AULA

12

Noções elementares da Teoria de Galois

META:

Conceituar o grupo de Galois e a correspondência de Galois de uma extensão de corpos.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Definir o grupo de Galois de uma extensão de corpos.

Definir corpo intermediário de uma extensão de corpos.

Definir corpo fixado de um subgrupo do grupo de Galois e estabelecer a correspondência de Galois de uma extensão.

Determinar o grupo de Galois de certas extensões de corpos.

Determinar a correspondência de Galois para certas extensões.

PRÉ-REQUISITOS

Teoria de grupos: definição de grupo, ordem de um grupo, subgrupo, subgrupo normal, isomorfismo de grupos, o grupo de permutações S_n.

Teoria de corpos: Aulas 8, 9, 10 e 11.

Noções elementares da
Teoria de Galois

12.1 Introdução

12.2 O grupo de Galois

Seja K uma extensão de um corpo F. Um F-automorfismo de K é um automorfismo $\sigma : K \to K$ que fixa os elementos de F, isto é, $\sigma(c) = c$ para todo $c \in F$. Na linguagem da aula 8, um F-automorfismo é uma extensão $\sigma : K \to K$ do automorfismo identidade $I_F : F \to F$. Denotamos por $Gal_F(K)$ ao conjunto de todos os F-automorfismos de K.
Se σ e τ são dois automorfismos de K extensões da identidade em F então a composição $\sigma \circ \tau$ é também um automorfismo de K extensão da identidade em F.

Composição define uma operação em GAL_FK

A composição de funções é uma operação associativa. O isomorfismo identidade em K é uma extensão da identidade em F. E, se $\sigma \in Gal_FK$ então $\sigma(c) = c \forall c \in F$. Aplicando o isomorfismo inverso σ^{-1} a ambos os termos da igualdade obtém-se $c = \sigma^{-1} \circ \sigma(c) = \sigma^{-1}(c)$. Logo, Gal_FK é fechado com respeito à inversos. Então

Gal_FK é um grupo com respeito à operação composição

Definição 12.1. O grupo Gal_FK é chamado o grupo de Galois da extensão $F \subset K$.

12.3 Fatos

1. Seja K uma extensão de um corpo F e $f(x) \in F[x]$. Se $\alpha \in K$ é raiz de $f(x)$ e $\sigma \in Gal_FK$ então $\sigma(\alpha)$ é também

raiz de $f(x)$.

2. Seja $K = SF_F(f(x))$ o corpo de raízes de $f(x) \in F[x]$ sobre F e sejam $\alpha, \beta \in K$. Então, existe $\sigma \in Gal_F K$ tal que $\sigma(\alpha) = \beta$ se somente se α e β têm o mesmo polinômio mínimo.

3. Seja $K = F(\alpha_1, \ldots, \alpha_n)$ uma extensão algébrica sobre F. Se $\sigma, \tau \in Gal_F K$ e $\sigma(\alpha_i) = \tau(\alpha_i)$, para todo $i = 1, 2, \ldots, n$ então $\sigma = \tau$. Em outras palavras, um automorfismo em $Gal_F K$ é completamente determinado pelas imagens de $\alpha_1, \ldots, \alpha_n$.

4. Se K é um corpo de raízes de um polinômio separável $f(x) \in F[x]$ de grau n então $Gal_F K$ é isomorfo à um subgrupo de S_n.

12.4 Exemplos

Exemplo 12.1. O grupo de Galois de $\mathbb{C}$ sobre $\mathbb{R}$. Primeiramente, devemos expressar $\mathbb{C}$ como uma extensão simples ou finitamente gerada se possível. Sabemos que $\mathbb{C} = \mathbb{R}(i)$. Em seguida, determinamos os polinômios mínimos de cada gerador, neste caso, $m_{i,\mathbb{R}} = x^2 + 1$. Agora, usaremos os fatos acima para determinar $Gal_{\mathbb{R}}\mathbb{C}$.

