AULA

8

Extensão de um Isomorfismo

META:

Obter uma condição suficiente para duas extensões simples serem isomorfas e elaborar um método para construir automorfismos de uma extensão fixando o corpo base.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Definir extensão de um isomorfismo.

Usar o critério sobre polinômios mínimos para determinar se duas extensões simples são isomorfas.

Aplicar o método descrito na aula para construir automorfismos de uma extensão finitamente.

PRÉ-REQUISITOS

A noção de isomorfismo de corpos e polinômio mínimo e o fato 5 da seção 7.4.

8.1 Introdução

Dada uma função $f : A \to B$ e um subconjunto $C \subset A$, a restrição de f ao conjunto C é a função $f_{|_C} : C \to B$ definida por $f_{|_C}(x) = f(x)$ para $x \in C$. Seja $\varphi : F \to E$ um homomorfismo de corpos e sejam A, B anéis tais que $F \subset A$, $E \subset B$. Um homomorfismo $\psi : A \to B$ é dito uma extensão de φ (ou que φ estende-se à ψ) se $\psi_{|_F} = \varphi$.

Se $\varphi : F \to E$ é um homomorfismo (isomorfismo) de corpos então a aplicação

$$\tilde{\varphi} : F[x] \to E[x]$$

definida por

$$\tilde{\varphi}(a_0 + a_1x + \cdots + a_nx^n) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n$$

define um homomorfismo (isomorfismo) de $F[x]$ em $E[x]$ (você consegue verificar isto?). Além disso, se $c \in F \subset F[x]$ então $\tilde{\varphi}(c) = \varphi(c)$ e, consequentemente, $\tilde{\varphi}$ é uma extensão de φ. Em outras palavras, todo homomorfismo (isomorfismo) $\varphi : F \to E$ estende-se à um homomorfismo (isomorfismo) $\tilde{\varphi} : F[x] \to E[x]$ definido por

$$\tilde{\varphi}(a_0 + a_1x + \cdots + a_nx^n) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n.$$

Nesta aula, mostraremos que a igualdade entre os polinômios mínimos de dois elementos algébricos sobre um mesmo corpo acarreta isomorfismo entre as extensões simples geradas pelos mesmos. Veremos que esta condição de igualdade entre polinômios mínimos, para ocorrer isomorfismo, é o caso particular para se estender o automorfismo identidade.

8.2 $m_{\alpha,F}(x) = m_{\beta,F}(x) \Rightarrow F(\alpha) \cong F(\beta)$

Sejam L e K duas extensões de um mesmo corpo F e sejam $\alpha \in L$ e $\beta \in K$ elementos algébricos. Se $m_{\alpha,F}(x) = m_{\beta,F}(x)$ então, do fato 5 da seção 7.4, tem-se

$$F(\alpha) = F[\alpha] \cong F[x]/(m_\alpha(x)) = F[x]/(m_\beta(x)) \cong F[\beta] = F(\beta).$$

Podemos mostrar ainda que existe um isomorfismo

$$\varphi : F(\alpha) \to F(\beta)$$

satisfazendo as condições $\varphi(\alpha) = \beta$ e $\varphi(c) = c$ para todo $c \in F$. De fato, o isomorfismo identidade sobre F, aqui denotado por $I_{\mathbb{F}}$, se estende à um isomorfismo $\tilde{I}_F$ sobre $F[x]$. Considere o diagrama de homomorfismos

$$\begin{array}{ccccc} F[x] & \overset{\tilde{I}_F}{\to} & F[x] & \overset{\pi}{\to} & F[x]/(m_{\beta,F}(x)) \overset{\Psi}{\cong} F(\beta) \\ \uparrow & & \uparrow & & \\ F & \overset{I_F}{\to} & F & & \end{array}$$

Então, o homomorfismo composição $\Psi \circ \pi \circ \tilde{I}_F$ é sobrejetivo (composição de homomorfismos sobrejetivos) e

$$\Psi \circ \pi \circ \tilde{I}_F(f(x)) = 0 \Leftrightarrow f(\beta) = 0 \Leftrightarrow f(x) \in (m_{\beta,F}(x))$$

Mas, $(m_{\beta,F}(x)) = (m_{\alpha,F}(x))$ donde

$$\Psi \circ \pi \circ \tilde{I}_F(f(x)) = 0 \Leftrightarrow f(x) \in (m_{\alpha,F}(x))$$

