ESTRUTURAS ALGÉBRICAS II

Por

Kalasas Vasconcelos de Araujo

UFS - 2009.2

Sumário

AULA

Polinômios

1

META:

Apresentar polinômios em uma indeterminada sobre um anel.

OBJETIVOS:

Ao fim da aula os alunos deverão ser capazes de:

Definir polinômios em uma indeterminada sobre um anel.

Compatibilizar a estrutura do anel A com a de $A[x]$.

Efetuar as operações de soma e produto de polinômios.

Reconhecer o grau de um polinômio.

Reconhecer coeficientes, termos, termo líder, coeficiente líder, monômio líder e o termo constante de um polinômio.

PRÉ-REQUISITOS

Definição de anel, domínio de integridade e corpo.

1.1 Introdução

Prezado aluno, bem vindo ao curso estruturas algébricas II. Esta é nossa primeira aula e começarei fazendo-lhe a seguinte pergunta: você sabe a diferença entre as seguintes expressões?

a) $f(X) = X^2 + X + 1$, $X \in \mathbb{R}$.

b) $X \in \mathbb{R}$ tal que $X^2 + X + 1 = 0$.

c) $X^2 + X + 1$.

Até o momento, você deveria saber tratarem-se, respectivamente, de uma função polinomial, uma equação polinomial e um polinômio.

Para diferenciarmos um objeto de um outro se faz necessário sabermos a definição precisa de cada um deles. Neste caso, o que é uma função? O que é uma equação algébrica? O que é um polinômio?

À luz da teoria dos conjuntos, a diferença entre função e equação torna-se evidente. Os nomes variável e incógnita servem justamente para diferenciarmos o papel de x quando o mesmo representa o elemento genérico do domínio de uma função ou uma solução genérica de uma equação. Já o x figurando-se em um polinômio passa a ser chamado de *indeterminada*.

Nesta aula, definiremos polinômios via um certo tipo de sequências. Esta definição evita o uso de indeterminada e ressalta a importância da estrutura do anel dos coeficientes na estrutura de anel dos polinômios.

1.2 Polinômios

A definição de polinômio que trazes consigo certamente é como uma expressão formal do tipo

$$a_n x^n + \cdots + a_1 x^1 + a_0$$

em que $a_0, a_1, \ldots, a_n$ são números reais e $i \in \mathbb{Z}$ é um inteiro positivo para todo i, $0 \leq i \leq n$.

Mas, você sabe o que é uma *expressão formal*? Qual o significado do termo ax^n? Isto é um produto ou meramente uma aglutinação de letras? Os coeficientes a_i's devem necessariamente ser reais ou complexos? O que mudaria no conjunto dos polinômios se considerássemos seus coeficientes em $\mathbb{Q}$, em $\mathbb{Z}$ ou até mesmo em $\mathbb{Z}_n$? Até que ponto a estrutura algébrica dos coeficientes interfere na estrutura algébrica do conjunto de polinômios? E o x, o que realmente ele representa?

A definição a seguir tanto evita qualquer tipo de obstrução psicológica quanto resolve a crise existencial dos polinômios e do x enquanto indeterminada.

Definição 1.1. Seja A um anel. Um polinômio com coeficientes no anel A é uma sequência infinita de elementos em A escrita na forma

$$(a_0, a_1, a_2, \ldots)$$

na qual todos os a_i's são nulos exceto para uma quantidade finita de índices. Os elementos $a_0, a_1, a_2, \ldots$ são chamados coeficientes do polinômio.

Usaremos o símbolo $\mathcal{P}_A$ para denotar o conjunto de todos os polinômios definidos sobre um anel A. Dois polinômios $P = (a_0, a_1, a_2, \ldots)$ e $Q = (b_0, b_1, b_2, \ldots)$ em $\mathcal{P}_A$ são iguais se são iguais como sequências, isto é, $a_i = b_i$ para cada índice i.

A sequência nula $(0, 0, 0, \ldots)$ é um polinômio chamado *polinômio nulo* e denotado por 0. Se $P = (a_0, a_1, a_2, \ldots) \in \mathcal{P}_A$ é não nulo então existe $n \geq 0$ tal que $a_n \neq 0$ e $a_i = 0$ para todo $i > n$. Tal inteiro n é chamado *grau* de P e denotado por $deg\ P$. Em símbolos,

$$deg\ P := max\{i\ :\ a_i \neq 0\}, \qquad (P \neq 0).$$

OBS 1.1. O grau do polinômio nulo não está definido. No entanto, a convenção $deg\ (0, 0, 0, \ldots) = -\infty$ não põe abaixo nenhuma das propriedades requeridas para o grau de polinômios. Definiremos $\deg 0 = \infty$ para estendermos a noção de grau à todos polinômios. O uso deste símbolo requer certa maturidade matemática mas, para nossos propósitos, basta termos em mente que $-\infty + k = -\infty$ qualquer que seja $k \in \mathbb{Z}$.

1.3 A estrutura algébrica dos polinômios e o significado da expressão $a_n x^n + \ldots a_1 x + a_0$

Seja A um anel. Por definição de anel, estão definidas em A duas operações: a adição $(a, b) \mapsto a + b$ e a multiplicação $(a, b) \mapsto a.b$ em que $(a, b) \in A \times A$. Usaremos tais operações em A para induzir uma adição e uma multiplicação no conjunto dos polinômios $\mathcal{P}_A$.

Teorema 1.1. *As operações*
Adição:

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

onde $c_k = a_k + b_k$ *para todo índice* k.
Multiplicação:

$$(a_0, a_1, a_2, \ldots).(b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

onde $c_k = a_0 b_k + a_1 b_{k-1} + \cdots a_{k-1} b_1 + a_k b_0$ *para todo índice* k.

estão bem definidas em $\mathcal{P}_A$.

Prova: Devemos mostrar que $\mathcal{P}_A$ é fechado com respeito a tais operações. Sejam P e Q dois polinômios em $\mathcal{P}_A$. Se P ou Q é o polinômio nulo então $P+Q$ é P ou Q e $PQ=0$. Suponhamos então P e Q ambos não nulos de graus n e m, respectivamente. Se $k > max\{n,m\}$ então $a_k + b_k = 0$, por definição de grau. Com relação ao produto, se $k > n+m$ então $c_k = \sum_{i=0}^{i=k} a_i b_{k-i}$ é nulo. De fato, se $i > n$ então $a_i = 0$ donde $a_i b_{k-i} = 0$. Se $i \leq n$ então $-i \geq -n$. Deste modo, $k > n+m$ implica $k-i > n+m-i \geq n+m-n = m$ donde $a_i b_{k-i} = 0$ pois $b_{k-i} = 0$. Assim, $c_k = 0$ para todo $k > n+m$. □

O propósito de definir tais operações em $\mathcal{P}_A$ é determinar uma estrutura de anel compatível com a estrutura do anel A de modo que A possa ser visto como subanel de $\mathcal{P}_A$.

Teorema 1.2. *A estrutua de anel em A induz uma estrutura de anel em $(\mathcal{P}_A, +, \bullet)$. Além disso, se A é comutativo e/ou com identidade então assim é $\mathcal{P}_A$.*

Prova: Com relação à adição devemos mostrar que $\mathcal{P}_A$ é um grupo abeliano. Mais precisamente,

G1 **Elemento neutro**: O polinômio nulo $\mathbf{0} = (0,0,0,\ldots)$ é tal que $\mathbf{O} + P = P + \ = P$ qualquer que seja $P \in \mathcal{P}_A$. Logo, $\mathbf{0}$ é o elemento neutro.

G2 **Inverso aditivo**: Se $P = (a_0, a_1, a_2, \ldots) \in \mathcal{P}_A$ então $-P = (-a_0, -a_1, -a_2, \ldots) \in \mathcal{P}_A$ é tal que $P + (-P) = \mathbf{0}$. Logo, todo polinômio admite inverso aditivo.

G3 **Associatividade**: Sejam $P_1 = (a_0, a_1, a_2, \ldots)$, $P_2 = (b_0, b_1, b_2, \ldots)$ e $P_3 = (c_0, c_1, c_2, \ldots)$ polinômios em $\mathcal{P}_A$.

Desde que

$$(a_i + b_i) + c_i = a_i + (b_i + c_i)$$

em A segue que $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$.

G4 **Comutatividade**: Analogamente, a comutatividade em $\mathcal{P}_A$ decorre diretamente da comutatividade em A.

Com relação à multiplicação:

M1 **Associatividade**: Sejam $A = (a_0, a_1, a_2, \ldots)$, $B = (b_0, b_1, b_2, \ldots)$ e $C = (c_0, c_1, c_2, \ldots)$ polinômios em $\mathcal{P}_A$. Por definição, a n-ésima coordenada do produto $(A.B).C$ é

$$\begin{aligned}
\sum_{i=0}^{n}(A.B)_i.c_{n-i} &= \sum_{i=0}^{n}\left[\sum_{j=0}^{i} a_j b_{i-j}\right] c_{n-i} \\
&= \sum_{i=0}^{n}\sum_{j=0}^{i} a_j b_{i-j} c_{n-i} \\
&= \sum_{u+v+w=n} a_u b_v c_w \quad (u, v, w \geq 0) \quad (*)
\end{aligned}$$

Por outro lado, a n-ésima coordenada do produto $A.(B.C)$ é

$$\begin{aligned}
\sum_{r=0}^{n} a_r (B.C) &= \sum_{r=0}^{n}\left[\sum_{s=0}^{n-r} c_s b_{n-r-s}\right] \\
&= \sum_{r=0}^{n}\sum_{s=0}^{n-r-s} a_r b_s c_{n-r-s} \\
&= \sum_{u+v+w=n} a_u b_v c_w \quad (u, v, w \geq 0) \quad (**)
\end{aligned}$$

Deste modo, $[(A.B).C]_n = [A.(B.C)]_n$ para todo índice n. Isto mostra a associatividade.

- **Distributividade** : Sejam $A, B, C \in \mathcal{P}_A$ como anteriormente. Então,

$$\begin{aligned}
[A.(B+C)]_n &= \sum_{i=0}^{n} a_i.(B+C)_{n-i} \\
&= \sum_{i=0}^{n} a_i.(b_{n-i}+c_{n-i}) \\
&= \sum_{i=0}^{n} a_i.b_{n-i} + a_i c_{n-i} \\
&= \sum_{i=0}^{n} a_i.b_{n-i} + \sum_{i=0}^{n} a_i.c_{n-i} \\
&= A.B + A.C
\end{aligned}$$

  Logo, $A.(B+C) = A.B + A.C$. Do mesmo modo, $(A+B).C = A.C + B.C$.

Isto mostra que $(\mathcal{P}_A, +, \bullet)$ é um anel. Se A tem identidade 1_A, então $(1_A, 0, 0, 0, \ldots) \in \mathcal{P}_A$ é a identidade de $\mathcal{P}_A$ (verifique!) e se A é comutativo então

$$[A.B]_n = \sum_{i=0}^{n} a_i.b_{n-i} = \sum_{i=0}^{n} b_{n-i}a_i = \sum_{i=0}^{n} b_j a_{n-j}.$$

Donde $A.B = B.A$. Isto conclui a demonstração. □

O próximo passo é tornarmos A um subanel de $\mathcal{P}_A$. Lembramos que um subanel de um anel B é um subconjunto $A \subset B$ tal que A é um anel com as operações definidas em B. Se, além disso, B é anel com identidade então é exigido, adicionalmente, que $1_A \in B$. Um anel B é dito uma extensão de um anel A se A é subanel de B. Costuma-se denotar isto simplesmente por $A \subset B$.
Queremos tornar $\mathcal{P}_A$ uma extensão de A de modo que se $a, b \in A$ e P_a, P_b são os polinômios associados aos elementos a e b, respectivamente, então $P_{a+b} = P_a + P_b$ e $P_{ab} = P_a.P_b$. Lembra-se de

homomorfismos de anéis? Desejamos definir um homomorfismo de A em $\mathcal{P}_A$. Uma função $\phi : A \to \mathcal{P}_a$ tal que $\phi(a+b) = \phi(a) + \phi(b)$ e $\phi(a.b) = \phi(a).\phi(b)$. Além disso, se A é um anel comutativo com identidade devemos ter satisfeita a condição $\phi(1_A) = 1_{\mathcal{P}_A}$. Queremos também que Im $\phi \subset \mathcal{P}_A$ seja uma cópia de A. Isto se realiza exigindo-se que o homomorfismo ϕ seja injetivo. Deste modo, A será isomorfo ao anel Im $\phi \subset \mathcal{P}_A$ e então poderemos fazer a identificação $a = \phi(a) = P_a$. Em álgebra, tal procedimento é canônico quando se quer tornar um anel A subanel de outro anel B e não se tem $A \subset B$. Tudo isto resume-se por meio de um teorema.