1. Pelo fato 1, $\sigma \in Gal_F K \Leftrightarrow \sigma(i)$ é raiz de $x^2 + 1 \Leftrightarrow \sigma(i) = i$ ou $\sigma(i) = -i$. Assim, só podem existir no máximo dois F-automorfismos de $\mathbb{C}$, isto é, $|Gal_{\mathbb{R}}\mathbb{C}| \leq 2$.

2. Como i e $-i$ são raízes do mesmo polinômio mínimo, o fato 2 nos garante a existência de $\sigma, \tau \in Gal_{\mathbb{R}}\mathbb{C}$ tal que $\sigma(i) = i$ e $\tau(i) = -i$.

3. Pelo fato 3, nos diz que um elemento $\sigma \in Gal_{\mathbb{R}}\mathbb{C}$ fica completamente determinado pelas imagens dos geradores da extensão, neste caso pela imagem de i. De fato, para todo $z = a + bi \in \mathbb{C}$, temos:

   $\sigma(z) = \sigma(a + bi) = \sigma(a) + \sigma(bi) = \sigma(a) + \sigma(b)\sigma(i) = a + bi$, pois $\sigma(c) = c$ se $c \in \mathbb{R}$ (definição de $Gal_F K$) e $\sigma(i) = i$ por construção). Logo, $\sigma = \iota$, a identidade em $\mathbb{C}$.

   $\tau(z) = \tau(a + bi) = \tau(a) + \tau(bi) = \tau(a) + \tau(b)\tau(i) = a + b(-i) = a - bi$. Logo, τ é a aplicação conjugação em $\mathbb{C}$.

   Como $|Gal_{\mathbb{R}}\mathbb{C}| \leq 2$ e $\{\iota, \tau\} \subset Gal_{\mathbb{R}}\mathbb{C}$ segue que $Gal_{\mathbb{R}}\mathbb{C} = \{\iota, \tau\}$.

4. Finalmente, o fato 4 afirma que o grupo de Galois do corpo de raízes de um polinômio separável de grau n é um subgrupo de S_n. Neste caso, temos o isomorfismo $\phi : Gal_{\mathbb{R}}\mathbb{C} \to S_2$ definido por $\iota \mapsto \iota$ e $\tau \mapsto (12)$. Note que ambos os grupos são isomorfos ao grupo aditivo $\mathbb{Z}_2$.

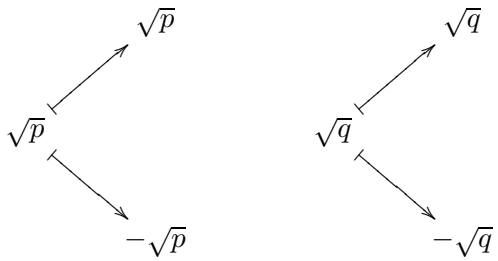
Exemplo 12.2. O grupo de Galois de $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ sobre $\mathbb{Q}$, p, q primos. A extensão já está na forma finitamente gerada. Só que desta vez são dois geradores, isto é, a extensão não é simples. Vamos aos procedimentos:

1. Polinômios mínimos dos geradores:

   $m_{\sqrt{p},\mathbb{Q}}(x) = x^2 - p$. Raízes: $\sqrt{p}, -\sqrt{p}$.

   $m_{\sqrt{q},\mathbb{Q}}(x) = x^2 - q$. Raízes: $\sqrt{q}, -\sqrt{q}$.