Assim, Ker $\Psi \circ \pi \circ \tilde{I}_F = (m_{\alpha,F}(x))$. Denotando

$$J = \text{ Ker } (\Psi \circ \pi \circ \tilde{I}_F) = (m_{\alpha,F}(x)),$$

segue, pelo teorema fundamental do isomorfismo, que a aplicação

$$\Theta : F[x]/J \to F[\beta]$$

definida por

$$\Theta(\overline{f(x)}) = \Psi \circ \pi \circ \tilde{I}_F(f(x)) = \Psi \circ \pi(f(x)) = \Psi(\overline{f(x)}) = f(\beta)$$

define um isomorfismo. Temos os seguintes isomorfismos

$$F(\alpha) \overset{\pi}{\leftarrow} F[x]/J \overset{\Theta}{\rightarrow} F[\beta].$$

Então,

$$\Theta \circ \pi^{-1} : F(\alpha) \to F(\beta)$$

é um isomorfismo tal que $\Theta \circ \pi^{-1}(f(\alpha)) = \Theta(\overline{f(x)}) = f(\beta)$. Em particular, $\Theta \circ \pi^{-1}(\alpha) = \beta$ e $\Theta \circ \pi^{-1}(c) = c$ para todo $c \in F$.

Exemplo 8.1. Considere $\alpha = \sqrt[3]{2} \in \mathbb{R}$ e $\beta = \sqrt[3]{2}(-\frac{1}{2} + \frac{\sqrt{3}}{2}i) \in \mathbb{C}$. Note que $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ é uma raiz cúbica complexa da unidade, pois $\omega = \cos 120° + \sin 120° i = e^{2\pi i/3}$ (fórmula de Euler) e, portanto, $\omega^3 = e^{2\pi i} = 1$. Assim, $\beta^3 = (\sqrt[3]{2}\omega)^3 = \sqrt[3]{2}^3\omega^3 = 2.1 = 2$. Então, α e β são raízes do polinômio $x^3 - 2 \in \mathbb{Q}[x]$. Como $x^3 - 2$ é irredutível em $\mathbb{Q}[x]$, α e β têm polinômios mínimos iguais sobre $\mathbb{Q}[x]$. Pelo resultado acima, existe um isomorfismo

$$\varphi : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}[\sqrt[3]{2}(-\frac{1}{2} + \frac{\sqrt{3}}{2}i))$$

tal que $\varphi(\alpha) = \beta$ e $\varphi(c) = c$ para todo $c \in \mathbb{Q}$ (extensão da identidade sobre $\mathbb{Q}$).

8.3 Extensão de isomorfismos para extensões simples

Segue uma generalização do resultado acima.

Teorema 8.1. *Seja $\varphi : F \to F'$ um isomorfismo de corpos e K, K' extensões de F e F', respectivamente. Seja $\alpha \in K$ algébrico sobre*

F com polinômio mínimo $m_{\alpha,F}(x) \in F[x]$ e $\alpha' \in K'$ algébrico sobre F' com polinômio mínimo $m_{\alpha',F'} \in F'$. Seja $\tilde{\varphi} : F[x] \to F'[x]$ a extensão de φ como acima. Se $\tilde{\varphi}(m_{\alpha,F}(x)) = m_{\alpha',F'}(x)$ então existe um isomorfismo $\sigma : F[\alpha] \xrightarrow{\sim} F'[\alpha']$ estendendo φ tal que $\sigma(\alpha) = \alpha'$.

Prova: Assim como na seção anterior, o isomorfismo φ estende-se à um isomorfismo

$$\tilde{\varphi} : F[x] \to F'.$$

Observe que $F'[x]/(\tilde{\varphi}(m_{\alpha,F}(x)) = F'[x]/(m_{\alpha',F'}(x)) \cong F'(\alpha')$, pois $\tilde{\varphi}(m_{\alpha,F}(x)) = m_{\alpha',F'}(x)$ por hipótese. Temos o seguinte diagrama de homomorfismos

$$\begin{array}{ccccc}
F[x] & \stackrel{\tilde{\varphi}}{\to} & F'[x] & \stackrel{\pi}{\to} & F[x]/(\tilde{\varphi}(m_{\alpha,F}(x)) \stackrel{\Psi}{\cong} F(\alpha') \\
\uparrow & & \uparrow & & \\
F & \stackrel{\varphi}{\to} & F' & &
\end{array}$$

onde

$$\Psi \circ \pi \circ \tilde{\varphi}(f(x)) = \Psi \circ \pi(\tilde{\varphi}(f)(x)) = \Psi(\overline{\varphi\widetilde{(f)}(x)}) = \varphi\widetilde{(f)}(\alpha').$$