Teorema 1.3. *Seja $\mathcal{P}_A$ o anel dos polinômios sobre um anel A. Se $A^* \subset \mathcal{P}_A$ é o conjunto de todos os polinômios da forma $(a, 0, 0, 0 \ldots)$, $a \in A$, então A^* é um subanel de $\mathcal{P}_A$ isomorfo à A.*

Prova: Defina a aplicação $\phi : A \to A^*$, $a \mapsto \phi(a) = P_a = (a, 0, 0, 0, \ldots)$. Você mesmo, prezado aluno, pode verificar que ϕ é bijetiva (Faça isto!). Além disso,

$$\phi(a+b) = (a+b, 0, 0, 0, \ldots) = (a, 0, 0, 0, \ldots)+(b, 0, 0, 0, \ldots) = \phi(a)+\phi(b)$$

e

$$\phi(a.b) = (a.b, 0, 0, 0, \ldots) = (a, 0, 0, 0, \ldots).(b, 0, 0, 0, \ldots) = \phi(a).\phi(b).$$

Finalmente, $\phi(1_A) = (1_A, 0, 0, 0, \ldots) = 1_{\mathcal{P}_A}$. Assim, ϕ é um isomorfismo de anéis e caso A tenha identidade, ϕ é um isomorfismo de anéis com identidade. □

Até o momento, estabelecemos os fatos básicos sobre polinômios. Agora, precisamos achar um jeito de exibir um polinômio em sua forma usual. Denotaremos por x ao polinômio $(0, 1, 0, 0, 0, \ldots)$. De acordo com o teorema acima, podemos fazer a identificação

$a := (a, 0, 0, 0, \ldots)$ para cada $a \in A$ e obtermos a inclusão de anéis $A \subset \mathcal{P}_A$. Deste modo, ao escrevermos a estaremos pensando no polinômio $(a, 0, 0, 0, \ldots)$. Com isto em mente vamos analisar as potências x^n de x e os produtos ax^n.
Por definição de potência:

$$\begin{aligned} x^0 = 1_{\mathcal{P}_A} &= (1_A, 0, 0, 0, \ldots) \\ x^1 = x &= (0, 1, 0, 0, 0, \ldots) \\ x^2 = x \cdot x &= (0, 0, 1, 0, 0, 0, \ldots) \end{aligned}$$

e $x^n = x^{n-1} \cdot x$. Supondo $x^{n-1} = (0, \ldots, 0, 1, 0, \ldots)$ com 1 na entrada de índice $n-1$ (hipótese indutiva!) obtemos

$$x^n = x^{n-1} \cdot x = (0, \ldots, 0, 1, 0, \ldots)$$

com 1 na posição de índice n. Logo, por indução segue que

$$X^n = (a_0, a_1, a_2, \ldots, a_n, \ldots)$$

em que $a_n = 1$ e $a_i = 0$ para todo $i \neq n$. Temos ainda

$$\begin{aligned} ax^n &= (a, 0, 0, 0, \ldots) \cdot (a_0, a_1, a_2, \ldots) \\ &= (aa_0, aa_1, aa_2, \ldots, aa_n \ldots) \\ &= (0, 0, 0 \ldots, 0, a, 0, \ldots) \end{aligned}$$

pois $a_n = 1$ e $a_i = 0$ para todo $i \neq n$. Assim, dado um polinômio $(a_0, a_1, a_2, \ldots)$ de grau n em $\mathcal{P}_A$ podemos escrever

$$\begin{aligned} (a_0, a_1, a_2, \ldots) &= (a_0, 0, 0, \ldots) + (0, a_1, 0, \ldots) + \\ &\quad + \cdots + (0, \ldots, 0, a_n, 0, \ldots) \\ &= a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \end{aligned}$$

Pela definição de igualdade de polinômios temos ainda que se $b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$ é uma outra forma de expressar o polinômio $(a_0, a_1, a_2, \ldots)$ então $m = n$ e $a_i = b_i$ para todo índice i. Logo, todo polinômio $(a_0, a_1, a_2, \ldots) \in \mathcal{P}_A$ com grau n se escreve, de maneira única, na forma

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n.$$

OBS 1.2. Nesta forma de expressão para polinômios usamos a notação $A[x]$ em vez de $\mathcal{P}_A$. A notação $A[x]$ é muito mais sugestiva. Por exemplo, se $A = \mathbb{R}$ então podemos ver $A[x]$ como um espaço vetorial sobre $\mathbb{R}$ (você saberia exibir uma base e dizer qual a sua dimensão?). Outra vantagem é que na notação $A[x]$, as operações com polinômios recaem naquelas vistas no ensino médio e fundamental. Nesta notação, costuma-se denotar polinômios pelas letras do alfabeto latino acrescidas de x entre parêntese, isto é, $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = p(x)$, por exemplo.

OBS 1.3. Um elemento ξ é chamado de indeterminada sobre um anel A se as expressões

$$a_0 + a_1\xi + a_2\xi^2 + \cdots + a_n\xi^n$$

estão definidas para todo inteiro não negativo n e a aplicação

$$\varphi : A[x] \to A[\xi]$$

definida por

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mapsto a_0 + a_1\xi + a_2\xi^2 + \cdots + a_n\xi^n$$

define um isomorfismo de anéis.

1.4 Termos e Monômios

Seja A um anel com identidade. Um polinômio da forma ax^n é chamado *termo*. Um termo com coefiente 1 é denominado monômio

ou monomial. Dado um polinômio de grau n

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

define-se:

		Notação
Coeficientes:	$a_0,\ a_1,\ \ldots a_n$	
Termos:	$a_0,\ a_1x,\ \ldots a_nx^n$	
Termo líder:	a_nx^n	LT (f)
Monômio líder:	x^n	LM (f)
Coeficiente líder:	a_n	LC (f)
Termo constante:	a_0	

OBS 1.4. Um polinômio é dito mônico se possui termo líder monomial.

OBS 1.5. Em alguns textos, o adjetivo *líder* é trocado por *dominante* e as definições acima ficam: termo dominante, coeficiente dominante e monômio dominante. Neste texto, usaremos líder em conformidade com uma notação mais universal.

1.5 Conclusão

Na aula de hoje, elaboramos uma definição de polinômios que evita qualquer tipo de expressões vagas e torna clara a noção de indeterminada. Vimos duas representações de um polinômio: por meio de sequências e por meio de uma indeterminada x. A segunda é mais apelativa e preferível perante a primeira. Por exemplo, a estrutura de espaço vetorial de $\mathbb{R}[x]$ sobre $\mathbb{R}$ com base infinita $1,\ x,\ x^2, \ldots$, torna-se muito mais evidente usando indeterminada.

RESUMO

Seja A um anel qualquer (não necessariamente comutativo com identidade).

Definições básicas

Polinômio sobre $A :=$ sequência infinita $(a_0, a_1, a_2, \ldots)$ com $a_i \in A$ na qual todos os elementos a_i^s são nulos exceto para um número finito de termos. Os elementos a_i's são chamados coeficientes do polinômio $(a_0, a_1, a_2, \ldots)$.

$\mathcal{P}_A :=$ conjunto dos polinômios com coeficientes em A.

$(0, 0, 0, \ldots) \in \mathcal{P}_A$ é chamado polinômio nulo.

Grau de Polinômios

$$\deg P = \begin{cases} -\infty, \text{ se } P = 0 \\ n = \max\{n \ : \ a_n \neq 0\}, \text{ se} P \neq 0 \end{cases}$$

Operações em $A[x]$:

Adição:

$(\ldots, a_i, \ldots) + (\ldots, b_i, \ldots) = (\ldots, a_i + b_i, \ldots)$

Multiplicação:

$(\ldots, a_i, \ldots) \cdot (\ldots, b_i, \ldots) = (\ldots, c_i, \ldots)$

onde $c_i = \sum_{j+k=i} a_j b_k$.

Estrutura algébrica: $(\mathcal{P}_A, +, \cdot)$ é um anel.

Quadro comparativo entre a estrutura do anel A e a estrutura do anel $A[x]$

A	$A[x]$
Comutativo	Sim
Com identidade	Sim
Domínio	Sim
Corpo	Não

A Aplicação

$$\begin{aligned} \phi : A &\rightarrow A[x] \\ a &\mapsto (a, 0, 0, 0 \ldots) \end{aligned}$$

define um isomorfismo de A no subconjunto

$$A^* = \{(a, 0, 0, 0, \ldots) : a \in A\} \subset \mathcal{P}_A.$$

Os elementos de A^* são chamados *polinômios constantes* ou de grau zero. (O termo *constante* refere-se ao fato da função associada aos polinômios em A^* serem constantes.

O significado da expressão $a_0 + a_1x + \ldots + a_nx^n$:

Fazendo as identificações:

$$a := (a, 0, 0, 0, \ldots)$$

$$x := (0, 1, 0, 0, 0, \ldots)$$

Pode-se mostrar que

$$x^n = (0, 0, \ldots, 0, 1, 0, \ldots)$$

com deg $x^n = n$. E

$$ax^n = (0, 0, \ldots, 0, a, 0, \ldots)$$

também de grau n. Nestas condições, todo polinômio

$$(a_0, a_1, a_2, \ldots) \in \mathcal{P}_A$$

de grau n pode ser escrito de maneira única na forma:

$$a_0 + a_1x + \dots a_nx^n.$$

Notação: $A[x] := \{p(x) = a_0 + a_1x + \dots a_nx^n : a_i \in A\}$.

A composição de um polinômio

Dado

$$a_0 + a_1x + \dots a_nx^n \in \mathcal{P}_A$$

defini-se

		Notação
Coeficientes:	a_0, a_1, $\dots a_n$	
Termos:	a_0, a_1x, $\dots a_nx^n$	
Termo líder:	a_nx^n	LT (f)
Monômio líder:	x^n	LM (f)
Coeficiente líder:	a_n	LC (f)
Termo constante:	a_0	

PRÓXIMA AULA

Na próxima aula, restringiremos nosso estudo de polinômios para polinômios definidos sobre um corpo. O fato do anel de coeficientes ser um corpo permite definir um algoritmo de divisão no anel de polinômios. Tal algoritmo é o pilar da aritmética dos anéis de polinômios definidos sobre corpos.

ATIVIDADES

ATIV. 1.1. Nos itens abaixo são dados polinômios representados por sequência e pelo uso de indeterminada. Faça a transposição de uma representação para a outra. Em cada caso, determine o grau e o termo líder usando as notações dadas no texto.

a) $(0, 1, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, \ldots)$.

b) $(0, 2, 0, 4, 0, 6, 0, 8, 0, 0, 0, \ldots)$

c) $9x^8 - 3x^5 + x^3 - x + 4$.

d) $(3x - 7)(x^3 - x + 1)$.

ATIV. 1.2. Efetue a operação indicada e simplifique sua resposta. Em cada caso, determine o grau e o termo líder usando as notações usadas no texto.

a) $(x + 2)^3$ em $\mathbb{Z}_3[x]$.

b) $(x + 1)^5$ em $\mathbb{Z}_5[x]$.

c) $(ax + b)^p$ em $\mathbb{Z}_p[x]$, p primo.

d) $(x^2 - 3x + 2)(2x^3 - 4x + 1)$ em $\mathbb{Z}_7[x]$

Sugestão: Nos itens de (a), (b) e (c) use a expansão do binômio de Newton. Note que $(a+b)^p = a^p + b^p$ em $\mathbb{Z}_p$. No item (d) aplique a propriedade distributiva.

ATIV. 1.3. Quais dos seguintes subconjuntos de $A[x]$ são subanéis de $A[x]$?

a) Polinômios com termo constante nulo.

b) $B = \{a_0 + a_1x + \cdots + a_nx^n \ : \ a_i = 0$, para i ímpar $\}$.

c) $B = \{a_0 + a_1x + \cdots + a_nx^n \ : \ a_i = 0$ sempre que i for par $\}$

ATIV. 1.4. Mostre que se A é um domínio de integridade então $A[x]$ é um dominio de integridade. Se k é um corpo então $k[x]$ também é um corpo?

Sugestão: Para a primeira parte, suponha $A[x]$ não domínio e mostre que A necessariamente não é domínio. Para a segunda, mostre que x não admite inverso multiplicativo em $A[x]$, isto é, a igualdade $g(x).x = 1$ para $g(x) \in A[x]$ conduz à uma contradição.

ATIV. 1.5. Considere a aplicação $\varphi : A \to A[x]$ definida por $\varphi(a) = (0, a, 0, 0, 0 \ldots)$. Tal aplicação é um homomorfismo de anéis?

Sugestão: Repare se a igualdade $\varphi(a.b) = \varphi(a).\varphi(b)$ é ou não satisfeita.

ATIV. 1.6. Mostre que o grau de polinômios satisfaz às seguintes propriedades:

i) $\deg p(x) + q(x) \leq \max \{ \deg f(x), \deg q(x)\}$

ii) $\deg p(x)q(x) = \deg p(x) + \deg q(x)$, se A é domínio.

iii) Dê um exemplo com desigualdade estrita no item (i) e caracterize quando ocorre tal desigualdade.