2. Possíveis imagens dos geradores $\sqrt{p}$ e $\sqrt{q}$:



Conclusão: Existem 4 possíveis $\mathbb{Q}$-automorfismos de $\mathbb{Q}(\sqrt{p}, \sqrt{q})$:

$$\begin{array}{lll} \sqrt{p} & \overset{\iota}{\longmapsto} & \sqrt{p} \\ \sqrt{q} & \longmapsto & \sqrt{q} \end{array} \qquad \begin{array}{lll} \sqrt{p} & \overset{\sigma_1}{\longmapsto} & \sqrt{p} \\ \sqrt{q} & \longmapsto & -\sqrt{q} \end{array}$$

$$\begin{array}{lll} \sqrt{p} & \overset{\sigma_2}{\longmapsto} & -\sqrt{p} \\ \sqrt{q} & \longmapsto & \sqrt{q} \end{array} \qquad \begin{array}{lll} \sqrt{p} & \overset{\sigma_3}{\longmapsto} & -\sqrt{p} \\ \sqrt{q} & \longmapsto & -\sqrt{q} \end{array}$$

3. Existência de $\iota, \sigma_1, \sigma_2, \sigma_3$:

   (a) Existência de σ_1. Considere o diagrama:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{p}, \sqrt{q}) & & \mathbb{Q}(\sqrt{p}, -\sqrt{q}) \\ \uparrow & & \uparrow \\ \mathbb{Q}(\sqrt{p}) & \xrightarrow{I_{\mathbb{Q}(\sqrt{p})}} & \mathbb{Q}(\sqrt{p}) \end{array}$$

   onde $I_{\mathbb{Q}(\sqrt{p})}$ denota a identidade em $\mathbb{Q}(\sqrt{p})$. Como

$$m_{\sqrt{q},\mathbb{Q}(\sqrt{p})}(x) = x^2 - q = m_{-\sqrt{q},\mathbb{Q}(\sqrt{p})}(x)$$

   segue que o isomorfismo identidade $I_{\mathbb{Q}(\sqrt{p})}$ estende-se à um isomorfismo

$$\varphi : \mathbb{Q}(\sqrt{p}, \sqrt{q}) \to \mathbb{Q}(\sqrt{p}, -\sqrt{q})$$

   tal que $\varphi(\sqrt{q}) = -\sqrt{q}$. Desde que φ fixa os elementos de $\mathbb{Q}(\sqrt{p})$, em particular fixa cada elemento em $\mathbb{Q}$. Deste modo, $\varphi \in Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{p}, \sqrt{q})$. Faça $\sigma_1 = \varphi$.

(b) Existência de σ_2: Análoga à de σ_1. (Faça como exercício, prezado aluno!)

(c) Existência de σ_3: A igualdade

$$m_{\sqrt{p},\mathbb{Q}}(x) = x^2 - p = m_{-\sqrt{p},\mathbb{Q}}(x)$$

implica que existe um isomorfismo

$$\varphi : \mathbb{Q}(\sqrt{p}) \to \mathbb{Q}(-\sqrt{p})$$

extensão da identidade que leva $\sqrt{p}$ em $-\sqrt{p}$. Do mesmo modo, a igualdade

$$m_{\sqrt{q},\mathbb{Q}(\sqrt{p}}(x) = x^2 - q = m_{-\sqrt{q},\mathbb{Q}(-\sqrt{p})}(x)$$

implica a existência de um isomorfismo

$$\sigma_3 : \mathbb{Q}(\sqrt{p})(\sqrt{q}) \to \mathbb{Q}(-\sqrt{p})(-\sqrt{q})$$

extensão de φ que leva $\sqrt{q}$ em $-\sqrt{q}$. Então, σ_3 é um elemento de $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{p})$ (verifique!) tal que $\sqrt{p} \mapsto -\sqrt{p}$ e $\sqrt{q} \mapsto -\sqrt{q}$. Assim, $|Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})| \leq 4$ e existem quatro elementos distintos $\iota, \sigma_1, \sigma_2, \sigma_3$ em $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$ segue que

$$Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q}) = \{\iota, \sigma_1, \sigma_2, \sigma_3\}.$$

(d) Temos

$$\begin{aligned} SF_{\mathbb{Q}}((x^2-p)(x^2-q)) &= \mathbb{Q}(\sqrt{p},-\sqrt{p},\sqrt{q},-\sqrt{q}) \\ &= \mathbb{Q}(\sqrt{p},\sqrt{q}). \end{aligned}$$

Logo, $\mathbb{Q}(\sqrt{p},\sqrt{q})$ é o corpo de raízes do polinômio separável $(x^2-p)(x^2-q)$. Pelo grau ser 4, segue do fato 4, que $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$ é isomorfo à um subgrupo de S_4.

