $f_i \in \tilde{K}[x]$ é um polinômio mônico e irredutível. Como f é o polinômio minimal de $\alpha \in K$, podemos supor que $f_1 = x - \alpha$. Defina o corpo $\tilde{K}_i = \tilde{K}[t]/\langle f_i(t)\rangle$, $1 \leq i \leq r$. Como $K = k(\alpha)$, podemos representar cada elemento de K como $g(\alpha)$, onde $g(x) \in k(x)$ possui grau menor que $n = deg(f)$. Defina a aplicação

$$\phi_i : K \to \tilde{K}_i, \quad g(\alpha) \mapsto g(x) \; mod \; f_i,$$

onde $id : K \to \tilde{K}_i$ é a aplicação identidade, e os conjuntos

$$L_i = \ker(\phi_i - id) = \{g(\alpha) \in K / g(x) \equiv g(\alpha) \; mod \; f_i\}, \;\; 1 \leq i \leq r. \tag{1}$$

Cada conjunto L_i é, na verdade, um subcorpo de K. Em [1], o seguinte resultado é mostrado,

Teorema 1. *Se L é um corpo tal que $k \subseteq L \subseteq K$, então*

$$L = \bigcap_{i \in I} L_i,$$

para certo conjunto $I \subseteq \{1, 2, \ldots, r\}$.

Portanto, todo subcorpo L tal que $k \subseteq L \subseteq K$ é a interseção de alguns L_i's. Além disso, como cada conjunto L_i é um subcorpo de K, segue que, para encontrarmos todos os subcorpos de K e que contém k, basta computar todas as interseções entre os conjuntos L_i. O conjunto $\{L_1, L_2, \ldots, L_r\}$ independe da escolha do corpo $\tilde{K}$ e os corpos L_i, $1 \leq i \leq r$ são chamados de *Subcorpos principais* da extensão $k \subseteq K$.

Em [1], também é mostrada uma forma inteligente de calcular todas essas interseções, evitando calcular interseções que já foram calculadas.

Como $K = k(\alpha) \cong k[t]/\langle f(t)\rangle$, segue que uma base para K, visto como espaço vetorial sobre k, é dada por $1, x, x^2, \ldots, x^{n-1} \; mod \; f$. Assim, para calcular os elementos de L_i na prática, podemos representar um elemento genérico g nesse subcorpo por

$$g = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} \tag{2}$$

DOI: 10.5540/03.2015.003.01.0308

e utilizar a condição $g(x) \equiv g(\alpha) \ mod \ f_i$, de (1), para encontrar condições sobre as constantes a_i's. A condição $g(x) \equiv g(\alpha) \ mod \ f_i$ gerará um sistema de equações lineares nas incógnitas $a_1, a_2, \ldots, a_{n-1}$. Assim, um elemento da forma (2) está em L_i se, e somente se, as incógnitas $a_1, a_2, \ldots, a_{n-1}$ satisfazem esse sistema linear. Ou seja, cada subcorpo L_i pode ser representado por um sistema linear, e a interseção de dois subcorpos pode ser calculado através da resolução de ambos os sistemas lineares associados a cada subcorpo simultaneamente.

Neste trabalho apresentamos uma nova forma de representar esses subcorpos. Seja $h_i = f \cdot f_i'/f_i$ e considere o conjunto $S = \{h_1, h_2, \ldots, h_r\}$. Uma partição do conjunto S é um conjunto $\{p_1, p_2, \ldots, p_k\}$ tal que cada p_i é um subconjunto de S, a união dos p_i's é S e $p_i \cap p_j = \emptyset$, para $i \neq j$.

Cada subcorpo L de K determina uma partição $P_L = \{p_1, p_2, \ldots, p_k\}$ de S tal que cada p_i é um subconjunto minimal de S, cuja soma de seus elementos está em $L[x]$. Se denotarmos por $P_{L_1}, P_{L_2}, \ldots, P_{L_r}$ as partições associadas aos subcorpos principais, então calcular a interseção de dois subcorpos L_i e L_j corresponde a calcular a menor partição P de S tal que P_{L_i} e P_{L_j} são refinamentos de P.

Dessa forma, quando a partição de cada subcorpo principal é conhecida, então toda árvore de subcorpos pode ser calculada rapidamente, calculando apenas refinamentos de partições, sem precisar resolver sistemas lineares que envolvem cálculos no próprio corpo. Este trabalho está em fase de desenvolvimento, e testes preliminares apontam que há de fato uma melhora em relação à abordagem anteorior para a representação dos subcorpos.

Palavras-chave: *Extensão de corpos, Subcorpos, Subcorpos Principais, Partições*

Referências

[1] M. van Hoeij, J. Klüners, A. Novocin, Generating Subfields *Journal of Symbolic Computation*, 52, (2013) 1-23.