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.

KAPLANSKY, I., Introdução à teoria de Galois, Notas de Matemática nº 13, IMPA, 1966.

AULA

Algoritmo da divisão em $k[x]$ 2

META:

Introduzir um algoritmo de divisão para anéis de polinômios definidos sobre corpos.

OBJETIVOS:

Ao fim da aula os alunos deverão ser capazes de:
Aplicar o algoritmo da divisão para determinar o quociente e o resto na divisão entre polinômios.
Conceituar função polinomial e zeros de uma função polinomial.
Estabelecer a diferença entre polinômios e funções polinomiais.
Enunciar e provar o teorema do resto e do fator.

PRÉ-REQUISITOS

A estrutura de anel para polinômios. Embora não seja necessário, os conhecimentos do ensino médio sobre divisão de polinômios, funções polinomiais, teorema do resto e do fator e uma revisão sobre o algoritmo da divisão para os inteiros ajudariam num melhor rendimento desta aula.

2.1 Introdução

Nesta aula, partiremos do seu conhecimento do ensino médio e fundamental sobre divisão de polinômios e formalizaremos tal método em forma de um algoritmo. A unicidade do quociente e do resto e o fato do resto ser nulo ou possuir grau estritamente menor que o grau do divisor são as propriedades fundamentais deste algoritmo. A última propriedade é de extrema importância teórica e terá profundas consequências no estudo de polinômios. A primeira delas é o teorema do fator e do resto já conhecido por você do ensino médio. As outras veremos na aula seguinte. Convém lembrar que $\mathrm{LT}(g)$ denota o termo líder do polinômio g.

OBS 2.1. Ao longo deste curso, a menos que seja dito o contrário, usaremos a letra k para denotar um corpo.

2.2 O Algoritmo da divisão em $k[x]$

Sejam $f(x) = 3x^5 + 2x^4 + 2x^3 + 4x^2 + x - 2$ e $g(x) = 2x^3 + 1$ dois polinômios em $\mathbb{Q}[x]$. Para dividir f por g, obtemos o primeiro termo do quociente $\dfrac{3x^5}{2x^3} = \dfrac{3}{2}x^2$. Este é o resultado da divisão dos termos dominantes de f e g. A diferença

$$f(x) - \frac{3}{2}x^2 g(x) = r_1(x) = 2x^4 + 2x^3 + \frac{5}{2}x^2 + x - 2$$

nos fornece o primeiro resto parcial. Repetindo este procedimento para $r_1(x)$ no lugar de $f(x)$ obtemos o segundo resto parcial

$$r_2(x) = r_1(x) - xg(x) = 2x^3 + \frac{5}{2}x^2 - 2.$$

Note que $\deg f(x) > \deg r_1(x) > \deg r_2(x)$. Podemos aplicar este procedimento enquanto o grau do resto for menor do que o grau de $g(x)$. Ao fazer isto, obtemos uma sequência de restos $r_1, r_2, r_3, \ldots$ na qual

$$\deg r_1 > \deg r_1 > \deg r_2 > \deg r_3 > \dots$$

Se deg $f >$ deg g então, após no máximo $k = \deg f - \deg g + 1$ passos, devemos ter deg $r_k <$ deg g. Assim, $f(x) = g(x).q(x) + r(x)$ com $r(x) = r_k(x)$ satisfazendo as condições $r(x) = 0$ ou $0 \geq \deg r(x) < \deg g(x)$. Se deg $f(x) <$ deg $g(x)$ podemos fazer $r(x) = f(x)$ e obter, ainda, $f(x) = g(x).0 + r(x)$ com $r(x) = 0$ ou $0 \geq \deg r(x) < \deg g(x)$. Em forma de algoritmo o que temos é o seguinte:

Input: g, f $(g \neq 0)$
Output: q, r.
$q := 0$; $r = f$
Enquanto $r \neq 0$ e LT(g) dividir LT(r) faça

$$q := q + \text{LT}(r)/\text{LT}(g)$$
$$r := r - [\text{LT}(r)/\text{LT}(g)]\, g$$

O grau do dividendo r, em cada passo, é estritamente menor que o grau do dividendo do passo anterior. Assim, o algoritmo termina no máximo em deg $f -$ deg $g + 1$ passos. Isto mostra a existência de q e r tais que

$$f = qg + r$$

com $r = 0$ ou $0 \leq \deg r \leq \deg g$. Podemos, ainda, mostrar que o quociente $q(x)$ e o resto $r(x)$, assim obtidos, são únicos. De fato, suponham q_1, q_2 dois quocientes e r_1, r_2 dois restos para uma mesma divisão de f por g com os restos satisfazendo as condições acima. Então,

$$q_1 g + r_1 = f = q_2 g + r_2$$

donde $(q_1 - q_2)g = r_2 - r_1$. Se $q_1 \neq q_2$, então, $q_1 - q_2 \neq 0$. Assim,

$$\deg r_2 - r_1 = \deg (q_1 - q_2)g = \deg (q_1 - q_2) + \deg g \geq \deg g$$

e isto é uma contradição, pois, ambos r_1 e r_2 têm graus menor do que o grau de g. Logo, $q_1 = q_2$ e, portanto,

$$r_1 - r_2 = (q_1 - q_2)g = 0g = 0$$

donde $r_1 = r_2$. O resultado que acabamos de provar é chamado *algoritmo da divisão*. Segue o enunciado em forma de teorema.

Teorema 2.1. *(Algoritmo da divisão) Seja k um corpo e $f(x), r(x) \in k[x]$ com $g(x) \neq 0$. Então, existem únicos polinômios $q(x), r(x) \in k[x]$ tais que*

$$f(x) = q(x)g(x) + r(x)$$

com $r(x) = 0$ ou $0 \leq$ deg $r(x) <$ deg $g(x)$. □

Prezado aluno, caso você não tenha se convencido da existência de q e r em forma de algoritmo, segue a prova convencional.

Prova: (Existência) Se $f(x) = 0$ ou deg $f <$ deg $g(x)$ faça $r(x) = f(x)$ e $q(x) = 0$. Suponha deg $f(x) \geq$ deg $g(x)$. Neste caso, procederemos por indução em deg $f(x)$. O polinômio $h(x) = f(x) - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)}g$ tem grau menor que o polinômio f (seus termos dominantes são iguais). Por hipótese indutiva, existem $q'(x), r'(x) \in k[x]$ tais que

$$h(x) = f(x) - \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)}g = q'(x)g(x) + r'(x)$$

com $r'(x) = 0$ ou $0 \leq$ deg $r'(x) <$ deg $g(x)$. Assim,

$$f(x) = \left(q'(x) + \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)}\right)g + r'(x).$$

Então, $q(x) = q'(x) + \frac{\mathrm{LT}(f)}{\mathrm{LT}(g)}$ e $r(x) = r'(x)$ satisfazem as propriedades requeridas.

Exemplo 2.1. Vamos determinar o quociente e o resto da divisão

de $f(x) = 3x^4 - 2x^3 + 6x^2 - x + 2$ por $g(x) = x^2 + x + 1$ em $\mathbb{Q}[x]$.

$$\begin{array}{ll} 3x^4 - 2x^3 + 6x^2 - x + 2 & \underline{\mid x^2 + x + 1} \\ \underline{-3x^2 - 3x^3 - 3x^2} & 3x^2 - 5x + 8 \\ -5x^3 + 3x^2 - x + 2 & \\ \underline{5x^3 + 5x^2 + 5x} & \\ 8x^2 + 4x + 2 & \\ \underline{-8x^2 - 8x - 8} & \\ -4x - 6 & \end{array}$$

Resposta: Quociente: $3x^2 - 5x + 8$; Resto: $-4x - 6$.

2.3 O teorema do resto e do fator

Seja $A \subset B$ uma extensão de anéis. Uma função $f : A \to B$ é dita polinomial se existem $a_0, a_1, \ldots, a_n \in A$ tais que

$$f(a) = a_0 + a_1 a + \cdots a_n a^n$$

para todo $a \in A$. Um elemento $a \in A$ tal que $f(a) = 0$ é chamado zero da função f. Seja

$$p(x) = a_0 + a_1 x + \cdots a_n x^n \in A[x]$$

o polinômio associado à função polinomial f. A relação entre polinômios e funções polinomiais é sultil e merece algum comentário. Para todo polinômio

$$q(x) = b_0 + b_1 x + \cdots b_m x^m \in A[x]$$

está associado uma função polinomial $f\ A \to A$ definida por $f(a) = q(a)$ onde $q(a)$ denota a operação $b_0 + b_1 a + \cdots b_m a^m$ em A. Assim, $q(a) = b_0 + b_1 a + \cdots b_m a^m$ equivale a substituir a no lugar de x em $q(x)$ (tal operação não está definida no anel de polinômios).

Um elemento $a \in A$ tal que $q(a) = 0$ é chamado *raiz* do polinômio $q(x)$. A sultileza aqui é que funções polinomiais e polinômios são objetos distintos. A correspondência

$$\{\text{polinômios em } A[x]\} \overset{\Psi}{\leftrightarrow} \{\text{Funções polinomiais}\}$$

embora seja sempre sobrejetiva não é em geral injetiva. É o que mostra o exemplo abaixo.

Exemplo 2.2. Em $\mathbb{Z}_2[x]$ o polinômio $f(x) = x^2 + 1$ não é nulo, mas a função polinomial $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ é a função nula.

Exemplo 2.3. Os polinômios $p(x) = x^4+x+1, q(x) = x^3+x^2+1 \in \mathbb{Z}_3[x]$ definem as funções polinomiais $f : \mathbb{Z}_3 \to \mathbb{Z}_3$, $f(r) = r^4+r+1$ e $g : \mathbb{Z}_3 \to \mathbb{Z}_3$, $g(t) = t^3 + t^2 + 1$. Tem-se $f(0) = 1 = g(0)$, $f(1) = 0 = g(1)$ e $f(2) = 1 = g(2)$. Assim, $f(r) = g(r)$ para todo $r \in \mathbb{Z}_3$. Logo, f e g definem a mesma função em $\mathbb{Z}_3$ embora, como polinômios, sejam distintos.

Teorema 2.2. (Teorema do resto) *O resto da divisão de um polinômio $f(x) \in k[x]$ por $x - a$ é $f(a)$.*

Prova: Existem únicos $q(x), r(x) \in k[x]$ tais que

$$f(x) = q(x)(x - a) + r(x)$$

com $r(x) = 0$ ou $0 \leq \deg r(x) < \deg (x - a) = 1$. Então, $r(x) = 0$ ou $\deg r(x) = 0$. Assim, $r(x)$ necessariamente é uma constante $c \in k$. Da igualdade acima segue a igualdade

$$f(a) = q(a)(a - a) + c = c = r(x). \quad \square$$

Teorema 2.3. (Teorema do fator) *Seja $f(x) \in k[x]$. Um elemento $a \in k$ é uma raiz de $f(x)$ se e somente se $x - a$ divide $f(x)$.*

Prova: Seja $r(x)$ o resto da divisão de $f(x)$ por $x - a$. Pelo teorema do resto, tem-se $r(x) = f(a)$. Assim, a é raiz de $f(x) \Leftrightarrow f(a) = r(x) = 0 \Leftrightarrow x - a$ divide $f(x)$. $\square$

2.4 Conclusão

Nesta aula, implementamos um algoritmo de divisão em $k[x]$ semelhante àquele dos números inteiros. Como consequência imediata, obtivemos a relação fundamental entre os zeros de uma função polinomial e os fatores lineares da forma $x-a$ do polinômio que a define; a saber: o teorema do resto e do fator. A respeito do que diz estes resultados, podemos extrair duas importantes conclusões. Primeira, um polinômio admite sempre um número finito de raízes tendo seu grau como cota superior. Segunda, a existência de raízes para um polinômio é relativa ao anel de coeficientes em que se considera o polinômio. Por exemplo, x^2+1 não possui raízes reais, mas admite duas raízes em $\mathbb{C}$.

RESUMO

Algoritmo da divisão em $k[x]$

Input: g, f $\quad (g \neq 0)$
Output: q, r.
$q := 0$; $r = f$
Enquanto $r \neq 0$ e LT(g) dividir LT(r) faça

$$q := q + \text{LT}(r)/\text{LT}(g)$$
$$r := r - [\text{LT}(r)/\text{LT}(g)]\, g$$

Em forma de teorema:
Seja k um corpo e $f(x), r(x) \in k[x]$ com $g(x) \neq 0$. Então, existem únicos polinômios $q(x), r(x) \in k[x]$ tais que

$$f(x) = q(x)g(x) + r(x)$$

com $r(x) = 0$ ou $0 \leq \deg r(x) < \deg g(x)$.