Vejamos como montar um tal isomorfismo. Primeiro, estabeleça uma bijeção entre os conjunto das quatro raízes distintas de $(x^2 - p)(x^2 - q)$ com o conjunto $\{1, 2, 3, 4\}$, digamos

$$\begin{aligned} \sqrt{p} &\longmapsto 1 \\ \sqrt{q} &\longmapsto 2 \\ -\sqrt{p} &\longmapsto 3 \\ -\sqrt{q} &\longmapsto 4 \end{aligned}$$

Com isto, podemos enxergar um elemento do grupo $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{p}, \sqrt{q})$ como uma permutação em $\{1, 2, 3, 4\}$ de acordo com sua ação em $\sqrt{p}$ e $\sqrt{q}$. Por exemplo, a ação de σ_1 é dada por:

$$\begin{aligned} \sqrt{p} &\longmapsto \sigma_1(\sqrt{p}) = \sqrt{p} \\ \sqrt{q} &\longmapsto \sigma_1(\sqrt{q}) = -\sqrt{q}) \\ -\sqrt{p} &\longmapsto \sigma_1(-\sqrt{p}) = -\sqrt{p} \\ -\sqrt{q} &\longmapsto \sigma_1(-\sqrt{q}) = -\sigma_1(\sqrt{q}) = -(-\sqrt{q}) = \sqrt{q} \end{aligned}$$

Em notação de permutação:

$$\begin{pmatrix} \sqrt{p} & \sqrt{q} & -\sqrt{p} & -\sqrt{q} \\ \sqrt{p} & -\sqrt{q} & -\sqrt{p} & \sqrt{q} \end{pmatrix}$$

ou, equivalentemente, segundo nossa correspondência biunívoca:

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

Em notação de ciclos temos (24). Adotaremos a notação de ciclos daqui por diante. Neste caminho, temos a seguinte correspondência: $\iota \mapsto (1)$, $\sigma_1 \mapsto (24)$, $\sigma_2 \mapsto (13)$, $\sigma_3 \mapsto (13)(24)$. A tábua de operações do grupo $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{p}, \sqrt{q})$ é dada por

$\circ$	ι	σ_1	σ_2	σ_3
ι	ι	σ_1	σ_2	σ_3
σ_1	σ_1	ι	σ_3	σ_2
σ_2	σ_2	σ_3	ι	σ_1
σ_3	σ_3	σ_2	σ_1	ι

Fazendo as identificações $(1) = e$, $(24) = \theta_1$, $(13) = \theta_2$ e $(24)(13) = \theta_3$, a tábua para o subgrupo $H = \{(1), (24), (13), (24)(13)\}$ de S_4 é dada por

$\circ$	ι	θ_1	θ_2	θ_3
e	e	θ_1	θ_2	θ_3
θ_1	θ_1	e	θ_3	θ_2
θ_2	θ_2	θ_3	e	θ_1
θ_3	θ_3	θ_2	θ_1	e

Segue, pela análise das tábuas de operações dos respectivos grupos, que a aplicação

$$\Psi : Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{p}, \sqrt{q}) \to H$$

definida por $\iota \mapsto (1)$, $\sigma_1 \mapsto (24)$, $\sigma_2 \mapsto (13)$, $\sigma_3 \mapsto (13)(24)$ é um isomorfismo.

OBS 12.1. O grupo $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{p}, \sqrt{q})$ é também isomorfo à $\mathbb{Z}_2 \times \mathbb{Z}_2$. Prezado aluno, você seria capaz de definir um tal isomorfismo usando as tábuas de operações dos dois grupos? Tente, por favor.

