AULA

10

Corpo de raízes

META:

Conceituar corpo de raízes de um polinômio sobre um corpo, determinar sua existência e unicidade e caracterizá-lo por meio de extensões finitas e normais.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Determinar o corpo de raízes de alguns polinômios.

Reconhecer se uma dada extensão é normal.

PRÉ-REQUISITOS

As noções de extensão finita e finitamente gerada, o processo de adjunção de raízes e o teorema de extensão de isomorfismos para extensões simples.

10.1 Introdução

Seja $F \subset K$ uma extensão de corpos e $f(x) \in F[x]$ um polinômio não constante. Vimos, na aula 06, que o anel quociente $F[x]/I$, onde $I = (f(x))$, nos fornece um anel no qual o polinômio $f(x)$ possui uma raiz, a saber $\overline{x}$. No entanto, $F[x]/I$ pode não ser um corpo. Sabemos que $F[x]/I$ é corpo se e somente se o polinômio $f(x)$ é irredutível sobre $F[x]$. O procedimento exibido na seção 6.5, chamado adjunção de raízes, nos fornece um método para construirmos a menor extensão de F contendo todas as raízes de $f(x)$. Nesta aula, retomaremos este processo e mostraremos que o corpo, assim construído, é único a menos de um isomorfismo. Este corpo é, por definição, o corpo de raízes de $f(x)$ sobre F. Usaremos a notação $SF_F(f(x))$ para denotar o corpo de raízes de $f(x)$ sobre F. Assim, dado $f(x) \in k[x]$, uma extensão K de F é um corpo de raízes de $f(x)$ sobre F se K satisfaz as seguintes condições:

i) $f(x)$ decompõe-se em K, isto é, $f(x) = c(x-\alpha_1)\cdots(x-\alpha_r)$ para certos $\alpha_1 \ldots, \alpha_r \in K$.

ii) $K = F(\alpha_1, \ldots, \alpha_r)$.

A caracterização do corpo de raízes de um polinômio é dada por meio de uma noção bastante refinada em teoria dos corpos; a saber: normalidade. Mostraremos que uma extensão é um corpo de raízes de um polinômio se e somente se é finita e normal. Este será nosso grande resultado nesta aula e de extrema importância na teoria de Galois. Começaremos com alguns exemplos a fim de fixar idéias.

10.2 Exemplos

Exemplo 10.1. O corpo de raízes de $x^2 - 2$ sobre $\mathbb{Q}$ é o corpo $\mathbb{Q}(\sqrt{2})$, pois $\mathbb{Q}(x)/(x^2-2) \cong \mathbb{Q}(\sqrt{2})$ e $-\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

Exemplo 10.2. $SF_{\mathbb{R}}(x^2+1) = \mathbb{C}$ desde que $x^2+1 = (x-i)(x+i) \in \mathbb{C}[x]$ e $\mathbb{C} = \mathbb{R}(i)$. Mas, $SF_{\mathbb{Q}}(x^2+1) = \mathbb{Q}(i) \neq \mathbb{C}$.

Exemplo 10.3. $SF_{\mathbb{Q}}(x^4 - 7x^2 + 10) = SF_{\mathbb{Q}}((x^2-2)(x^2-5)) = \mathbb{Q}(\pm\sqrt{2}, \pm\sqrt{5}) = \mathbb{Q}(\sqrt{2}, \sqrt{5})$.

Exemplo 10.4. $SF_F(ax+b) = F$ desde que $ax + b = a(x + b/a)$ com $b/a \in F$.

10.3 Existência

Teorema 10.1. *Seja F um corpo e $f(x) \in F[x]$ um polinômio não constante de grau n. Então, existe um corpo de raízes de $f(x)$ sobre F, aqui denotado por $SF_F(f(x))$, tal que $[SF_F(f(x)) : F] \leq n!$.*