Funções polinomiais *versus* polinômios

Os polinômios $p(x) = x^4 + x + 1, q(x) = x^3 + x^2 + 1 \in \mathbb{Z}_3[x]$ são distintos mas estão associados à mesma função polinomial.

Análise	Álgebra	Geometria
Funções polinomiais	Polinômios	Gráfico
Zero	Raiz	Interseção com o eixo das abscissas

Teorema do resto

Resto$(p(x), x - a) = p(a)$.

Teorema do fator

$a \in k$ é raiz de $p(x) \in k[x] \iff x - a$ divide $p(x)$.

PRÓXIMA AULA

Na próxima aula estudaremos a aritmética do anel de polinômios $k[x]$. Por meio do algoritmo da divisão, mostraremos que $k[x]$ é um domínio de ideais principais (DIP), isto é, todo ideal de $k[x]$ é principal. Isto acarretará na existência de MDC em $k[x]$ e no fato de $k[x]$ ser um domínio fatorial (DFU).

ATIVIDADES

ATIV. 2.1. Enuncie o algoritmo da divisão em $k[x]$.

ATIV. 2.2. Aplique o algoritmo da divisão para determinar polinômios $q(x)$ e $r(x)$ tais que $f(x) = q(x)g(x) + r(x)$ com $r(x) = 0$ ou $0 \leq \deg r(x) \leq \deg g(x)$.

a) $f(x) = x^3 + x - 1$, $g(x) = x^2 + 1$ em $\mathbb{R}[x]$.

b) $f(x) = x^5 - 1$, $g(x) = x - 1$ em $\mathbb{R}[x]$.

c) $f(x) = x^5 - x^3 + 3x - 5$, $g(x) = x^2 + 7$ em $\mathbb{Q}[x]$.

d) $f(x) = x^5 - x^3 + 3x - 5$, $g(x) = x - 2$ em $\mathbb{Q}[x]$.

e) $f(x) = x^5 - x^3 + 3x - 5$, $g(x) = x + 2$ em $\mathbb{Z}_5[x]$.

f) $f(x) = x^5 - x^3 + 3x - 5$, $g(x) = x^3 + x - 1$ em $\mathbb{Z}_3[x]$.

ATIV. 2.3. Sejam $f(x), g(x) \in \mathbb{Z}[x]$ e $g(x) = b_0 + b_1x + \cdots + b_mx^m$ onde $b_m = 1$. Mostre que existem $q(x), r(x) \in \mathbb{Z}[x]$ tais que $f(x) = q(x)g(x) + r(x)$ onde $r(x) = 0$ ou $0 \leq \deg\,(r(x) \leq \deg\, g(x)$.

ATIV. 2.4. Enuncie e demonstre os teoremas do resto e do fator.

ATIV. 2.5. Seja $\phi : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$ a função definida do seguinte modo:

$$\phi(a_0 + a_1x + \cdots + a_nx^n) = \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_nx^n.$$

Mostre que ϕ é um homomorfismo sobrejetivo de anéis.

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.

AULA

Teoria da divisibilidade Em $k[x]$

3

META:

Obter a propriedade de fatoração única para anéis de polinômios definidos sobre corpos.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Estabelecer os principais conceitos da teoria de divisibilidade para anéis de polinômios: unidades, divisores, divisor de zero, associados, irredutíveis, primos, máximo divisor comum e elementos relativamente primos.

Descrever a estrutura dos ideais em $k[x]$.

Usar os fatos de $k[x]$ ser DIP e DFU na solução de problemas na teoria de polinômios.

Aplicar o algoritmo de Euclides no cálculo de MDC de polinômios.

Expressar o MDC$(f(x), g(x))$ como combinação linear de $f(x)$ e $g(x)$.

Relacionar o MDC$(f(x), g(x))$ e o gerador do ideal gerado por $f(x)$ e $g(x)$.

PRÉ-REQUISITOS

Algoritmo da divisão em $k[x]$. Uma revisão da teoria da divisibilidade em $\mathbb{Z}$ ajudaria na compreensão desta aula.

3.1 Introdução

Prezado aluno, você deve estar familiarizado com a aritmética dos inteiros. A aritmética de $k[x]$, k corpo, é notavelmente semelhante à de $\mathbb{Z}$. Ambos admitem um algoritmo de divisão, máximo divisor comum e fatoração única em primos.

O "'set up"' da aritmética de um anel A reside na noção de divisibilidade: dados $a, b \in A$ dizemos que b divide a se existe $c \in A$ tal que $a = bc$. Desta noção, define-se: unidades, divisores de zero, elementos associados, elementos irredutíveis, elementos primos, mínimo múltiplo comum e máximo divisor comum. Por isso, num nível mais elementar a aritmética é, por vezes, chamada teoria de divisibilidade. Por outro lado, qualquer noção fundamentada na definição de divisibilidade pode ser interpretada via a noção de ideais principais. Para se ter uma idéia, um elemento a é dito associado a $b \overset{\text{def}}{\leftrightarrow} a|b$ e $b|a \leftrightarrow (a) = (b)$ onde $(x) = \{ax \mid a \in A\}$ denota o ideal principal gerado por x. Assim, em DIP's, aritmética, teoria de divisibilidade e estudo dos ideais principais são equivalentes e o uso de um dos termos depende apenas do ponto de vista. O primeiro reflete o da teoria dos números enquanto que o último o da álgebra abstrata. Esta aula trata justamente da teoria de divisibilidade do anel de polinômios em uma indeterminada sobre um corpo k. A idéia central é fazer um paralelo com a teoria já conhecida dos inteiros.

Na seção 3.2 são apresentadas as definições necessárias para a leitura do capítulo corrente. Sem tê-las em mente fica impossível compreender as idéias contidas neste capítulo. É aconselhável que num primeiro contato com álgebra, a cada palavra que remonte à uma definição, o aluno pare a leitura e relembre mentalmente a definição a fim de certifica-se que sua leitura esteja sendo ativa e

não meramente como a de um romance.

Na seção 3.3 descreveremos a estrutura dos ideais em $k[x]$. Mostraremos que todo ideal em $k[x]$ é principal, isto é, $k[x]$ é DIP. Finalmente, na seção 3.4 mostraremos a existência de MDC em $k[x]$ através do algoritmo de Euclides também conhecido como algoritmo das divisões sucessivas. Tal algoritmo ainda nos permite escrever o MDC como uma combinação dos fatores.

3.2 Glossário

1. **Divisibilidade:** um elemento $b \in A$ divide um elemento $a \in A$ em A se existe $c \in A$ tal que $a = bc$. Neste caso, diz-se também que a é múltiplo de b, b é divisor de a ou b é um fator de a.

2. **Unidade:** divisor da identidade; elemento $a \in A$ tal que $ab = 1_A$ para algum $binA$; elemento $a \in A$ para o qual a equação $ax = 1_A$ admite solução em A. Em um anel não trivial ($1_A \neq 0_A$) toda unidade é não nula. Pode-se mostrar que o elmento $b \in A$ tal que $ab = 1_A$ é único. Este elemento é chamado inverso de a e denotado por a^{-1}. Denotaremos por $\mathbb{U}(A)$ ao conjunto das unidades em A. (Exemplo: $\mathbb{U}(\mathbb{Z}_n) = \{\overline{x} \ : mdc(x, n) = 1\}$)

3. **Inversível:** o mesmo que unidade.

4. **Divisor de zero:** elemento $a \in A$ tal que existe elemento não nulo $b \in A$ tal que $ab = 0$; elemento $a \in$ para o qual a equação $ax = 0$ admite solução não trivial ($\neq 0$); elemento $a \in A$ tal que o endomorfismo $A \to A$, $x \mapsto ax$ admite núcleo não trivial (equivalentemente, é não injetivo).

5. **Nilpotente:** elemento $a \in A$ para o qual existe inteiro positivo n tal que $a^n = 0$. O menor inteiro positivo n tal que $a^n = 0$ é chamado *índice de nilpotência*.

6. **Elementos associados:** elementos $a, b \in A$ tais que $a|b$ e $b|a$. Em domínios, isto é equivalente a dizer que $a = ub$ para alguma unidade $u \in A$.

7. **Divisor trivial:** unidades e associados à um elemento.

8. **Divisor próprio:** divisor não trivial de um elemento. Exemplo: $\mathbb{U}(\mathbb{Z}_{12}) = \{1, 5, 7, 11\}$. Logo, 2 é um divisor trivial de 10 pois é um de seus associados. Por outro lado, 3 é divisor próprio de 6 pois $3|6$ com 3 não unidade e nem associado de 6.

9. **Elemento irredutível:** elemento não unidade $a \in A$ cujos divisores são seus associados ou unidades.

10. **Elemento redutível:** elemento não unidade que não é irredutível. Em outras palavras, elemento que possui divisores próprios.

11. **Elemento primo:** elemento não unidade $p \in A$ para o qual vale a seguinte propriedade: $p|ab \Rightarrow p|a$ ou $p|b$.

12. **Máximo divisor comum (MDC):** o máximo divisor comum de $a_1, \ldots, a_r \in A$ (não todos nulos) é um elemento $d \in A$ tal que

    i) $d|a_i$ para todo i, $1 \leq i \leq r$.

    ii) Se $c \in A$ divide cada a_i então $c|d$.

13. **Elementos relativamente primos:** Elementos cujo MDC é 1.

14. **Domínio de fatoração única (DFU):** domínio A no qual todo elemento não nulo e não unidade $a \in A$ satisfaz as seguintes condições:

    i) $a = p_1, \cdots p_r$, $p_i \in A$ irredutível para todo i, $1 \leq i \leq r$.

    ii) Se $a = q_1 \cdots q_s$ é uma outra fatoração com cada q_i irredutível então $r = s$ e, a menos de uma reordenação nos índices, p_i é associado à q_i para cada i, $1 \leq i \leq r$.

15. **Domínio de ideais principais (DIP):** domínio no qual todo ideal é principal.

16. **Domínio Euclidiano:** domínio A no qual está definido uma função $\delta : A^* \to \mathbb{Z}_{\geq 0}$ satisfazendo as seguintes propriedades:

    i) Se $a, b \in A$ são não nulos então $\delta a \leq \delta(ab)$.

    ii) Se $a, b \in A$ e $b \neq 0$ então existem $q, r \in A$ tais que $a = bq + r$ com $r = 0$ ou $0 \leq \delta(r) \leq \delta(b)$. Exemplo: a função módulo juntamente com o algoritmo da divisão em $\mathbb{Z}$ define em $\mathbb{Z}$ uma estrutura de domínio euclidiano. A notação A^* indica o conjunto dos elementos não nulos de A e $\mathbb{Z}_{\geq 0}$ é o conjunto dos inteiros não negativos.

3.3 Ideais em $k[x]$

Um ideal de um anel A é um subconjunto $I \subset A$ tal que $(I, +)$ é subgrupo aditivo de $(A, +)$ e $ax \in I$ sempre que $a \in A$ e $x \in I$. Um ideal $I \subset A$ é dito principal se $I = (a)$ para algum $a \in A$ onde $(a) = \{ax : x \in A\}$.

Teorema 3.1. *$k[x]$ é DIP.*

Prova: Seja $I \subset k[x]$ um ideal. Se $I = (0)$ é o ideal nulo nada temos a provar. Suponhamos I não nulo. Considere o conjunto

$$S = \{ \text{ deg } f \ : \ f \in I\}$$

Desde que $I \neq 0$, existe $f \in I$, $f \neq 0$. Então, $S \subset \mathbb{Z}_{\geq 0}$ é não vazio. Pelo Princípio da Boa Ordem existe $f(x) \in I$ tal que deg f é mínimo dentre os graus de todos os polinômios em I. Vamos mostrar que $I = (f(x))$. A inclusão $(f(x)) \subset I$ segue da definição de ideal visto que $f(x) \in I$. Seja $g(x) \in I$. Pelo algoritmo da divisão, existem $q(x), r(x) \in k[x]$ tais que

$$g(x) = q(x)f(x) + r(x)$$

com $r(x) = 0$ ou $0 \leq \text{deg } r(x) < \text{deg } f(X)$. Ora, se $r(x) \neq 0$ então $r(x) = g(x) - q(x)f(x) \in I$ (pois $g(x), q(x)f(x) \in I$) com deg $r(x) <$ deg $f(x)$. Isto contradiz a minimalidade de deg $f(x)$. Logo, $r(x) = 0$ e $g(x) = q(x)f(x) \in (f(x))$. Assim, $I \subset (f(x))$ donde $I = (f(x))$.

3.4 MDC em $k[x]$

A existência de MDC em $k[x]$ é uma consequência direta do fato de $k[x]$ ser DIP.

