AULA

11

Separabilidade

META:

Conceituar extensões separáveis e mostrar que toda extensão separável e finitamente gerada é simples.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Determinar a separabilidade de extensões sobre corpos de característica zero.

Usar o teorema do elemento primitivo para determinar um elemento primitivo para certas extensões separáveis finitamente geradas.

PRÉ-REQUISITOS

As noções de extensão simples, extensões finitamente gerada e multiplicidade de raízes.

11.1 Introdução

Seja $f(x) \in F[x]$. Se α é raiz de $f(x)$, o teorema do fator aplicado sucessivamente nos permite escrever

$$f(x) = (x - \alpha)^r g(x)$$

com $g(x) \in F[x]$ e $g(\alpha) \neq 0$. O inteiro positivo r, assim determinado, é chamado de multiplicidade da raiz α. Uma raiz é dita simples se possui multiplicidade 1. Um polinômio $f(x) \in F[x]$ é dito separável se possui somente raízes simples em seu corpo de raízes. Deste modo, se $f(x)$ é separável de grau n então $f(x)$ possui n raízes distintas sobre $SF_F(f(x))$ e, portanto,

$$f(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$$

com $\alpha_1, \ldots, \alpha_n \in SF_F(f(x)$ $(c \in SF_F(f(x)))$ e $\alpha_i \neq \alpha_j$ se $i \neq j$.

Um elemento $\alpha \in K$, $K \supset F$, é dito separável sobre F se $m_{\alpha,F}(x)$ é separável.

Uma extensão $F \subset K$ é separável se todo elemento $u \in K$ é separável sobre F.

Separabilidade é crucial na teoria de Galois e está intrinsicamente relacionada à característica do corpo base da extensão. Por exemplo, toda extensão sobre um corpo de característica zero é separável. Subjacente à separabilidade de uma extensão finitamente gerada reside o pilar da teoria de Galois: o teorema do elemento primitivo. Ele garante que toda extensão separável finitamente gerada é simples.

11.2 Critério da derivada para separabilidade de polinômios

Usaremos a derivada de um polinômio para caracterizar a irredutibilidade de um polinômio. Felizmente, a derivada de um polinômio recai em uma operação estritamente algébrica e não precisaremos recorrer a nenhum conhecimento de análise matemática.

Definição 11.1. Dado $f(x) = a_n x^n + \cdots a_1 x + a_0 \in F[x]$ a derivada, $f'(x)$, de $f(x)$ é o polinômio

$$f'(x) = na_n x^{n-1} + \cdots + 2a_2 x + a_1.$$

OBS 11.1. Vale as seguintes propriedades:

i) $(f+g)'(x) = f'(x) + g'(x)$.

ii) $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$. (Regra de Leibniz)

Teorema 11.1. *$f(x) \in F[x]$ é separável $\Leftrightarrow$ $MDC(f, f') = 1$.* □

Corolário 11.1. *Toda extensão sobre um corpo de característica zero é separável.* □

11.3 O teorema do elemento primitivo

OBS 11.2. Ao longo desta seção, usaremos a notação $Z_L(f(x))$ para denotar o conjunto das raízes de um polinômio $f(x) \in F[x]$ sobre uma extensão L de F. Quando quisermos denotar o conjunto de todas as raízes omitiremos o L e escreveremos simplesmente $Z(f(x))$.

Eis o teorema:

separável e finitamente gerada $\Rightarrow$ simples.

Eis a prova:(indução no número de geradores, F infinito)
Suponha $K = F(u_1, \ldots, u_r)$ separável sobre F.

Caso $r = 1$**:** $K = F(u_1)$ já é simples e nada tem-se para provar.

Caso $r = 2$**:** Suponha $K = F(v, w)$ separável sobre F. Sejam $q(x) = m_{w,F}(x)$ e $p(x) = m_{v,F}(x)$ com graus n e m, respectivamente. Seja $L = SF_F(p(x)q(x))$ o corpo de raízes de $q(x)p(x)$. Por hipótese de separabilidade, $q(x)$ possui n raízes distintas $w = w_1, w_2, \ldots, w_n$ e $p(x)$, m raízes distintas $v = v_1, v_2, \ldots, v_m$. Em símbolos,

$$Z(q(x)) = \{w = w_1, w_2, \ldots, w_n\} \text{ com } w_i \neq w_j \text{ se } i \neq j$$

e

$$Z(p(x)) = \{v = v_1, v_2, \ldots, v_n\} \text{ com } v_i \neq v_j \text{ se } i \neq j.$$