A composição acima é um homomorfismo sobrejetivo, pois composição de homomorfimos sobrejetivos é homomorfismo sobrejetivo. Além disso,

$$\begin{aligned}
\Psi \circ \pi \circ \tilde{\varphi}(f(x)) = 0 &\Leftrightarrow (\tilde{\varphi}(f))(\alpha') = 0 \\
&\Leftrightarrow \tilde{\varphi}(f(x)) = \overline{0} \\
&\Leftrightarrow \tilde{\varphi}(f(x)) \in (\tilde{\varphi}(m_{\alpha,F}(x))) \\
&\Leftrightarrow \tilde{\varphi}(f(x)) = g(x)\tilde{\varphi}(m_{\alpha,F}(x)) \\
&\Leftrightarrow \tilde{\varphi}(f(x)) = \tilde{\varphi}(h(x))\tilde{\varphi}(m_{\alpha,F}(x)) \\
&\Leftrightarrow \tilde{\varphi}(f(x)) = \tilde{\varphi}(h(x)m_{\alpha,F}(x)) \\
&\Leftrightarrow f(x) = h(x)m_{\alpha,F}(x) \\
&\Leftrightarrow f(x) = (m_{\alpha,F}(x))
\end{aligned}$$

Usamos acima o fato de $\tilde{\varphi}$ ser isomorfismo. Denotando $\Theta = \Psi \circ \pi \circ \tilde{\varphi}$, temos Ker $\Theta = (m_{\alpha,F}(x))$. Assim, pelo teorema fundamental do isomorfismo, a aplicação

$$\overline{\Theta} : F[x]/(m_{\alpha,F}(x)) \to F'(\alpha')$$

dada por $\overline{\Theta}(\overline{f(x)}) = \Theta(f(x)) = (\tilde{\varphi}(f))(\alpha')$ define um isomorfismo. Temos então os seguintes isomorfismos:

$$F(\alpha) \overset{\pi}{\leftarrow} F[x]/(m_{\alpha,F}(x)) \overset{\Theta}{\to} F'(\alpha').$$

Assim,

$$\Theta \circ \pi^{-1} : F(\alpha) \to F'(\alpha')$$

é um isomorfismo tal que $\Theta \circ \pi^{-1}(f(\alpha)) = \Theta(\overline{f(x)}) = (\tilde{\varphi}(f))(\alpha')$. Em particular, $\Theta \circ \pi^{-1}(\alpha) = \alpha'$ e $\Theta \circ \pi^{-1}(c) = \varphi(c)$ para todo $c \in F$. $\square$

OBS 8.1. Daqui por diante, usaremos o diagrama

$$\begin{array}{cccc}
\sigma : & F(\alpha) & \overset{\sim}{\to} & F'(\alpha') \\
 & \uparrow & & \uparrow \\
\varphi : & F & \overset{\sim}{\to} & F'
\end{array}$$

para representar o teorema acima. Nestes termos, o resultado $F(\alpha) \cong F(\beta)$ sempre que $m_\alpha(x) = m_\beta(x)$, obtido na seção anterior, é um caso particular do teorema acima e tem sua representação pictórica dada por

$$\begin{array}{rccc} \sigma: & F(\alpha) & \overset{\sim}{\to} & F'(\alpha') \\ & \uparrow & & \uparrow \\ I_F: & F & \overset{\sim}{\to} & F' \end{array}$$

onde I_F denota o isomorfismo identidade em F.

OBS 8.2. Uma extensão da identidade $\iota : \mathbb{Q} \to \mathbb{Q}$ será chamada um $\mathbb{Q}$-homomorfismo, $\mathbb{Q}$-isomorfismo ou $\mathbb{Q}$-automorfismo conforme seja um homomorfismo, isomorfismo ou automorfismo, respectivamente.

Exemplo 8.2. Sejam $p, q \in \mathbb{Z}$ primos positivos. Mostre que existe um $\mathbb{Q}$-automorfismo $\tau : \mathbb{Q}(\sqrt{p}, \sqrt{q}) \to \mathbb{Q}(\sqrt{p}, \sqrt{q})$ tal que $\tau(\sqrt{p}) = -\sqrt{p}$ e $\tau(\sqrt{q}) = -\sqrt{q}$.