Teorema 3.2. (Existência de MDC) *Sejam $f(x), g(x) \in k[x]$. Então, MDC$(f(x), g(x))$ existe e é único a menos de um produto por uma constante não nula em k.*

Prova: Considere $(f(x), g(x)) \subset k[x]$ o ideal gerado por $f(x)$ e $g(x)$. Desde que $k[x]$ é DIP, existe $d(x) \in k[x]$ tal que $(d(x)) = (f(x), g(x))$. Vamos mostrar que $d(x) = \text{MDC}(f(x), g(x))$. Primeiramente, $d(x)|f(x)$ e $d(x)|g(x)$ pois, $f(x), g(x) \in (f(x), g(x)) =$

$(d(x))$. Suponha $h(x) \in k[x]$ tal que $h(x)|f(x)$ e $h(x)|g(x)$. Então, $f(x) = h(x)q_1(x)$ e $g(x) = h(x)q_2(x)$. Desde que $d(x) \in (f(x), g(x))$ existem $r(x), s(x) \in k[x]$ tais que $d(x) = r(x)f(x) + s(x)g(x)$. Logo,

$$\begin{aligned} d(x) &= r(x)f(x) + s(x)g(x) \\ &= r(x)h(x)q_1(x) + s(x)h(x)q_2(x) \\ &= h(x)\left[r(x)q_1(x) + s(x)q_2(x)\right] \end{aligned}$$

donde $h(x)|d(x)$. Resta mostrar a unicidade a menos de uma multiplicação por uma constante não nula. Suponham $d_1(x), d_2(x)$ sob as condições de serem um máximo divisor comum de $f(x)$ e $g(x)$. Por definição de MDC segue que $d_1(x)|d_2(x)$ e $d_2(x)|d_1(x)$. Logo, $d_1(x) \sim d_2(x)$ donde $d_1(x) = ud_2(x)$ com $u \in \mathbb{U}(k[x]) = k \setminus 0$. □

OBS 3.1. O teorema acima nos mostra que o MDC de dois polinômios $f, g \in k[x]$ é um gerador do ideal (f, g). Embora este resultado tenha relevância teórica ele não nos ensina como obter o MDC de $f(x)$ e $g(x)$. A rigor, deveríamos determinar o polinômio de menor grau escrito como combinação linear de $f(x)$ e $g(x)$. Na prática, isto torna-se impraticável. Felizmente, existe um algoritmo clássico, conhecido como Algoritmo Euclidiano, para computar o MDC de dois polinômios. Este algoritmo é fundamentado no resultado a seguir.

Lema 3.1. *Sejam $f(x), g(x) \in k[x]$. Se $f(x) = q(x)g(x) + r(x)$ com $q(x), r(x) \in k[x]$ então $MDC(f(x), g(x)) = MDC(g(x), r(x))$.*

Prova: Usaremos noções de ideais e a verificação das inclusões ficarão como exercícios. A relação $f(x) = q(x)g(x) + r(x)$ fornece-nos as inclusões de ideais $(f) \subset (g, r)$ e $(r) \subset (f, g)$. Logo,

$(f,g) \subset (g,r) \subset (f,g)$. Assim, $(\text{MDC}(f,g)) = (f,g) = (g,r) = (\text{MDC}(g,r))$ donde $\text{MDC}(f,g) = \text{MDC}(g,r)$. $\square$

Eis o Algoritmo Euclidiano para computar $\text{MDC}(f,g)$:

Input: f, g

Output: h

$h := f$

$s := g$

Enquanto $s \neq 0$ faça

$r :=$ resto (h, s)

$h := s$

$s := r$

Caso o leitor não tenha visualizado, este algoritmo é aquele visto no ensino fundamental e chamado método das divisões sucessivas. De fato, dados $f, g \in k[x]$, $g \neq 0$, o algoritmo nos fornece:

Passo	Resultado
0	$h_0 = f$, $s_0 = g$ e $f = q_0 g + r_0$, $r_0 = \text{resto}(f,g)$.
1	$h_1 = s_0 = g$, $s_1 = r_0$ e $g = q_1 r_0 + r_1$, $r_1 = \text{resto}(g, r_0)$.
2	$h_2 = r_0$, $s_2 = r_1$ e $r_0 = q_2 r_1 + r_2$, $r_2 = \text{resto}(r_0, r_1)$.
3	$h_3 = r_1$, $s_3 = r_2$ e $r_1 = q_3 r_2 + r_3$, $r_3 = \text{resto}(r_1, r_2)$.
	$\vdots$

Pela propriedade do resto, tem-se uma sequência estritamente decrescente de inteiros não negativos

$$\deg r_0 > \deg r_1 > \deg r_2 > \ldots.$$

Usando o princípio da boa ordem pode-se mostrar (verifique!) que em algum passo, necessariamente, deveremos ter um resto nulo, digamos no passo $n+1$. Deste modo,

Passo	Resultado
n	$h_n = r_{n-2}$, $s_n = r_{n-1}$ e $r_{n-2} = q_n r_{n-1} + r_n$.
$n+1$	$h_{n+1} = r_{n-1}$, $s_{n+1} = r_n$ e $r_{n-1} = q_{n+1} r_n + 0$.

onde $r_{n+1} = \text{resto}(r_{n-1}, r_n) = 0$. Pelo Lema 3.1, $\text{MDC}(f, g) = \text{MDC}(g, r_0) = \text{MDC}(r_0, r_1) = \ldots = \text{MDC}(r_{n-1}, r_n) = \text{MDC}(r_n, 0) = r_n$.

OBS 3.2. Outra propriedade também importante de tal algoritmo é que nos permite expressar o $\text{MDC}(f, g)$ como uma combinação linear entre f e g. De fato, basta retroceder aos passos do algoritmo para determinar $r, s \in k[x]$ tais que $\text{MDC}(f, g) = rf + sg$. Vejamos um exemplo para ilustrar tais idéias.

Exemplo 3.1. Vamos calcular o MDC entre $f(x) = x^4 - x^3 - x^2 + 1$ e $g(x) = x^3 - 1$ e expressá-lo como uma combinação linear de $f(x)$ e $g(x)$. Seguindo os passos do algoritmo obtém-se:

$$x^4 - x^3 - x^2 + 1 = (x-1)(x^3-1) - x^2 + x \quad (3.1)$$

$$x^3 - 1 = (-x-1)(-x^2+x) + x - 1 \quad (3.2)$$

$$-x^2 + x = -x(x-1) \quad (3.3)$$

Assim, $\text{MDC}\,(f(x), g(x)) = x - 1$. Vamos agora expressar o MDC obtido como combinação linear de $f(x)$ e $g(x)$. Isolando $x - 1$ na equação 3.2 tem-se:

$$x - 1 = x^3 - 1 - (-x-1)(-x^2+x) \quad (3.4)$$

Por outro lado, isolando $-x^2 + x$ na equação 3.1 e substituindo na equação 3.4 obtém-se:

$$\begin{aligned} x-1 &= x^3-1-(-x-1)(-x^2+x) \\ &= x^3-1-(-x-1)\left[x^4-x^3-x^2+1-(x-1)(x^3-1)\right] \\ &= \left[1+(-x-1)(x-1)\right](x^3-1)- \\ &\quad (-x-1)(x^4-x^3-x^2+1) \\ &= (-x^2+2)(x^3-1)+(x+1)(x^4-x^3-x^2+1) \end{aligned}$$

3.5 MDC $\not\Rightarrow$ DIP

Em geral, todo DIP admite MDC. Neste exemplo, mostraremos que a recíproca não é verdadeira por exibir um anel com MDC que não é DIP. Considere $\mathbb{Z}[x]$ e $2, x \in \mathbb{Z}[x]$. Vamos mostrar que o ideal $(2, x)$ não é principal. Suponha, por absurdo, que existe $p(x) \in \mathbb{Z}[x]$ tal que $(2, x) = (p(x))$. Então, existiriam $r(x), s(x) \in \mathbb{Z}[x]$ tais que

$$p(x) = r(x).2 + s(x).x$$

Por outro lado $2 \in (2, x) = (p(x))$ donde $2 = p(x)q_1(x)$. Assim, $0 = \deg 2 = \deg p(x) + \deg q_1(x)$ donde $\deg p(x) = 0$. Logo, $p(x) = c \in \mathbb{Z}$ é um polinômio constante. Analogamente, $x = p(x)q_2(x)$ para algum $q_2(x) \in \mathbb{Z}[x]$. Assim, $1 = \text{LC } x = c.\text{LC } q_2(x)$ (onde LC denota o coeficiente líder). Conclusão: $c \in \mathbb{U}(\mathbb{Z}) = \{\pm 1\}$ (onde $\mathbb{U}(A)$ denota o conjunto das unidades de A). Podemos considerar $c = 1$ (Por quê?). Assim,

$$1 = p(x) = r(x).2 + s(x).x$$

Isto é um absurdo (você sabe por quê?). Logo, tal $p(x)$ não existe.

OBS 3.3. O domínio $\mathbb{Z}[x]$ não é um DIP. Mas, pode-se mostrar se A é DFU então $A[x]$ é DFU (a prova disto está além das pretensões

deste texto!). Como $\mathbb{Z}$ é DFU então $\mathbb{Z}[x]$ é DFU. Logo, admite MDC. Seja $d(x) = \text{MDC } (2, x)$ (você saberia mostrar que $d(x) = 1$?). Por definição de MDC, $(2, x) \subset (d(x)) = (1) = \mathbb{Z}[x]$ mas $d(x) = 1 \notin (2, x)$, pois $(2, x)$ não é principal. Assim, MDC $(2, x)$ não pode ser escrito como combinação linear de 2 e x.

3.6 Irredutíveis e Fatoração única em $k[x]$

Seja A um anel. Lembramos que um elemento $a \in A$ é dito irredutível se não admite divisores próprios. Em outras palavras, se $b|a$ então ou b é unidade ou $b \sim a$. No caso de domínios, $a \sim b$ se e somente se $a = ub$ com u uma unidade. Em nosso caso, $k[x]$ é domínio. Então, dizer que $p(x)$ é associado a $q(x)$ é equivalente a dizer que $p(x) = cq(x)$ para algum $c \in k$, isto é, $p(x)$ e $q(x)$ diferem por uma constante. Comecemos por investigar os elementos irredutíveis de $k[x]$. Mostraremos que polinômios irredutíveis são elementos primos em $k[x]$ - esta é uma condição básica para um anel ser DFU. Precisaremos do seguinte fato elementar visto em Estruturas Algébricas I: em um domínio euclidiano A (ou em que vale o algoritmo euclidiano) se $a|bc$ e MDC $(a, b) = 1$ então $a|c$ (você sabe provar isto?).

Lema 3.2. *Irredutíveis em $k[x]$ são elementos primos.*

Prova: Seja $p(x) \in k[x]$ irredutível. Pela definição de elemento primo, devemos mostrar que se $p(x)|f(x)g(x)$ então $p(x)|f(x)$ ou $p(x)|g(x)$. Suponha $p(x)|f(x)g(x)$ com $p(x) \not| f(x)$. Por definição de irredutível, o fato de $p(x)$ não dividir $f(x)$ implica que $p(x)$ e $f(x)$ são relativamente primos. Assim, $p(x)|f(x)g(x)$ com MDC $(p(x), f(x)) = 1$. Então, $p(x)|g(x)$ como queríamos demonstrar. □

OBS 3.4. Pelo lema acima, se $p(x)$ é irredutível e $p(x)$ divide o produto $q_1(x)\cdots q_r(x)$ então $p(x)$ divide um dos fatores $q_i(x)$ para algum i, $1 \leq i \leq r$ (pode-se provar isto usando-se recursivamente o lema ou por indução no número de fatores). Deste modo, sempre que tivermos $p_1(x), \ldots, p_r(x)$ e $q_1(x), \ldots, q_s(x)$ irredutíveis com

$$p_1(x)\cdots p_r(x) = q_1(x)\cdots q_s(x)$$

poderemos supor $p_1|q_1$ a menos de uma permutação nos índices.

Teorema 3.3. *(Fatoração única em $k[x]$) Seja k um corpo. Todo polinômio não constante $f(x) \in k[x]$ é um produto de polinômios irredutíveis em $k[x]$. Esta fatoração é única a menos de uma constante não nula, isto é, se*

$$f(x) = p_1(x)\cdots p_r(x) \quad e \quad f(x) = q_1(x)\cdots q_s(x)$$

são duas fatorações em irredutíveis de $f(x)$ então $r = s$ e, a menos de uma permutação nos índices, $p_i = u_i q_i$ com $u_i \in k$, $u_i \neq 0$, para todo i, $1 \leq i \leq r$.