12.5 A correspondência de Galois

Seja $F \subset K$ uma extensão de corpos e $Gal_F K$ o grupo de Galois de K sobre F. Estão definidos:

Corpo intermediário da extensão $F \subset K$:

Um corpo E tal que $F \subset E \subset K$.

Subgrupo de $Gal_F K$ associado à um corpo intermediário E:

$$\Gamma(E) := Gal_E K := \{ \text{ automorfismos de } K \text{ que fixam } E\}.$$

Corpo intermediário associado à um subgrupo H de $Gal_F K$:

$$\Phi(H) = \{x \in K \ : \ \sigma(x) = x, \text{ para todo } \sigma \in H\}$$

OBS 12.2. O corpo $\Phi(H)$ é chamado *corpo fixado* de H.

De acordo com as associações acima fica bem definida a correspondência:

$$\begin{array}{ccc} \{ \text{ Corpos intermediários de } F \subset K\} & \longleftrightarrow & \{ \text{ Subgrupos de } Gal_F K\} \\ E & \xrightarrow{\Gamma} & Gal_E K \\ \Phi(H) & \xleftarrow{\Phi} & H \end{array}$$

A correspondência assim definida é conhecida como a *correspondênica de Galois* da extensão $F \subset K$.

Exemplo 12.3. Considere $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \{\iota, \sigma_1, \sigma_2, \sigma_3\}$ como no exemplo 12.2. Vamos determinar o corpo fixado $\Phi(H)$ do subgrupo $H = \{\iota, \sigma_1\}$. Por definição,

$$\Phi(H) = \{x \in \mathbb{Q}(\sqrt{p}, \sqrt{q}) : \ \sigma(x) = x, \ \forall \ \sigma \in H\}.$$

Desde que ι fixa todo o corpo $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ (isomorfismo identidade), basta determinarmos os elementos de $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ fixados por σ_1.

Sabemos que $\{1, \sqrt{p}, \sqrt{q}, \sqrt{pq}\}$ é uma base de $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ sobre $\mathbb{Q}$. Assim, todo elemento $x \in \mathbb{Q}(\sqrt{p}, \sqrt{q})$ pode ser escrito na forma:

$$x = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}$$

para únicos $a, b, c, d \in \mathbb{Q}$. Então, $\sigma_1(x) = x$ se e somente se

$$\begin{aligned} a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} &= \sigma_1(a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}) \\ &= \sigma_1(a) + \sigma_1(b)\sigma_1(\sqrt{p}) + \\ &\quad \sigma_1(c)\sigma_1(\sqrt{q}) + \sigma_1(d)\sigma_1(\sqrt{pq}) \end{aligned}$$

Sabemos que $\sigma_1(c) = c$ para todo $c \in \mathbb{Q}$, $\sigma_1(\sqrt{p}) = \sqrt{p}$ e $\sigma_1(\sqrt{q}) = -\sqrt{q}$. Então,

$$\begin{aligned} a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} &= a + b\sqrt{p} - c\sqrt{q} + d\sigma_1(\sqrt{p})\sigma_1(\sqrt{q}) \\ &= a + b\sqrt{p} - c\sqrt{q} + d\sqrt{p}(-\sqrt{q}) \\ &= a + b\sqrt{p} - c\sqrt{q} - d\sqrt{p}\sqrt{q} \end{aligned}$$

Pela unicidade da expressão de um elemento com respeito à uma base, temos $\sigma_1(x) = x$ se e somente se $a = a$, $b = b$, $c = -c$ e $d = -d$ se e somente se $a, b \in \mathbb{Q}$ e $c = d = 0$. Portanto, $\sigma_1(x) = x$ se e somente se $x = a + b\sqrt{p} + 0.\sqrt{q} + 0\sqrt{pq} = a + b\sqrt{p}$ se e somente se $x \in \mathbb{Q}(\sqrt{p})$. Logo, $\Phi(H) = \mathbb{Q}(\sqrt{p})$.