Da infinitude de F, existe $c \in F$ tal que $c \neq \frac{v_i - v}{w - w_j}$, $1 \leq i \leq m$ e $1 < j \leq n$. Seja $u = v + cw$. Vamos mostrar que $K = F(u)$. Considere o polinômio $h(x) = p(u - cx) \in F(u)[x]$. Então, w é raiz de $h(x)$ desde que $u - cw = v$ e $p(v) = 0$. Se algum w_j, $j \neq 1$, é raiz de $h(x)$, então $h(w_j) = p(u - cw_j) = 0$. Logo, $u - cw_j \in \{v, v_2, \ldots, v_m\}$. Assim, $u - cw_j = v_i$ para algum i, $1 \leq i \leq m$, donde $v + cw - cw_j = v_i$. Daí, $c = \frac{v_i - v}{w - w_j}$ e isto contradiz a escolha de c. Portanto,

$$Z(q(x)) \cap Z(h(x)) = \{w\}$$

Então, $h(x), q(x) \in F(u)[x]$ e ambos têm w como raiz. Pela condição de polinômio mínimo, devemos ter $m_{w,F(u)}(x) | q(x)$ e $m_{w,F(u)}(x) | h(x)$. Assim,

$$Z(m_{w,F(u)}(x)) \subset Z(q(x)) \cap Z(h(x)) = \{w\}.$$

Deste modo, $w \in L$ é a única raiz de $m_{w,F(u)}(x)$. Mas, $m_{w,F(u)}(x)|q(x)$ e $q(x)$ separável implica $m_{w,F(u)}(x)$ separável. Logo, $m_{w,F(u)}(x) \in F(u)[x]$ é um polinômio mônico, separável com uma única raiz. Então, $m_{w,F(u)}(x) = x - c$ para algum $c \in F(u)$. Como $m_{w,F(u)}(w) = 0$, segue que $c = w$ e, portanto, $w \in F(u)$. Mas, $v = u - cw$ com $u, w \in F(u)$ implica $v \in F(u)$. Assim, $F(v, w) \subset F(u)$. Por outro lado, $u = v + cw \in F(v, w)$ implica $F(u) \subset F(v, w)$. Logo, $F(u) = F(v, w)$.

Caso geral: Seja $K = F(u_1, \ldots, u_r)$ separável sobre F. Temos $K = F(u_1, \ldots, u_{r-1})(u_r)$ com $F(u_1, \ldots, u_{r-1})$ separável sobre F. Por hipótese indutiva, $F(u_1, \ldots, u_{r-1}) = F(v)$ para algum $v \in F(u_1, \ldots, u_{r-1})$. Logo, $K = F(v, u_r)$ é separável sobre F. Pelo caso de dois geradores, $K = F(w)$, $w \in K$. □

11.4 Conclusão

Exibir um extensão como uma extensão simples não é uma tarefa fácil. Para extensões separáveis e finitamente geradas, o teorema do elemento primitivo não somente mostra que tais extensões são simples, mas torna este processo bem computacional. Por este motivo, o teorema do elemento primitivo é o resultado mais forte provado até o momento.

RESUMO

Separabilidade

$f(x)$ separável := $f(x)$ tem somente raízes simples.

α separável sobre $F := \alpha$ é algébrico sobre F e $m_{\alpha,F}(x)$ é separável.

$F \subset K$ separável := α é separável sobre F, $\forall \alpha \in K$.

Critério da derivada para separabilidade

$f(x) \in F[x]$ é separável $\Leftrightarrow$ MDC$(f, f') = 1$.

Toda extensão sobre um corpo de característica zero é separável.

Teorema do elemento primitivo

$K = F(\alpha_1, \ldots, \alpha_n)$ separável sobre $F \Rightarrow K = F(\theta)$ para algum $\theta \in K$.

Nota: O elemento θ como acima é chamado *elemento primitivo* da extensão.

PRÓXIMA AULA

Estudaremos a teoria de Galois propriamente dita. Veremos a parte básica da teoria. Começaremos por estudar o grupo de Galois de uma extensão e finalizaremos com a correspondência de Galois entre subgrupos do grupo de Galois e corpos intermediários. A parte não trivial estabelece a bijetividade em tal correspondência para extensões galoisianas (finita, normal e separável).

ATIVIDADES

ATIV. 11.1. Mostre as propriedades abaixo sobre a derivada de polinômios usando a definição de derivada dada no texto.

i) $(f+g)'(x) = f'(x) + g'(x)$.

ii) $(fg)'(x) = f'(x)g(x) + f(x)g'(x)$. (Regra de Leibniz)

ATIV. 11.2. Mostre que um polinômio $f(x) \in F[x]$ é separável $\Leftrightarrow$ MDC$(f, f') = 1$.

ATIV. 11.3. Mostre que toda extensão sobre um corpo de característica zero é separável.

ATIV. 11.4. Mostre que toda extensão finita sobre um corpo de característica zero é simples.

ATIV. 11.5. Mostre que todo polinômio separável com uma única raiz tem grau 1.

ATIV. 11.6. Determinar $\theta \in \mathbb{Q}(\alpha, \beta)$ de modo que $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$ para cada α e β dados.

1. $\alpha = \sqrt{2}$, $\beta = i$.
2. $\alpha = \sqrt{2}$, $\beta = \sqrt[3]{2}$.
3. $\alpha = \sqrt[3]{2}$, β é tal que $\beta^4 + 6\beta + 2 = 0$.

ATIV. 11.7. Determine θ tal que $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\theta)$.

LEITURA COMPLEMENTAR

GONÇALVES, Adilson, Introdução à álgebra, IMPA, Projeto Euclides, 5.ed., Rio de Janeiro, 2008.
HUNGERFORD, Thomas W., Abstract algebra: an introduction, Saunders College Publishing, 1990.