Prova: (Existência) Seja $f(x) \in k[x]$ um polinômio não constante. Usaremos indução em $\deg f(x) = n \geq 1$. Se $\deg f(x) = 1$ então $f(x)$ é irredutível (todo polinômio de grau 1 é irredutível). Suponhamos o teorema verdadeiro para todo polinômio de grau $< n$. Se $f(x)$ é irredutível então nada temos a provar pois $f(x) = 1.f(x)$ que um produto de irredutíveis com somente um fator (permissível em nosso contexto). Se $f(X)$ é redutível então, por definição, $f(x) = g(x)h(x)$ com $\deg g(x) < n$ e $\deg h(x) < n$. Por hipótese indutiva, $g(x) = u_1 p_1 \cdots p_r$ e $h(x) = u_2 p_{r+1} \cdots p_k$ com $u_1, u_2 \in k$. Pondo $u = u_1 u_2$ temos $f(x) = u p_1 \cdots p_k$ como queríamos.
(Unicidade) Sejam $f(x) = u_1 p_1 \cdots p_r$ e $f(x) = u_2 q_1 \cdots q_s$ duas

fatorações de f em irredutíveis. Se $r \neq s$ podemos supor, sem perda de generalidade, $r < s$. Então, a menos de uma permutação nos índices, $p_1 \sim q_1$, $p_2 \sim q_2$, ..., $p_r \sim q_r$. Assim, $p_1 \cdots p_r = cq_1 \cdots q_r q_{r+1} \cdot q_s$ donde $q_{r+1} \cdots q_s = u \in k$ donde $q_{r+1}, \ldots, q_s$ são unidades. Isto contradiz a irredutibilidade de $q_{r+1}, \ldots, q_s$. Logo, $r = s$ e $p_i \sim q_i$ para todo i, $1 \leq i \leq r$. $\square$

3.7 Irredutibilidade *versus* raízes de funções polinomiais

As noções de irredutibilidade e zeros de funções polinomiais são antagônicas. Para que um polinômio (de grau > 1) seja irredutível sobre um corpo k não é suficiente mas é necessário que ele não admita raízes em k (teorema do fator). Em linguagem simbólica:

$$\text{irredutibilidade sobre } k \Rightarrow \text{ não existência de raízes em } k.$$

A recíproca não é verdadeira. Considere dois polinômios quadráticos $f(x), g(x) \in \mathbb{R}[x]$ sem raízes em $\mathbb{R}$. Então, $h(x) = f(x)g(x)$ não admite raízes reais e, no entanto, é redutível.
A não equivalência da implicação acima não a desfavorece teoricamente. Sua contrapositiva é de grande utilidade teórica e nos fornece um critério de redutibilidade para polinômios de grau ≤ 2. É importante também ressaltar que para polinômios de grau 2 e 3 a implicação acima torna-se uma equivalência. Todas estas observações são decorrentes dos teoremas do resto e do fator.

3.8 Conclusão

Estruturalmente, a teoria da divisibilidade em $k[x]$, k corpo, é idêndica à de $\mathbb{Z}$. Ambos são domínios euclidianos. Apenas a função

norma difere. Em $\mathbb{Z}$ é dada pela função módulo $a \mapsto |a|$ e em $k[x]$, pela função grau $f(x) \mapsto \deg f(x)$. Consequentemente, tanto a teoria de ideais quanto a existência e o cálculo do MDC também são idênticos. Em geral, todo domínio euclidiano é um DIP e admite MDC.

RESUMO

Ideais em $k[x]$

$$\boxed{I \subset k[x] \text{ ideal} \Rightarrow I = (f(x)) \text{ para algum } f(x) \in k[x]}$$

O elemento $f(x)$ que gera o ideal I é um polinômio de menor grau em I.

MDC em $k[x]$

$$\boxed{k[x] \text{ DIP} \Rightarrow \text{Existe MDC em } k[x]}$$

De fato, todo gerador de um ideal não nulo $(f(x), g(x))$ (existe pois $k[x]$ é DIP) é um MDC de $f(x)$ e $g(x)$. A recíproca é também verdadeira para domínios euclidianos. Deste modo, em domínios euclidianos, embora o MDC não seja único, quaisquer dois são associados. Assim, em $k[x]$, existe um único MDC mônico. Alguns textos definem o MDC em $k[x]$ como este representante mônico nesta classe de equivalência e garante, já na definição, a unicidade do MDC.

Algoritmo Euclidiano

Input: f, g

Output: h

$h := f$

$s := g$

Enquanto $s \neq 0$ faça

$r :=$ resto (h, s)

$h := s$

$s := r$

Quadro comparativo entre a teoria de divisibilidade de $\mathbb{Z}$, $k[x]$ e $\mathbb{Z}[x]$.

$\mathbb{Z}$	$k[x]$	$\mathbb{Z}[x]$
Comutativo	Sim	Sim
Com identidade	Sim	Sim
Domínio	Sim	Sim
Euclidiano	Sim	**Não**
DIP	Sim	**Não**
DFU	Sim	Sim
$\exists$ MDC	Sim	Sim
MDC pode ser escrito como combinação linear	Sim	**Não**

OBS 3.5. Em geral, tem-se as seguintes inclusões (todas próprias):

Domínios euclidianos $\subset$ DIP $\subset$ DFU.

Irredutibilidade *versus* raízes de funções polinomiais

irredutibilidade sobre $k \Rightarrow$ não existência de raízes em k.

A recíproca não é verdadeira: x^2+1 não possui raízes reais donde $(x^2+1)^2$ também não possui raízes reais, mas é redutível. Contudo, vale a recíproca para polinômios de grau 2 e 3.

Fatoração única em $k[x]$

$$k \text{ corpo } \Rightarrow k[x] \text{ DFU}$$

PRÓXIMA AULA

Focalizaremos o estudo de irredutibilidade no anel de polinômios definidos sobre o corpo dos racionais. Mostraremos que a irredutibilidade em $\mathbb{Z}[x]$ é suficiente para a irredutibilidade em $\mathbb{Q}[x]$.

ATIVIDADES

ATIV. 3.1. Classifique e caracterize os elementos em $k[x]$ quanto a cada definição dada no glossário.

ATIV. 3.2. Mostre que a noção de elementos associados define uma relação de equivalência em $k[x]$. Verifique que para cada classe de equivalência existe um único representante mônico.

ATIV. 3.3. Determine todos os polinômios irredutíveis de grau 2 e 3 em $\mathbb{Z}_2[x]$.

ATIV. 3.4. Calcule MDC $(f(x), g(x))$ em $\mathbb{Q}[x]$ para os pares de polinômios nos itens abaixo. Expresse o MDC como combinação linear entre os pares de polinômios dados.

a) $f(x) = x^3 - 6x^2 + x + 4$; $g(x) = x^5 - 6x + 1$.

b) $f(x) = x^2 + 1$; $g(x) = x^6 + x^3 + x + 1$.

ATIV. 3.5. Mostre que o MDC é único a menos de um fator constante não nulo. Em outras palavras, mostre que $d_1(x), d_2(x)$ são MDC de $f(x)$ e $g(x)$ se e somente se $d_1(x) \sim d_2(x)$. Deste modo, existe um único MDC mônico.

ATIV. 3.6. Verifique que a igualdade $1 = r(x)2 + s(x)x$ é um absurdo quaisquer que sejam $r(x), s(x) \in k[x]$

ATIV. 3.7. Mostre que se $p(x)|f(x)g(x)$ e MDC $(p(x), f(x)) = 1$ então $p(x)|g(x)$.

ATIV. 3.8. Mostre que se $p(x)$ é irredutível e $p(x) \not| f(x)$ então $p(x)$ e $f(x)$ são relativamente primos. Conclua que irredutíveis em $k[x]$ são primos.

ATIV. 3.9. Demonstre a implicação: irredutibilidade sobre $k \Rightarrow$ não existência de raízes em k. Mostre a recíproca para polinômios de grau 2 e 3.

ATIV. 3.10. Mostre que todo polinômio de grau 1 é irredutível sobre $k[x]$.

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.

AULA

Irredutibilidade em $\mathbb{Q}[x]$

4

META:

Fundamentar a busca de critérios de irredutibilidade em $\mathbb{Z}[x]$ para mostrar irredutibilidade em $\mathbb{Q}[x]$.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Definir polinômios primitivos em $\mathbb{Z}[x]$.

Enunciar o lema de Gauss.

Mostrar que um polinômio primitivo é irredutível em $\mathbb{Z}[x]$ se e somente se é irredutível em $\mathbb{Q}[x]$.

PRÉ-REQUISITOS

As definições de raiz de polinômio, máximo divisor comum e elemento irredutível.

4.1 Introdução

Nesta aula, restringiremos nosso estudo de polinômios ao conjunto $\mathbb{Q}[x]$. Focalizaremos sobre os elementos irredutíveis. Pela relação entre redutibilidade e existência de raízes, começaremos por caracterizar as raízes racionais de um polinômio em $\mathbb{Q}[x]$. Este é o teste da raiz racional. Na seção 4.2, abordaremos o conceito de conteúdo de um polinômio com coeficientes inteiros e provaremos o resultado fundamental a cerca deste; a saber: o teorema de Gauss. Na seção que segue, provaremos o lema de Gauss, nosso principal resultado desta aula. Finalmente, fecharemos a aula colhendo o fruto de tanto esforço. Concluiremos que irredutibilidade em $\mathbb{Q}[x]$ pode ser obtida por meio de irredutibilidade em $\mathbb{Z}[x]$.

4.2 Teste da raiz racional

Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ um polinômio de grau $n \geq 1$. Seja $\frac{r}{s}\mathbb{Q}$ uma raiz não nula de $f(x)$. Podemos assumir $\frac{r}{s}$ nos menores termos, isto é, MDC $(r, s) = 1$. Por definição de raiz,

$$f(\frac{r}{s}) = a_0 + a_1\frac{r}{s} + \cdots r_n\frac{a^n}{s^n} = 0.$$

Multiplicando ambos os termos da igualdade acima por s^n obtém-se:

$$f(\frac{r}{s}) = a_0s^n + a_1rs^{n-1} + \cdots a_{n-1}r^{n-1}s + a_nr^n = 0.$$

Assim,

$$\begin{aligned} -a_0s^n &= a_1rs^{n-1} + \cdots a_{n-1}r^{n-1}s + a_nr^n \\ &= r\left(a_1s^{n-1} + \cdots a_{n-1}r^{n-2}sa_nr^{n-1}\right) \end{aligned}$$

e

$$\begin{aligned} -a_n a^n &= a_0 s^n + a_1 r s^{n-1} + \cdots a_{n-1} r^{n-1} s \\ &= s\left(a_1 s^{n-2} + \cdots a_{n-1} r^{n-2}\right) \end{aligned}$$

As duas últimas equações acarretam $r|a_0 s^n$ e $s|a_n r^n$. Mas, MDC $(r,s) = 1$ implica MDC $(r^n, s) =$ MDC $(r, s^n) = 1$. Logo, $r|a_0$ e $s|a_n$. Podemos resumir este resultado na forma de um teorema.

Teorema 4.1. *(Teste da raiz racional) Seja $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ um polinômio com coeficientes inteiros. Se um número racional não nulo $\frac{r}{s}$ com MDC $(r,s) = 1$ é raiz de $f(x)$, então $r|a_0$ e $s|a_n$.*

Exemplo 4.1. As possíveis raízes em $\mathbb{Q}$ de $f(x) = 2x^4 + x^3 - 21x^2 - 14x + 12$ são da forma $\frac{r}{s}$ com $r \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$ e $s \in \{\pm 1, \pm 2\}$. Assim,

$$\frac{r}{s} \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm\frac{1}{2}, \pm\frac{3}{2}\}$$

Pode-se verificar que -3 e $\frac{1}{2}$ são as únicas raízes racionais de $f(x)$. Usando o teorema do fator obtém-se:

$$f(x) = (x+3)(x - \frac{1}{2})(2x^2 - 4x - 8).$$

Exemplo 4.2. As únicas raízes racionais possíveis do polinômio $f(x) = x^3 + 4x^2 + x - 1$ são ± 1. Mas, $f(1) = 5$ e $f(-1) = 1$. Logo, $f(x)$ não possui raízes em $\mathbb{Q}$. Como deg $f(x) = 3$ segue que $f(x)$ é irredutível sobre $\mathbb{Q}$.

4.3 O conteúdo de um polinômio

O contéudo de um polinômio não nulo $f(x) = a_0 + a_1 x + \cdots a_n x^n \in \mathbb{Z}[x]$ é o MDC de seus coeficientes. Um polinômio é dito primitivo

se possui conteúdo igual a 1.

Notação: $\text{cont}(f(x)) = \text{MDC } (a_0, a_1 \ldots, a_n)$.

O "set up" no estudo do conteúdo de polinômios reside no seguinte fato: se um primo $p \in \mathbb{Z}$ divide todos os coeficientes de um produto $f(x)g(x)$ de polinômios em $\mathbb{Z}[x]$ então p divide todos os coeficientes de $f(x)$ ou p divide todos os coeficientes de $g(x)$.