Prova: (indução em $\deg f(x) = n$). Se $\deg f(x) = 1$ então $f(x) = ax + b$ com $a, b \in F$, $a \neq 0$. Logo, $f(x) = a(x - (-b/a))$ com $-b/a \in F$. Como $F = F(-b/a)$ segue então que $F = SF_F(f(x))$ e $[F : F] = 1 \leq 1!$. O teorema é verificado para $n = 1$. Suponha $n > 1$ e o teorema verdadeiro para polinômios de grau $n-1$. Pelo uso da fatoração única em $F[x]$ seja $p(x)$ um fator irredutível de $f(x)$ em $F[x]$. Sabemos que o anel quociente

$$F[x]/(p(x)) = F[\alpha]$$

onde $\alpha = \overline{x}$ é um corpo ($(p(x))$ é ideal maximal) contendo F como subcorpo e α como uma raiz de $p(x)$. Desde que $p(x)$ divide $f(x)$ segue que α é também raiz de $f(x)$. Pelo teorema do fator, em $F[\alpha][x]$, tem-se

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

para algum $g(x) \in F[\alpha][x]$ de grau $n-1$. Além disso, da irredutibilidade de $p(x)$ segue que $m_{\alpha,F}(x) = p(x)$. Portanto,

$$[F[\alpha] : F] = \deg p(x) \leq n \quad (p(x)|f(x)).$$

Agora, deg $g(x) = n-1$. Por hipótese indutiva, existe $SF_{F[\alpha]}(g(x))$, o corpo de raízes de $g(x)$ sobre $F[\alpha]$, com

$$[SF_{F[\alpha]}(g(x)) : F[\alpha]] \leq (n-1)!$$

Por definição de corpo de raízes, temos

$$g(x) = c(x-\alpha_2)\cdots(x-\alpha_n), \quad \alpha_2, \ldots, \alpha_n \in SF_{F[\alpha]}(g(x)).$$

e

$$SF_{F[\alpha]}(g(x)) = F[\alpha](\alpha_2, \ldots, \alpha_n) = F(\alpha, \alpha_2, \ldots, \alpha_n)$$

Então,

$$f(x) = (x-\alpha)g(x) = c(x-\alpha)(x-\alpha_2)\cdots(x-\alpha_n) \in SF_{F[\alpha]}(g(x)).$$

com

$$SF_{F[\alpha]}(g(x)) = F[\alpha](\alpha_2, \ldots, \alpha_n) = F(\alpha, \alpha_2, \ldots, \alpha_n).$$

Logo, $SF_{F[\alpha]}(g(x)) = SF_F(f(x))$ e isto mostra a existência do corpo de raízes de $f(x)$ sobre F. Finalmente,

$$\begin{aligned} [SF_F(f(x)) : F] &= [SF_F(f(x)) : F[\alpha]].[F[\alpha] : F] \\ &= [SF_{F[\alpha]}(g(x)) : F[\alpha]].[F[\alpha] : F] \\ &\leq (n-1)!n = n! \end{aligned}$$

pois $[SF_{F[\alpha]}(g(x)) : F[\alpha]] \leq (n-1)!$ e $[F[\alpha] : F] \leq n$. $\square$

10.4 Unicidade

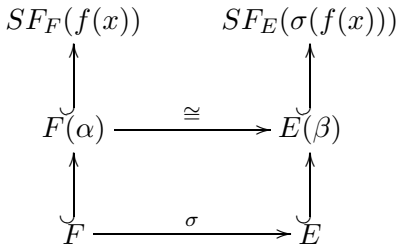
Teorema 10.2. *Seja $\sigma : F \to E$ um isomorfismo de corpos, $f(x) \in F[x]$ não constante, e $\sigma(f(x)) \in E[x]$. Então, σ estende-se à um isomorfismo $SF_F(f(x)) \cong SF_E(\sigma(f(x)))$.*

Prova: (indução no grau de $f(x)$) Se deg $f(x) = 1$, então $f(x) = ax+b$, $a, b \in F$ e $a \neq 0$. Logo, $f(x) = a(x-(-b/a))$ com $-b/a \in F$. Como $F[-b/a] = F$ segue, por definição de corpo de raízes, que $SF_F(f(x)) = F$.