Outra maneira de determinar $\Phi(H)$, seria como segue: $\sigma_1(x) = x$ para todo $x \in \mathbb{P}$, pois σ_1 fixa $\mathbb{Q}$ e $\sqrt{p}$. Então, $\mathbb{Q}(\sqrt{p}) \subset \Phi(H) \subset \mathbb{Q}(\sqrt{P}, \sqrt{q})$. Como $[\mathbb{Q}(\sqrt{P}, \sqrt{q}) : \mathbb{Q}(\sqrt{p})] = 2$, primo, segue que $\Phi(H) = \mathbb{Q}(\sqrt{p})$ ou $\Phi(H) = \mathbb{Q}(\sqrt{P}, \sqrt{q})$. Mas, $\sigma_1(\sqrt{q}) = -\sqrt{q} \neq \sqrt{q}$ donde $\sqrt{q} \notin \Phi(H)$. Logo, $\Phi(H) \neq \mathbb{Q}(\sqrt{P}, \sqrt{q})$ e, portanto, $\Phi(H) = \mathbb{Q}(\sqrt{p})$.

OBS 12.3. Seguindo o exemplo acima temos

Para o subgrupo $< \sigma_2 >= \{\iota, \sigma_2\}$ (subgrupo simples gerado por σ_2:

$$a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \in \Phi(< \sigma_2 >)$$

se e somente se

$$\begin{aligned} a+b\sqrt{p}+c\sqrt{q}+d\sqrt{pq} &= \sigma_2(a+b\sqrt{p}+c\sqrt{q}+d\sqrt{pq}) \\ &= a-b\sqrt{p}+c\sqrt{q}-d\sqrt{pq} \end{aligned}$$

se e somente se $b=d=0$. Assim, $\Phi(<\sigma_2>)=\{a+c\sqrt{q} \ : \ a,c\in\mathbb{Q}\}=\mathbb{Q}(\sqrt{q})$.

Note que

$$\sigma_3(\sqrt{pq})=\sigma_3(\sqrt{p})\sigma_3(\sqrt{q})=(-\sqrt{p})(-\sqrt{q})=\sqrt{pq}$$

Assim, para o subgrupo $<\sigma_3>=\{\iota,\sigma_3\}$:

$$a+b\sqrt{p}+c\sqrt{q}+d\sqrt{pq}\in\Phi(<\sigma_3>)$$

se e somente se

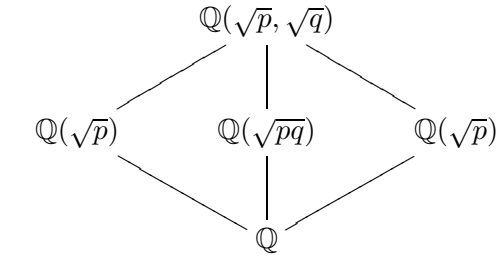
$$\begin{aligned} a+b\sqrt{p}+c\sqrt{q}+d\sqrt{pq} &= \sigma_3(a+b\sqrt{p}+c\sqrt{q}+d\sqrt{pq}) \\ &= a-b\sqrt{p}-c\sqrt{q}+d\sqrt{pq} \end{aligned}$$

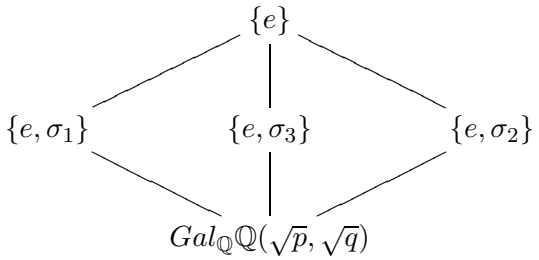
se e somente se $b=c=0$. Assim, $\Phi(<\sigma_2>)=\{a+d\sqrt{pq} \ : \ a,d\in\mathbb{Q}\}=\mathbb{Q}(\sqrt{pq})$. Temos mostrado a seguinte correspondência:

Subgrupos		Corpos fixados
$\{e\}$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt{p},\sqrt{q})$
$<\sigma_1>$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt{p})$
$<\sigma_2>$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt{q})$
$<\sigma_3>$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt{pq})$
$Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{p},\sqrt{q})$	$\longleftrightarrow$	$\mathbb{Q}$

Costuma-se representar tal correspondência na linguagem de

reticulados:





Onde subcorpos e subgrupos se correspondem de acordo com suas respectivas posições.

