AULA 9

Extensões algébricas

META:

Determinar condições necessárias e/ou suficientes para caracterizar extensões algébricas.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Reconhecer se uma dada extensão é algébrica.

PRÉ-REQUISITOS

As seguintes definições sobre extensões: algébrica, finita, finitamente gerada.

9.1 Introdução

Para sua maior comodidade, seguem as definições usadas nesta aula.

O **Grau de uma extensão** $F \subset K$ é a dimensão de K como espaço vetorial sobre F. Notação: $[K : F]$.
Extensão finita := extensão de grau finito.

$F \subset K$ **é dita finitamente gerada** := existem $u_1, \ldots, u_r \in K$ tais que $K = F(u_1, \ldots, u_r)$.

$\alpha \in K$ é algébrico sobre F := existe $f(x) \in F[x]$, $f(x) \neq 0$, com $f(\alpha) = 0$.

$F \subset K$ algébrica := todo elemento de K é algébrico sobre F.

Todo corpo F é algébrico sobre si mesmo. De fato, para todo $\alpha \in F$, o polinômio $f(x) = x - \alpha \in F[x]$ é não nulo e tem α como raiz.
Esta aula é para relacionar os três tipos de extensões de corpos: finita, finitamente gerada e algébrica. A relação buscada aqui é de implicação, isto é, quem implica em quem. A implicação finita $\Rightarrow$ algébrica é a fundamental. Desta seguirão as outras. Por exemplo, finitamente gerada por elementos algébricos $\Rightarrow$ algébrica. A recíproca algébrica $\Rightarrow$ finita não vale em geral. O que vale é a equivalência algébrica + finitamente gerada $\Leftrightarrow$ finita.
Aproveitando o contexto do estudo de extensões algébricas, definiremos o fecho algébrico de um corpo F sobre um corpo K e mostraremos que o conjunto, assim considerado, admite a estrutura de corpo.

9.2 Finita $\Rightarrow$ algébrica

Seja K uma extensão finita de grau n. Por definição de grau, a dimensão de K como um espaço vetorial sobre F é n. O conjunto $1, \alpha, \alpha^2, \dots, \alpha^n$ tem $n+1$ elementos e, portanto, tem cardinalidade maior que a dimensão de K sobre F. Então é linearmente dependente. Por definição de dependência linear, existem $a_0, a_1, \dots, a_n \in F$, não todos nulos, tais que

$$a_0.1 + a_1.\alpha + \cdots a_n\alpha^n = 0.$$

Logo, $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$ é não nulo (por quê?) e tem α como raiz. Assim, todo elemento $\alpha \in K$ é algébrico sobre F. Por definição, K é algébrico sobre F.

Teorema 9.1. *Toda extensão finita é algébrica.* □

9.3 Finitamente gerada $\Rightarrow$ algébrica ?

Seja $F(\alpha_1, \dots, \alpha_r)$ uma extensão finitamente gerada de um corpo F. Se um dos α_i's é transcendente sobre F então $F(\alpha_1, \dots, \alpha_r)$ é infinita sobre F (por quê?). Assim, a implicação só tem sentido quando $\alpha_1, \dots, \alpha_r$ são algébricos sobre F. Neste caso, a resposta é afirmativa.

Teorema 9.2. *Se $K = F(\alpha_1, \dots, \alpha_r)$ é uma extensão finitamente gerada de F por elementos algébricos $\alpha_1, \dots, \alpha_r$, então K é uma extensão algébrica finita de F.*

Prova: Pela seção anterior basta provarmos a finitude. Usaremos indução em r. Se $r = 1$ então $K = F(\alpha_1)$ com α_1 algébrico sobre F. Então, $[F(\alpha_1 : F] = \deg\, m_{\alpha,F}(x)$, logo finita. Suponhamos toda extensão finitamente gerada por $r-1$ elementos algébricos sobre F finita e consideremos $K = F(\alpha_1, \ldots, \alpha_r)$ com $\alpha_1, \ldots, \alpha_r$ algébricos sobre F. Por hipótese indutiva, $F(\alpha_1, \ldots, \alpha_{r-1})$ é finita sobre F. Por outro lado, α_1 algébrico sobre F implica α_1 algébrico sobre $L = F(\alpha_1, \ldots, \alpha_{r-1})$. A extensão simples $L(\alpha_r) = \big(F(\alpha_1, \ldots, \alpha_{r-1})\big)(\alpha_r) = K$ é então finita sobre L. Temos então $F \subset L \subset K$ com K finita sobre L e L finita sobre F. Pela multiplicatividade dos graus, K é finita sobre F. $\square$

9.4 Finita $\Leftrightarrow$ finitamente gerada e algébrica

A seção anterior mostra que *finitamente gerada e algébica $\Rightarrow$ finita*. Esta seção trata da recíproca à esta implicação.