Suponhamos deg $f(x) = n$ e o teorema verdadeiro para polinômios de grau $n-1$. Seja $p(x)$ um fator irredutível mônico de $f(x)$ em $F[x]$. O isomorfismo extensão $\sigma : F[x] \to E[x]$ leva $p(x)$ no polinômio irredutível mônico $\sigma(p(x))$. Toda raiz de $p(x)$ é também raiz de $f(x)$, pois $p(x)$ divide $f(x)$. Assim, $SF_F(f(x))$ contém todas as raízes de $p(x)$. Da mesma forma, $SF_E(\sigma(f(x))$ contém todas as raízes de $\sigma(p(x))$. Seja $\alpha \in SF_F(f(x))$ uma raiz de $p(x)$ e $\beta \in SF_E(\sigma(f(x)))$ uma raiz de $\sigma(p(x))$. Pelo teorema de extensão para extensões simples, σ estende-se à um isomorfismo

$$\tilde{\sigma} : F(\alpha) \to E(\beta)$$

no qual $\tilde{\sigma}(\alpha) = \beta$. Temos então o diagrama



Os elementos α e β são raízes de $f(x)$ e $\sigma(f(x))$. Pelo teorema do fator,

$$f(x) = (x-\alpha)g(x), g(x) \in F(\alpha)[x]$$

e

$$\sigma(f(x)) = \sigma(x-\alpha)\sigma(g(x)) = (x-\sigma(\alpha))\sigma(g(x)) = (x-\beta)\sigma(g(x)).$$

Em $SF_F(f(x))$ temos

$$f(x) = c(x-\alpha)(x-\alpha_2)\cdots(x-\alpha_n)$$

com $SF_F(f(x)) = F(\alpha, \alpha_2, \ldots, \alpha_n)$. Analogamente, em $SF_E(\sigma(f(x)))$, temos

$$\sigma(f(x)) = c'(x-\beta)(x-\beta_2)\cdots(x-\beta_n)$$

com $SF_E(\sigma(f(x))) = E(\beta, \beta_2, \ldots, \beta_n)$. Então,

$$c(x-\alpha)(x-\alpha_2)\cdots(x-\alpha_n) = (x-\alpha)g(x)$$

e

$$c'(x-\beta)(x-\beta_2)\cdots(x-\beta_n) = (x-\beta)\sigma(g(x)).$$

Donde,

$$g(x) = c(x-\alpha_2)\cdots(x-\alpha_n)$$

e

$$\sigma(g(x)) = c'(x-\beta_2)\cdots(x-\beta_n)$$

Então, por definição de corpo de raízes,

$$SF_{F(\alpha)}(g(x)) = F(\alpha)(\alpha_2, \ldots, \alpha_n) = F(\alpha, \alpha_2, \ldots, \alpha_n) = SF_F(f(x))$$

e

$$SF_{E(\beta)}(\sigma(g(x))) = E(\beta)(\beta_2, \ldots, \beta_n) = E(\beta, \beta_2, \ldots, \beta_n) = SF_E(\sigma(f(x))).$$

Desde que $g(x)$ tem grau $n-1$, a hipótese indutiva aplicada para $g(x)$ e $\sigma(g(x))$ sobre o isomorfismo $F(\alpha) \cong E(\beta)$ implica que tal isomorfismo estende-se à um isomorfismo $SF_F(f(x)) \cong SF_E(\sigma(f(x)))$. $\square$.

Corolário 10.1. *Dois corpos de raízes de um mesmo polinômio são isomorfos.*

Prova: Seja $f(x) \in F[x]$ um polinômio não constante e sejam K e L dois corpos de raízes de $f(x)$ sobre F. O teorema anterior aplicado ao isomorfismo identidade $I_F : F \to F$ mostra que existe um isomorfismo $K \cong L$ (extensão da identidade). $\square$

10.5 Corpo de raízes ⇔ finita e normal

Uma extensão de corpos $F \subset K$ é dita *normal* se

i) K é uma extensão algébrica de F; e

ii) todo polinômio $p(x) \in F[x]$, irredutível sobre F, que tem uma raiz $\alpha \in K$ possui todas as suas raízes em K.