Teorema 4.2. *(Gauss) Seja $p \in \mathbb{Z}$ primo e $f(x) = a_0 + a_1x + \cdots + a_nx^n$ e $g(x) = b_0 + b_1x + \cdots b_mx^m$ dois polinômios em $\mathbb{Z}[x]$ não nulos. Seja $h(x) = f(x)g(x) = c_0 + c_1x + \cdots c_{n+m}x^{n+m}$. Se $p|c_i$ $(0 \leq i \leq n+m)$ então $p|a_i$ $(0 \leq i \leq n)$ ou $p|b_i$ $(0 \leq i \leq m)$.*

Prova: (Redução ao absurdo) Suponha que existam i_0, j_0 tais que $p \not| a_{i_0}$ e $p \not| b_{j_0}$. Sejam a_r e b_s os primeiros coeficientes de $f(x)$ e $g(x)$ (a contar de c_0 e b_0), respectivamente, não divisíveis por p. Pela escolha de r e s, $p|a_i$ $0 \leq i < r$ e $p|b_j$ $0 \leq j < s$. Então,

$$c_{r+s} = a_0b_{r+s} + \cdots a_{r-1}b_{s+1} + a_rb_s + a_{r+1}b_{s-1} + \cdots a_{r+s}b_0$$

é tal que $p|c_{r+s}$ por hipótese e $p|a_0, \ldots, a_{r-1}, b_0, \ldots, b_{s-1}$ pela escolha de r e s. Logo, $p|a_rb_s$. Como p é primo (hipótese) devemos ter $p|a_r$ ou $p|b_s$, absurdo. $\square$

OBS 4.1. Se $cf(x) = g(x)h(x)$, $f(x), g(x), h(x) \in \mathbb{Z}[x]$, então $f(x) = \pm\tilde{g}(x)\tilde{h}(x)$ com $\tilde{g}(x), \tilde{h}(x) \in \mathbb{Z}[x]$, deg $\tilde{g}(x) =$ deg $g(x)$ e deg $\tilde{h}(x) =$ deg $h(x)$. Aplique a lei do cancelamento em domínios juntamente com o teorema anterior para todos os fatores primos de c.

4.4 Lema de Gauss

Dados $f(x) = x^4 - 4x^3 + 6x - 2$ e $g(x) = 5x^3 + 6x - 3$ temos $\text{cont}(f) = 1$ e $\text{cont}(g) = 1$. Assim, ambos f e g são primitivos. Por outro lado,

$$f(x).g(x) = 5x^7 - 20x^6 + 6x^5 + 3x^4 + 2x^3 + 36x^2 - 30x + 6$$

e $\text{cont}(fg) = 1$. Este resultado não é mera coincidência e sim uma regra. Se considerarmos dois polinômios primitivos, o produto será sempre primitivo. Em outras palavras, a noção de primitivo é preservada pelo produto. Este resultado é conhecido como lema de Gauss.

OBS 4.2. Se a é um inteiro positivo e $f(x) \in \mathbb{Z}[x]$ então $\text{cont}(af) = a.\text{cont}(f)$. Em particular, se $d = \text{cont}(f)$ então $\frac{1}{d}f$ é primitivo.

Teorema 4.3. *(Lema de Gauss) O produto de polinômios primitivos é um polinômio primitivo. Mais geralmente, o conteúdo do produto é o produto dos conteúdos.*

Prova: Sejam $f(x), g(x) \in \mathbb{Z}[x]$ primitivos e $d = \text{cont}(fg)$. Queremos provar que $d = 1$. Suponha $d \neq 1$. Existe ao menos um primo p tal que $p|d$. Por definição de MDC, p divide todos os coeficientes de fg. Pelo teorema 4.2, p divide todos os coeficientes de f ou p divide todos os coefientes de g. Logo, $p \mid \text{cont}(f)$ ou $p \mid \text{cont}(g)$, isto é, $p|1$, uma contradição. Assim, $d = 1$. Para finalizar, sejam $f(x), g(x) \in \mathbb{Z}$ polinômios quaisquer e d_1,d_2 seus respectivos conteúdos. Então, $\frac{1}{d_1}f$ e $\frac{1}{d_2}g$ são primitivos donde

$\left(\frac{1}{d_1}f\right)\left(\frac{1}{d_2}g\right) = \frac{1}{d_1 d_2}fg$ é também primitivo. Assim,

$$\begin{aligned}\text{cont}(fg) &= \text{cont}\left[d_1 d_2\left(\frac{1}{d_1 d_2}fg\right)\right] \\ &= d_1 d_2.\text{cont}\left(\frac{1}{d_1 d_2}fg\right) \\ &= d_1 d_2.1 = d_1 d_2 = \text{cont}(f)\text{cont}(g). \quad \square\end{aligned}$$

4.5 Irredutibilidade em $\mathbb{Q}[x] \Leftrightarrow$ irredutibilidade em $\mathbb{Z}[x]$

A equivalência acima precisa de algumas ressalvas. Primeiro, a noção de irredutibilidade é relativa e não absoluta. Por exemplo, 2 é um polinômio irredutível em $\mathbb{Z}[x]$, mas é unidade em $\mathbb{Q}[x]$ e $2x-4$ é redutível em $\mathbb{Z}[x]$, mas é irredutível em $\mathbb{Q}[x]$. Segundo, um polinômio com coeficientes em $\mathbb{Q}[x]$ não pode ser considerado um polinômio em $\mathbb{Z}[x]$. Deste modo, para a equivalência acima fazer sentido devemos considerar polinômios primitivos.

Seja $f(x) \in \mathbb{Z}[x]$ primitivo. Obviamente, irredutibilidade em $\mathbb{Q}[x]$ implica irredutibilidade em $\mathbb{Z}[x]$ (raciocine por contrapositiva!).

Suponha $f(x)$ redutível em $\mathbb{Q}[x]$, isto é, $f(x) = g(x)h(x)$ com $g(x), h(x) \in \mathbb{Q}[x]$ e $\deg g(x), \deg h(x) < \deg f(x)$. Existem inteiros a e b tais que $ag(x), bh(x) \in \mathbb{Z}[x]$. Então, $abf(x) = (ag(x))\,(bh(x))$ é uma fatoração de $abf(x)$ em $\mathbb{Z}[x]$. Denotando $c = ab$ e $\tilde{g}(x) = ag(x)$ e $\tilde{h}(x) = bh(x)$ temos $cf(x) = \tilde{g}(x)\tilde{h}(x)$. Segue da observação 4.1 que $f(x) = \pm\tilde{g}(x)\tilde{h}(x)$ com $\deg \tilde{g}(x) = \deg g(x) < \deg f(x)$ e $\deg \tilde{h}(x) = \deg h(x) < \deg f(x)$. Assim, $f(x)$ redutível em $\mathbb{Q}[x]$ implica $f(x)$ redutível em $\mathbb{Z}[x]$. Temos provado o seguinte:

Teorema 4.4. *Um polinômio primitivo em $\mathbb{Z}[x]$ é irredutível em $\mathbb{Z}[x]$ se e somente se é irredutível em $\mathbb{Q}[x]$.*

OBS 4.3. Dado $f(x) \in \mathbb{Q}[x]$, existe um inteiro c tal que $cf(x) \in \mathbb{Z}[x]$. Temos $f(x)$ redutível em $\mathbb{Q}[x]$ se e somente se $cf(x)$ irredutível em $\mathbb{Q}[x]$. Assim, com respeito à redutibilidade em $\mathbb{Q}[x]$ podemos sempre supor o polinômio em $\mathbb{Z}[x]$. Ademais, como redutibilidade é invariante pela noção de associados e sobre corpos sempre existe associado mônico (único) podemos também supor $f(x)$ primitivo. Pelo teorema anterior, $f(x)$ irredutível em $\mathbb{Z}[x]$ implica $f(x)$ irredutível em $\mathbb{Q}[x]$. Deste modo, se quisermos provar que um polinômio $f(x)$ em $\mathbb{Q}[x]$ é irredutível (em $\mathbb{Q}[x]$) é suficiente provar a irredutibilidade em $\mathbb{Z}[x]$ de um polinômio primitivo em $\mathbb{Z}[x]$ associado à $f(x)$ em $\mathbb{Q}[x]$. É neste fato que reside a importância de se elaborar critérios de irredutibilidade em $\mathbb{Z}[x]$.

4.6 Conclusão

Por meio do conceito de conteúdo de um polinômio com coeficientes inteiros, concluimos que o estudo dos irredutíveis em $\mathbb{Q}[x]$ está incluído no estudo dos irredutíveis em $\mathbb{Z}[x]$. Daí a necessidade de se obter critérios de irredutibilidade em $\mathbb{Z}[x]$.

RESUMO

Teste da raiz racional

> Se um número racional $\frac{a}{b}$, MDC$(a,b) = 1$, é raiz de $a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ então $a|a_0$ e $b|a_n$.

O conteúdo de um polinômio

1. **Definição:** cont $(a_0+a_1x+\cdots+a_nx^n) = \text{MDC}\,(a_0,\ldots,a_n)$.
2. **Polinômio primitivo:** polinômio de conteúdo 1.

3. **Teorema:** (Gauss) Se um primo p divide todos os coeficientes de um produto de polinômios então p divide todos os coeficientes de um dos fatores.

Lema de Gauss

$$\text{cont}(f(x)g(x)) = \text{cont}(f(x))\text{cont}(g(x)).$$

Irredutibilidade em $\mathbb{Q}[x]$ *versus* **Irredutibilidade em $\mathbb{Z}[x]$**

Para polinômios primitivos vale a equivalência

$$\text{Irredutibilidade em } \mathbb{Z}[x] \Leftrightarrow \text{Irredutibilidade em } \mathbb{Q}[x].$$

Consequência:

Seja $f(x) \in \mathbb{Q}[x]$ e $\tilde{f}(x)$ seu associado mônico em $\mathbb{Z}[x]$. Então, $\tilde{f}(x)$ irredutível em $\mathbb{Z}[x]$ implica $f(x)$ irredutível em $\mathbb{Q}[x]$.

PRÓXIMA AULA

Seguindo a motivação dos resultados obtidos nesta aula, buscaremos critérios de irredutibilidade em $\mathbb{Z}[x]$.

ATIVIDADES

ATIV. 4.1. Use o teste da raiz racional para escrever cada polinômio como um produto de polinômios irredutíveis em $\mathbb{Q}[x]$.

a) $3x^5 + 2x^4 - 7x^3 + 2x^2$.

b) $2x^4 - 5x^3 + 3x^2 + 4x - 6$.

ATIV. 4.2. Mostre que $\sqrt{p}$ é irracional para cada p primo.

ATIV. 4.3. Mostre que todo polinômio não nulo $f(x) \in \mathbb{Q}[x]$ pode ser escrito de maneira única na forma $f(x) = c\tilde{f}(x)$ com $c \in \mathbb{Q}$ e $\tilde{f}(x) \in \mathbb{Z}(x)$ primitivo. Conclua que todo polinômio em $\mathbb{Q}[x]$ possui um único associado mônico em $\mathbb{Z}[x]$.

ATIV. 4.4. Seja $f(x) \in \mathbb{Z}(x)$ primitivo. Mostre que se $f(x)$ é redutível em $\mathbb{Q}(x)$ então $f(x)$ é redutível em $\mathbb{Z}(x)$.

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.

AULA

Critérios de irredutibilidade Em $\mathbb{Z}[x]$

5

META:

Determinar critérios de irredutibilidade em $\mathbb{Z}[x]$ para mostrar irredutibilidade em $\mathbb{Q}[x]$.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:
Aplicar os critérios de irredutibilidade para determinar se um dado polinômio com coeficientes inteiros é irredutível em $\mathbb{Q}[x]$.

PRÉ-REQUISITOS

A definição de isomorfismo de anéis e a noção de polinômio irredutível.