12.6 Conclusão

À toda extensão de corpos está associado o grupo de Galois da extensão. Nesta associação, existe uma correspondência entre corpos intermediários e subgrupos. Esta é o que se chama correspondência de Galois. A idéia é obter informações estruturais da extensão via teoria de grupos.

RESUMO

Dada uma extensão $F \subset K$:

Grupo de Galois:

$$Gal_F K := \{ \text{ conjunto dos } F\text{-automorfismos de } K \ \}$$

Correspondência de Galois:

$$\begin{array}{ccc} \{ \text{ Corpos intermediários de } F \subset K \} & \longleftrightarrow & \{ \text{ Subgrupos de } Gal_F K \ \} \\ E & \xrightarrow{\Gamma} & Gal_E K \\ \Phi(H) & \xleftarrow{\Phi} & H \end{array}$$

onde $\Phi(H) = \{x \in K \ : \ \sigma(x) = x, \forall \sigma \in H\}$ é chamado o corpo fixado de H.

PRÓXIMA AULA

Iremos determinar condições suficientes sobre a extensão para que a correspondência de Galois seja biunívoca.

ATIVIDADES

ATIV. 12.1. Demonstre todos os fatos da seção 12.3.

ATIV. 12.2. Determine $Gal_{\mathbb{Q}}(\sqrt{2}, \sqrt{3})$ e mostre que tal grupo é isomorfo à um subgrupo de S_4. Determine tal isomorfismo.

ATIV. 12.3. A tábua de $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (1,0), (0,1), (1,1)\}$ é dada por

$+$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(1,0)$	$(1,0)$	$(0,0)$	$(1,1)$	$(0,1)$
$(0,1)$	$(0,1)$	$(1,1)$	$(0,0)$	$(1,0)$
$(1,1)$	$(1,1)$	$(0,1)$	$(1,0)$	$(0,0)$

Defina explicitamnte um isomorfismo entre o grupo $Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt{2},\sqrt{3})$ e o grupo $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Sugestão: Use as tábuas de operações dos dois grupos.

ATIV. 12.4. Determine $Gal_{\mathbb{Q}}(\sqrt{2},\sqrt{3},\sqrt{5})$ e mostre que tal grupo é isomorfo à um subgrupo de S_8. Determine tal isomorfismo. Mostre também que $Gal_{\mathbb{Q}}(\sqrt{2},\sqrt{3},\sqrt{5}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

ATIV. 12.5. Mostre que a correspondência de Galois está bem definida. Em outras palavras, mostre que:

a) Se E é um corpo intermediário da extensão $F \subset K$ então $Gal_E K$ é um subgrupo de $Gal_F K$.

b) Se H é um subgrupo de $Gal_F K$ então $\Phi(H)$ é um corpo intermediário da extensão $F \subset K$.

ATIV. 12.6. Mostre que $\Phi(\Gamma(E)) \supset E$ para todo corpo intermediário de $F \subset K$ e $\Gamma(\Phi(H)) \supset H$ para todo subgrupo H de $Gal_F K$.

ATIV. 12.7. Mostre que a correspondência de galois é reversa com relação à inclusão. Mais precisamente, mostre que:

a) $E_1 \subset E_2$ implica $\Gamma(E_2) \subset \Gamma(E_1)$.

b) $H_1 \subset H_2$ implica $\Phi(H_2) \subset \Phi(H_1)$.

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.

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