Podemos dizer, então, que uma extensão $F \subset K$ é normal se e somente se K contém o corpo de raízes de todo polinômio irredutível sobre F que tem uma raiz em K. Sabemos que toda extensão finita é algébrica e finitamente gerada. Se K é uma extensão finita de um corpo F então existem $\alpha_1, \ldots, \alpha_r \in K$ tais que $K = F(\alpha_1, \ldots, \alpha_r)$. Sejam $p_i(x) \in F[x]$ o polinômio mínimo de cada α_i, $i = 1, \ldots, r$. Se, além disso, K é uma extensão normal de F então K contém todas as raízes de cada $p_i(x)$. Deste modo, se

$$\alpha_{1i} = \alpha_i, \alpha_{2i}, \ldots, \alpha_{n_i i} \in K$$

são todas as raízes de $p_i(x)$ então

$$\begin{aligned} K &= F(\alpha_1, \ldots, \alpha_r) \\ &= F(\alpha_{11}, \ldots, \alpha_{1n_1}, \ldots, \alpha_{1r}, \ldots, \alpha_{n_r r}) \\ &= SF_F(p_1 \cdots p_r). \end{aligned}$$

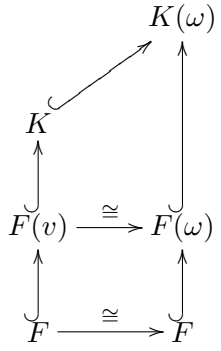
Assim, toda extensão normal e finita é o corpo de raízes de um polinômio. O resultado a seguir mostra que a recíproca é também verdadeira.

Teorema 10.3. *Um corpo K é um corpo de raízes sobre o corpo F de algum polinômio em $F[x]$ se e somente se K é uma extensão finita e normal de F.*

Prova: A condição necessária foi provada acima. Resta mostrar a condição suficiente. Suponha $K = SF_F(f(x))$, o corpo de raízes de um polinômio $f(x) \in F[x]$. Por definição de corpos de raízes:

$$K = F(\alpha_1, \ldots, \alpha_n)$$

onde $\alpha_1, \ldots, \alpha_n$ são todas as raízes de $f(x)$. Então, K é finita sobre F, pois toda extensão finitamente gerada por elementos algébricos é finita. Seja $p(x) \in F[x]$ um polinômio irredutível em $F[x]$ tendo uma raiz $v \in K$. Podemos supor $p(x)$ mônico. Sejam $L = SF_K(p(x))$ o corpo de raízes de $p(x)$ sobre K e $\omega \in L$ uma outra raíz de $p(x)$. Desde que $m_{v,F}(x) = p(x) = m_{\omega,F}(x)$ então o isomorfismo identidade em F estende-se à um isomorfismo $F(v) \cong F(\omega)$. Temos então, o seguinte diagrama:



Queremos mostrar que $K(\omega) = K$. Temos

$$\begin{aligned} K(\omega) &= F(\alpha_1, \ldots, \alpha_n)(\omega) \\ &= F(\alpha_1, \ldots, \alpha_n, \omega) \\ &= F(\omega)(\alpha_1, \ldots, \alpha_n) \\ &= SF_{F(\omega)}(f(x)). \end{aligned}$$

e

$$\begin{aligned} SF_{F(v)}(f(x)) &= F(v)(\alpha_1, \ldots, \alpha_n) \\ &= F(v, \alpha_1, \ldots, \alpha_n) \\ &= F(\alpha_1, \ldots, \alpha_n)(v) \\ &= K(v) = K. \end{aligned}$$

pois $v \in K$, por hipótese. Assim, K e $K(\omega)$ são corpos de raízes do mesmo polinômio $f(x)$ sobre corpos isomorfos. Pelo teorema da unicidade, o isomorfismo $F(v) \cong F(\omega)$ estende-se à um isomorfismo $K \cong K(\omega)$. Temos $[K : F] = [K(\omega) : F]$, pois espaços vetoriais isomorfos têm mesma dimensão. Logo, pela multiplicatividade dos graus:

$$[K : F] = [K(\omega) : F] = [K(\omega) : K][K : F]$$

donde $[K(\omega) : K] = 1$. Então, $K(\omega) = K$ e $\omega \in K$. Isto conclui a demonstração. $\square$.