Teorema 9.3. *$F \subset K$ finita $\Leftrightarrow$ $F \subset K$ finitamente gerada e algébrica.*

Prova: A condição necessária foi provada na seção anterior. Resta provar a condição suficiente. Suponha $F \subset K$ finita de grau r. Sejam $\alpha_1, \ldots, \alpha_r$ uma base de K sobre F. Temos

$$F \subset F(\alpha_1, \ldots, \alpha_r) \subset K$$

com K finita sobre F. Então, $F \subset F(\alpha_1, \ldots, \alpha_r)$ é finita e vale a igualdade

$$[K : F] = [F(\alpha_1, \ldots, \alpha_r) : F][K : F(\alpha_1, \ldots, \alpha_r)]$$

donde

$$[K : F] = r \geq [F(\alpha_1, \ldots, \alpha_r) : F].$$

Mas, $\alpha_1, \ldots, \alpha_r \in F(\alpha_1, \ldots, \alpha_r)$ são linearmente independentes sobre F, logo

$$[F(\alpha_1, \ldots, \alpha_r) : F] \geq r = [K : F].$$

Assim, $[F(\alpha_1, \ldots, \alpha_r) : F] = r = [K : F]$. Logo,

$$r = r.[K : F(\alpha_1, \ldots, \alpha_r)]$$

donde $[K : F(\alpha_1, \ldots, \alpha_r)] = 1$ e, portanto, $K = F(\alpha_1, \ldots, \alpha_r)$. $\square$.

9.5 Transitividade

A noção de extensão algébrica é transitiva.

Teorema 9.4. *Se $F \subset K \subset L$ são extensões de corpos com L algébrica sobre K e K algébrica sobre F então L é algébrica sobre F.*

Prova: Seja $\alpha \in L$. Por hipótese, L é algébrico sobre K. Assim, α é algébrico sobre K. Por definição de elemento algébrico, existe um polinômio $f(x) = a_m x^m + \cdots + a_1 x + a_0 \in K[x]$, não nulo, tal que $f(\alpha) = a_m \alpha^m + \cdots + a_1 \alpha + a_0 = 0$, $a_i \in K$. Desde que $a_0, \ldots, a_m \in L = F(a_0, \ldots, a_m)$, α é algébrico sobre L. Assim, $F \subset L \subset L(\alpha)$ com $L(\alpha)$ finita sobre L. Mas, L é finitamente gerada sobre F por elementos algébricos. Pela seção anterior, L é finita sobre F. Pelo teorema da multiplicatividade dos graus, $L(\alpha)$ é finita sobre F. Pelo teorema 9.1, $L(\alpha)$ é algébrica sobre F donde α é algébrico sobre F. Desde que temos considerado $\alpha \in K$ arbitrário segue que K é algébrico sobre F. $\square$

9.6 O corpo dos elementos algébricos

Seja $F \subset K$ uma extensão de corpos. Denotemos por $\overline{F}_K$ o conjunto dos elementos de K algébricos sobre F. Temos $F \subset \overline{F}_K$, pois $F \subset K$ e todo elemento de F é algébrico sobre F. Se $\alpha, \beta \in \overline{F}_K$

então α e β são algébricos sobre F, por definição de $\overline{F}_K$. Então, $F \subset F(\alpha,\beta)$ é uma extensão algébrica. Como $F(\alpha,\beta)$ é corpo, temos $\alpha+\beta$, $\alpha.\beta$, $-\alpha$, $-\beta \in F(\alpha,\beta) \subset \overline{F}_K$. Do mesmo modo, se α é não nulo então $\alpha^{-1} \in F(\alpha,\beta) \subset \overline{F}_K$. Assim, $\overline{F}_K$ é fechado sob adição e multiplicação bem como sob inversos aditivos e multiplicativos. Logo, $\overline{F}_K$ é corpo. Este corpo é chamado de fecho algébrico de F em K ou relativo ao corpo K.

9.7 Algébrica $\not\Rightarrow$ Finita

Vamos conhecer agora um exemplo de uma extensão algébrica não finita. Considere a extensão $\mathbb{Q} \subset \mathbb{C}$ e seja $\overline{\mathbb{Q}}_{\mathbb{C}}$ o fecho algébrico dos racionais relativo aos complexos. Por definição, $\overline{\mathbb{Q}}_{\mathbb{C}}$ é o conjunto dos complexos algébricos sobre $\mathbb{Q}$. Os números $\sqrt[n]{2} \in \mathbb{R} \subset \mathbb{C}$ são todos elementos de $\overline{\mathbb{Q}}_{\mathbb{C}}$ com polinômio mínimo $m_{\sqrt[n]{2},\mathbb{Q}}(x) = x^n - 2$ (Eisenstein, $p=2$). Logo, $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. Então, para todo inteiro positivo k, $\mathbb{Q} \subset \mathbb{Q}(\sqrt[k+1]{)}2 \subset \overline{\mathbb{Q}}_{\mathbb{C}}$ com $[\mathbb{Q}(\sqrt[k+1]{2}) : \mathbb{Q}] = k+1 > k$. Logo, $[\overline{\mathbb{Q}}_{\mathbb{C}} : \mathbb{Q}] > k$ qualquer que seja o inteiro positivo k. Portanto, $\overline{\mathbb{Q}}_{\mathbb{C}}$ é uma extensão algébrica infinita de $\mathbb{Q}$.