8.4 Conclusão

Estender isomorfismos de corpos perante a análise de polinômios mínimos é prático e será de muita utilidade na teoria de Galois.

RESUMO

- Todo homomorfismo (isomorfismo) $\varphi : F \to E$ estende-se à um homomorfismo (isomorfismo) $\tilde{\varphi} : F[x] \to E[x]$ definido por

$$\tilde{\varphi}(a_0 + a_1 x + \cdots + a_n x^n) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_n)x^n.$$

- $m_{\alpha,F}(x) = m_{\beta,F}(x) \Rightarrow F(\alpha) \cong F(\beta)$.

- Seja $\varphi : F \to F'$ um isomorfismo de corpos e K, K' extensões de F e F', respectivamente. Seja $\alpha \in K$ algébrico sobre F com polinômio mínimo $m_{\alpha,F}(x) \in F[x]$ e $\alpha' \in K'$ algébrico sobre F' com polinômio mínimo $m_{\alpha',F'} \in F'$. Seja $\tilde{\varphi} : F[x] \to F'[x]$ a extensão de φ como acima. Se $\tilde{\varphi}(m_{\alpha,F}(x)) = m_{\alpha',F'}(x)$ então existe um isomorfismo $\sigma : F[\alpha] \xrightarrow{\sim} F'[\alpha']$ estendendo φ tal que $\sigma(\alpha) = \alpha'$.

PRÓXIMA AULA

Estudaremos extensões algébricas. Relacionaremos os tipos de extensões com extensões algébricas sempre buscando condições suficientes para caracterizar quando uma extensão dada é algébrica sobre o corpo base.

ATIVIDADES

Durante as atividades a seguir, K é uma extensão do corpo F.

ATIV. 8.1. Seja $\sigma : F \to E$ um isomorfismo de corpos, $f(x) \in F[x]$ e $\sigma : F[x] \to E[x]$ o isomorfismo induzido por σ. Mostre que:

i) deg $f(x) =$ deg $\sigma(f(x))$.

ii) $f(x)$ irredutível se e somente se $\sigma(f(x))$ irredutível. item[iii)] Sejam K e L extensões de F e E, respectivamente. Se $\tilde{\sigma} : K \to L$ é uma extensão de σ e $\alpha \in K$ é uma raiz de $f(x)$ mostre que $\tilde{\sigma}(\alpha) \in L$ é uma raiz de $\sigma(f(x))$.

ATIV. 8.2. Mostre que existe um automorfismo $\sigma : \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(\sqrt{3})$ tal que $\sigma(\sqrt{3}) = -\sqrt{3}$ e $\sigma(c) = c$ para todo $cin\mathbb{Q}$.

ATIV. 8.3. Mostre que existe o isomorfismo σ obtido na atividade anterior estende-se à um $\mathbb{Q}$-automorfismo $\tau : \mathbb{Q}(\sqrt{3})(\sqrt{5}) \to \mathbb{Q}(\sqrt{3})(\sqrt{5})$ tal que $\tau(\sqrt{5}) = \sqrt{5}$.

ATIV. 8.4. Mostre que existe um $\mathbb{Q}$-automorfismo $\tau : \mathbb{Q}(\sqrt{3}, \sqrt{5}) \to \mathbb{Q}(\sqrt{3}, \sqrt{5})$ tal que $\tau(\sqrt{3}) = -\sqrt{3}$ e $\tau(\sqrt{5}) = -\sqrt{5}$.

ATIV. 8.5. Mostre que existe um $\mathbb{Q}$-automorfismo $\tau : \mathbb{Q}(\sqrt{2}, i) \to \mathbb{Q}(\sqrt{2}, i)$ tal que $\tau(\sqrt{2}) = \sqrt{2}$ e $\tau(i) = -i$.

ATIV. 8.6. Mostre que existe um $\mathbb{Q}$-automorfismo $\tau : \mathbb{Q}(\sqrt{2}, i) \to \mathbb{Q}(\sqrt{2}, i)$ tal que $\tau(\sqrt{2}) = -\sqrt{2}$ e $\tau(i) = i$.

ATIV. 8.7. Mostre que existe um $\mathbb{Q}$-automorfismo $\tau : \mathbb{Q}(\sqrt{2}, i) \to \mathbb{Q}(\sqrt{2}, i)$ tal que $\tau(\sqrt{2}) = -\sqrt{2}$ e $\tau(i) = -i$.

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.

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