OBS 10.1. A noção de corpo de raízes de um polinômio é fundamental na teoria dos corpos. Sabemos, ao menos teoricamente, que para todo polinômio existe um corpo no qual podemos determinar todas as suas raízes. A resposta afirmativa para a existência de corpos de raízes também nos fornece uma outra questão. Se para todo corpo F existe um corpo no qual todo polinômio não constante com coeficientes em F decompõe-se completamente. Em outras palavras, um corpo contendo os corpos de raízes de todos os polinômios não constantes com coeficientes em F. A resposta é afirmativa e a construção de um tal corpo é não trivial e está acima do nível deste curso. O corpo, assim determinado, é denotado por $\overline{F}$ e chamado de *fecho algébrico de* F. Assim como o corpo de raízes, o fecho algébrico de um corpo é único a menos de

isomorfismo. Um corpo K no qual todo polinômio não constante com coeficientes em K fatora-se completamente é chamado *corpo algebricamente fechado*. Pode-se mostrar que o fecho algébrico de um corpo é algebricamente fechado. O exemplo mais conhecido de um fecho algébrico é o corpo $\mathbb{C}$ dos complexos sobre $\mathbb{R}$. Este resultado ficou conhecido como teorema fundamental da álgebra. Ironicamente, não existe ainda uma prova completamente algébrica do teorema fundamental da álgebra. Obteremos neste curso, uma prova usando teoria de Galois e mínimos conhecimentos de análise. Para uma leitura mais detalhada sobre este assunto consultar os livros listados nas leituras complementares.

10.6 Conclusão

Corpo de raízes é um tipo de extensão algébrica finitamente gerada muito especial: os geradores compõem o conjunto das raízes de um polinômio. Esta peculiaridade a distingue de todas as outras extensões algébricas finitamente geradas. Embora tenham a mesma estrutura simples de um espaço vetorial de dimensão finita, o fato dos geradores serem todas as raízes de um polinômio confere aos corpos de raízes uma forte propriedade: normalidade.

RESUMO

DEFINIÇÃO

Dado $f(x) \in F[x]$, chama-se corpo de raízes de $f(x)$ sobre F ao menor corpo contendo F e todas as raízes de $f(x)$.

NOTAÇÃO:

$SF_F(f(x))$:= corpo de raízes de $f(x)$ sobre F.

OBSERVAÇÃO:

$SF_F(f(x)) := f(\alpha_1, \ldots, \alpha_n)$ com $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$.

EXISTÊNCIA:

Seja F um corpo e $f(x) \in F[x]$ um polinômio não constante de grau n. Então, existe um corpo de raízes de $f(x)$ sobre F.

UNICIDADE:

Dois corpos de raízes de um mesmo polinômio são isomorfos.

CARACTERIZAÇÃO:

$K = SF_F(f(x)) \Leftrightarrow K$ é uma extensão normal e finita do corpo F.

PRÓXIMA AULA

Estudaremos extensões separáveis. O principal resultado será o teorema do elemento primitivo, a saber: toda extensão separável finitamente gerada é simples.

ATIVIDADES

ATIV. 10.1. Mostre que $x^2 - 3$ e $x^2 - 2x - 2$ têm o mesmo corpo de raízes sobre $\mathbb{Q}$.

ATIV. 10.2. Determine $SF_{\mathbb{Q}}(x^4 - 3)$, $SF_{\mathbb{Q}}(x^-2)$ e $SF_{\mathbb{Q}}(x^7 - 5)$.

ATIV. 10.3. Seja $f(x) \in F[x]$ não constante. Mostre que se $[SF_F(f(x)) : F]$ é primo, $\theta \in SF_F(f(x))$ é uma raiz de $f(x)$, e $\theta \notin F$, então $SF_F(f(x)) = F(\theta)$.

ATIV. 10.4. Seja $f(x) \in F[x]$ não constante. Se E é um corpo tal que $F \subset E \subset SF_F(f(x))$ mostre que $K = SF_E(f(x))$.

ATIV. 10.5. Determine $SF_{\mathbb{Q}}(x^n - p)$, p primo. Determine também $[SF_{\mathbb{Q}}(x^n - p) : \mathbb{Q}]$.

LEITURA COMPLEMENTAR

DUMMIT, David S., FOOTE, Richard M. Abstract Algebra. John Wiley and Sons, 3.ed., USA, 2004.

GONÇALVES, Adilson, Introdução à álgebra, IMPA, Projeto Euclides, 5.ed., Rio de Janeiro, 2008.

HARDY, G. H., WRIGHT, E. M. An introduction to the theory of numbers. 4.ed., Oxford University Press, 1960.

HUNGERFORD, Thomas W., Abstract algebra: an introduction, Saunders College Publishing, 1990.

STEWART, Ian. Galois Theory, Chapman & Hall, 3.ed, 2004.