OBS 9.1. Considere o corpo $\overline{\mathbb{Q}}_{\mathbb{R}} = \overline{\mathbb{Q}}_{\mathbb{C}} \cap \mathbb{R}$ dos números reais algébricos sobre $\mathbb{Q}$. O corpo $\mathbb{Q}$ é enumerável. Qualquer que seja o inteiro positivo n, o número de polinômios de grau exatamente n é enumerável (um polinômio de grau n é determinado unicamente pelos seus $n+1$ coeficientes em $\mathbb{Q}$). Como um polinômio de grau n tem no máximo n raízes, o conjunto

$$\overline{\mathbb{Q}}_{\mathbb{R}}(n) = \{\alpha \in \mathbb{R} \ : \ \deg m_{\alpha,\mathbb{Q}(x)} = n\}$$

é enumerável. Finalmente, $\overline{\mathbb{Q}}_{\mathbb{R}} = \cup_{n>0}\overline{\mathbb{Q}}_{\mathbb{R}}(n)$ é uma união enumerável de conjuntos enumeráveis e, portanto, é também enumerável. Como $\mathbb{R}$ é não enumerável, existem elementos reais não algébricos, isto é, transcendentes sobre $\mathbb{Q}$. Temos a inclusão própria $\overline{\mathbb{Q}}_{\mathbb{R}} \subsetneq \mathbb{R}$ donde $\overline{\mathbb{Q}}_{\mathbb{R}} \subsetneq \mathbb{C}$. Segue também que $\mathbb{R}$ é uma extensão infinita dos racionais.

OBS 9.2. Sabemos que $\pi = 3,14159\ldots$ e $e = 2.71828\ldots$ são transcendentes sobre $\mathbb{Q}$ (a prova é não trivial!). Ver o livro do Hardy (Leitura complementar) para uma introdução ao assunto.

9.8 Conclusão

As extensões algébricas finitamente geradas possuem uma estrutura algébrica bastante simples: são espaços vetoriais de dimensão finita.

RESUMO

$$\begin{array}{ccc} & \textbf{Finita} & \\ \swarrow & \Updownarrow & \searrow \\ \textbf{Algébrica} & + & \textbf{Finitamente gerada} \end{array}$$

Contra-exemplos:

Algébrica $\not\Rightarrow$ Finita: $\overline{\mathbb{Q}}_{\mathbb{R}}$ sobre $\mathbb{Q}$.

Algébrica $\not\Rightarrow$ Finitamente gerada: $\overline{\mathbb{Q}}_{\mathbb{R}}$ sobre $\mathbb{Q}$.

Finitamente gerada $\not\Rightarrow$ Finita: $\mathbb{Q}(\pi)$ sobre $\mathbb{Q}$.

Finitamente gerada $\not\Rightarrow$ Algébrica: $\mathbb{Q}(\pi)$ sobre $\mathbb{Q}$.

Transitividade

$$\left.\begin{array}{c} L \\ \Big| \Big) \text{algébrica} \\ K \\ \Big| \Big) \text{algébrica} \\ F \end{array}\right. \Longrightarrow \left.\begin{array}{c} L \\ \Big| \\ K \\ \Big| \\ F \end{array}\right) \text{algébrica}$$

PRÓXIMA AULA

Voltaremos a ver o processo de adjunção de raízes para construção do corpo de raízes de um polinômio. Mostraremos a existência de tais corpos, a unicidade, e a caracterizaremos por meio de extensões finita e normal.

ATIVIDADES

ATIV. 9.1.

Determine uma base de cada extensão de $\mathbb{Q}$ dada abaixo.

a) $\mathbb{Q}(\sqrt{5}, i)$.

b) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$.

c) $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$.

d) $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Se $F \subset K$ é uma extensão finita e α é algébrico sobre K prove que $[K(\alpha) : K] \leq [K : F]$.

ATIV. 9.2.

ATIV. 9.3. Suponha que $\alpha, \beta \in K$ são algébricos sobre F.

a) Se $\deg m_{\alpha,F}(x) = m$ e $\deg m_{\beta,F}(x) = n$ são relativamente primos (MDC$(m, n) = 1$)), mostre que $[F(\alpha, \beta) : F] = mn$.

b) Mostre, por meio de um contraexemplo, que a conclusão da parte a) pode ser falsa se m e n não são relativamente primos.

c) Determine $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$.

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.