5.1 Introdução

Considere $f(x) = x^4 - 5x^2 + 1 \in \mathbb{Q}[x]$. Vamos testar a redutibilidade de $f(x)$ em $\mathbb{Q}[x]$? Pela aula anterior, é suficiente testarmos a redutibilidade de $f(x)$ em $\mathbb{Z}[x]$. As possíveis combinações dos graus para fatorações de $f(x)$ são da forma 1.1.1.1, 1.1.2, 1.3 e 2.2. As três primeiras implicam (pelo teorema do fator) na existência de pelo menos uma raiz racional. Pelo teste da raiz racional, as únicas possíveis raízes de $f(x)$ em $\mathbb{Q}[x]$ são $1, -1$. Mas, $f(1) = f(-1) = -3 \neq 0$. Logo, $f(x)$ não possui raízes em $\mathbb{Q}$ e, portanto, não possui fatores de grau 1. Deste modo, a única maneira de fatoração para $f(x)$ seria na forma

$$f(x) = (a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0), \quad a_0, a_1, b_0, b_1 \in \mathbb{Z}$$

No entanto, $f(x)$ é mônico e isto acarreta $a_2 = b_2 = 1$ (você consegue enxergar isto?). Assim temos:

$$f(x) = (x^2 + a_1x + a_0)(x^2 + b_1x + b_0).$$

Efetuando este produto obtemos:

$$x^4+(a_1+b_1)x^3+(a_0+a_1b_1+b_0)x^2+(a_1b_0+a_0b_1)x+a_0b_0 = x^4-5x^2+1$$

Da igualdade de polinômios, obtemos o seguinte sistema em $\mathbb{Z}$:

$$a_1 + b_1 = 0 \quad a_0 + a_1b_1 + b_0 = -5 \quad a_1b_0 + a_0b_1 = 0 \quad a_0b_0 = 1$$

Mas, $a_0b_0 = 1$ em $\mathbb{Z}$ acarreta $a_0 = b_0 = 1$ ou $a_0 = b_0 = -1$ e $a_1 + b_1 = 0$ acarreta $a_1 = -b_1$. Então, da equação

$$a_0 + a_1b_1 + b_0 = -5$$

podemos concluir que

$$a_1^2 - 1 - 1 = 5 \quad \text{ou} \quad a_1^2 + 1 + 1 = 5$$

donde $a_1^2 = 7$ ou $a_1^2 = 3$. Como não existem inteiros cujo quadrados são 3 ou 7 segue a impossibilidade de fatorar $f(x)$ em $\mathbb{Z}[x]$. Assim, $f(x)$ é irredutível em $\mathbb{Z}[x]$, logo também em $\mathbb{Q}[x]$.
Observe, prezado aluno, que a tarefa de caracterizar irredutibilidade pela definição é impraticável. Por exemplo, você saberia discutir a irredutibilidade do polinômio $x^{17}+6x^{13}-15x^4+3x^2-9x+12$ em $\mathbb{Q}[x]$? Imagine quantas combinações possíveis existem para se fatorar tal polinômio. Felizmente, existem critérios muito eficazes para nos auxiliar nesta tarefa. É o que nos ensina os critérios de irredutibilidade a seguir.

5.2 Critério de Eisenstein

Seja $f(x) = a_0 + a_1x + \ldots a_nx^n \in \mathbb{Z}[x]$ não constante. Suponha que existe um primo $p \in \mathbb{Z}$ tal que $p|a_0, \ldots, p|a_{n-1}$, $p \nmid a_n$ e $p^2 \nmid a_0$. Vamos mostrar, nestas condições, que $f(x)$ é irredutível em $\mathbb{Q}[x]$. Seguiremos o raciocínio por redução ao absurdo. Suponhamos $f(x)$ redutível em $\mathbb{Q}[x]$ e um primo p nas condições acima. Pela aula anterior, $f(x)$ admitiria uma fatoração em $\mathbb{Z}[x]$, digamos

$$f(x) = (b_0 + b_1x + \cdots + b_rx^r)(c_0 + c_1x + \cdots + c_sx^s)$$

com $b_i, c_j \in \mathbb{Z}$, $1 \leq r < n$ e $1 \leq s < n$. Temos a seguinte sequência de implicações:

1. $p|a_0$, $a_0 = b_0c_0$ e p primo $\Rightarrow p|b_0$ ou $p|c_0$. Podemos supor $p|b_0$.

2. $p \nmid a_n$, $a_n = b_rc_s \Rightarrow p \nmid b_r$ e $p \nmid c_s$.

3. $p^2 \nmid a_0$, $a_0 = c_0b_0$ e $p|b_0 \Rightarrow p \nmid c_0$.

4. $p|b_0$ e $p \nmid b_r \Rightarrow$ existe um menor inteiro k, $1 \leq k \leq r$, tal que $p \nmid p_k$.

O inteiro k, determinado no item 4, tem a seguinte propriedade:

$$p|b_i, \quad 0 \leq i < k, \quad \text{e} \quad p \nmid b_k$$

com $1 \leq k \leq r < n$. Desde que

$$a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0$$

temos

$$b_kc_0 = a_k - b_0c_k - b_1c_{k-1} + \cdots - b_{k-1}c_1 \tag{5.5}$$

Mas, $p|a_k$ $(k < n)$ e $p|b_i$, para $i < k$. Então p divide cada parcela do membro direito da equação 5.5 e, portanto, $p|b_kc_0$. Isto implica $p|b_k$ e $p|c_0$, um absurdo. Este resultado é conhecido como critério de Eisenstein. Segue o enunciado em forma de teorema.

Teorema 5.1. *(Critério de Eisenstein) Seja* $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ *não constante. Se existe um primo* $p \in \mathbb{Z}$ *tal que* $p|a_0,\ldots,p|a_{n-1}$, $p \nmid a_n$ *e* $p^2 \nmid a_0$, *então,* $f(x)$ *é irredutível em* $\mathbb{Q}[x]$. □

Exemplo 5.1. O polinômio $x^{17}+6x^{13}-15x^4+3x^2-9x+12$ dado na introdução é irredutível em $\mathbb{Q}[x]$ pelo critério de Eisenstein para $p = 3$. Os polinômios da forma $x^n - p$ são irredutíveis pelo critério de Eisenstein para p primo.

5.3 Critério $\mathbb{Z}_p[x]$

Embora o critério de Eisenstein seja bastante eficiente, existem muitos polinômios para os quais o critério não se aplica. Por exemplo, $f(x) = x^5 + 8x^4 + 3x^2 + 4x + 7$. Neste caso, precisamos

desenvolver um novo método. Para todo inteiro n está definido o homomorfismo de anéis de polinômios

$$\varphi_n : \mathbb{Z}[x] \to \mathbb{Z}_n[x]$$

em que para cada polinômio $f(x) = a_0 + a_1x + \cdots a_rx^r$ associa o polinômio $\varphi_n(f(x)) = \overline{a}_0 + \overline{a}_1x + \cdots + \overline{a}_rx^r$ onde $\overline{a}_i$ denota a classe de equivalência de a_i no anel quociente $\mathbb{Z}_n$. Usaremos este homomorfismo para p primo. Assim, o anel quociente $\mathbb{Z}_p$ é um corpo e podemos então aplicar toda a teoria desenvolvida até aqui para anéis polinomiais sobre corpos.

Seja $f(x) = a_0 + a_1x + \cdots a_nx^n \in \mathbb{Z}[x]$ de grau n. Considere um primo p tal que $p \nmid a_n$. Então, $\varphi_p(f(x))$ é um polinômio em $\mathbb{Z}_p[x]$ de grau n visto que $\overline{a}_n \neq \overline{0}$ pois $p \nmid a_n$. Vamos mostrar que se $\varphi_p(f(x))$ é irredutível em $\mathbb{Z}_p[x]$ então $f(x)$ é irredutível em $\mathbb{Z}[x]$. Usaremos a contrapositiva. Se $f(x)$ é redutível em $\mathbb{Z}[x]$ então $f(x) = g(x)h(x)$ com $g(x), h(x)$ polinômios não constantes em $\mathbb{Z}[x]$ de graus menores do que n, digamos r e s, respectivamente. Se b_r e c_s são os coeficientes líderes de $g(x)$ e $h(x)$, respectivamente, então $a_n = b_rc_s$. Como $p \nmid a_n$, então, $p \nmid b_r$ e $p \nmid c_s$. Assim, $\overline{b}_r$ e $\overline{c_s}$ são não nulos em $\mathbb{Z}_p$. Então, deg $\varphi_p(g(x))$ = deg $g(x)$ e deg $\varphi_p(h(x))$ = deg $h(x)$. Como $\varphi_p(f(x)) = \varphi_p(g(x))\varphi_p(h(x))$ segue que $\varphi_p(f(x))$ é redutível em $\mathbb{Z}_p[x]$. Temos demonstrado o seguinte resultado:

Teorema 5.2. *Seja $f(x) \in \mathbb{Z}[x]$ um polinômio não constante e seja p um primo que não divida o coeficiente líder de $f(x)$. Se $\varphi_p(f(x))$ é irredutível em $\mathbb{Z}_p[x]$ então $f(x)$ é irredutível em $\mathbb{Q}[x]$.*
□

Exemplo 5.2. Vamos mostrar que $f(x) = x^5 + 8x^4 + 3x^2 + 4x + 7$ é irredutível em $\mathbb{Q}[x]$. Para $p = 2$ temos $\varphi_2(f(x)) = x^5 + x^2 + 1$.

$\varphi_p(f(x))$ não admite fatores lineares em $\mathbb{Z}_2[x]$, pois não possui raízes em $\mathbb{Z}_2$ (verifique isto). Os únicos polinômios de grau dois em $\mathbb{Z}_2[x]$ são x^2, x^2+x, x^2+1 e x^2+x+1 e nenhum destes divide $\varphi_p(f(x))$ (use o algoritmo da divisão para verificar isto!). Assim, $f(x)$ também não admite fatores quadráticos em $\mathbb{Z}_2[x]$. Finalmente, $\varphi_p(f(x))$ também não admite fatores de grau 3 e 4 pois se tivesse o outro fator seria de grau 2 ou 1, que é impossível. Logo, $\varphi_p(f(x))$ é irredutível em $\mathbb{Z}_2[x]$. Pelo teorema 5.2 $f(x)$ é irredutível em $\mathbb{Q}[x]$.

5.4 Critério $f(x+c)$

Seja $f(x) \in k[x]$ e $c \in k$. A aplicação $\Psi : k[x] \to k[x]$, $\Psi(f(x)) = f(x+c)$, define um isomorfismo. Assim, $f(x)$ é irredutível em $k[x]$ se e somente se $\Psi(f(x)) = f(x+c)$ é irredutível em $k[x]$. Em forma de teorema:

Teorema 5.3. *Seja $f(x) \in k[x]$, k corpo, e $c \in k$. Se $f(x+c)$ é irredutível em $k[x]$ se e somente se $f(x)$ é irredutível em $k[x]$.* □

Tal critério aparentemente não traz nenhuma luz à caracterização da irredutibilidade de um polinômio. Mas, ele aplicado em conjunto com outros critérios pode ser bastante útil. Por exemplo, considere $f(x) = x^4+4x+1 \in \mathbb{Q}[x]$. Temos $f(x+1) = (x+1)^4+4(x+1)+1 = x^4+4x^3+6x^2+8x+6$ irredutível pelo critério de Eisenstein para $p = 2$. Logo, x^4+4x+1 é irredutível em $\mathbb{Q}[x]$. Prezado aluno, você pode fazer o teste de irredutibilidade tentando fatorar tal polinômio como foi feito na introdução à esta aula e verificar qual dos dois métodos é o mais trabalhoso. Outro exemplo segue na seção a seguir.

5.5 O polinômio ciclotômico $\Phi_p(x)$, p primo

Em matemática, a palavra *ciclotomia* remonta ao problema histórico de dividir o círculo em um dado número de partes iguais ou, equivalentemente, de construir polígonos regulares com régua e compasso. É conhecido que um polígono regular de n lados é construtível (isto significa com régua e compasso) se e somente se $\phi(n)$ é uma potência de 2. Lembramos que $\phi(n)$ denota a função phi de Euler em $n \in \mathbb{Z}_{\geq 0}$ e corresponde à quantidade de inteiros positivos $< n$ relativamente primo com n. Na teoria de grupos, $\phi(n)$ é a ordem do grupo multiplicativo das unidades de $\mathbb{Z}_n$. Pode-se mostrar que $\phi(n)$ é uma potência de 2 se e somente se $n = 2^r p_1 \cdots p_k$ com $p_i = 2^{2^{q_i}} + 1$ primo para todo $i = 1, \ldots, r$. Os primos da forma $2^{2^{q_i}} + 1$ são chamados primos de Fermat (1601-1665). Fermat conjecturou que todos os números da forma $2^{2^q} + 1$ são primos. De fato, $2^{2^q} + 1$ é primo para $q < 5$, mas Euler (1707-1783) mostrou em 1732 que $2^{2^5} + 1 = 641 \times 6.700.417$. Na literatura corrente consta que até o momento não se conhece nenhum primo de Fermat para q acima de 4.

A relação da ciclotomia com nossa aula consiste no fato que dividir o círculo em n arcos iguais é equivalente à construção com régua e compasso da n-ésima raiz complexa da unidade. Um número complexo $\zeta = a + bi$ é dito construtível se o ponto do plano complexo (a, b) é construtível com régua e compasso. Sabe-se que um complexo ζ é construtível somente se o corpo $\mathbb{Q}[\zeta]$ possui como dimensão vetorial sobre $\mathbb{Q}$ uma potência de 2. A dimensão vetorial de $\mathbb{Q}[\zeta]$ sobre $\mathbb{Q}$ é chamada *grau* pelo fato de coincidir com o grau do polinômio mônico irredutível sobre $\mathbb{Q}$ tendo ζ como raiz. Denota-se por $[\mathbb{Q}[\zeta] : \mathbb{Q}]$ o grau de $\mathbb{Q}[\zeta]$ sobre $\mathbb{Q}$. Se $\zeta = \exp^{\frac{2\pi i}{n}}$ é uma n-ésima raiz complexa da unidade então $[\mathbb{Q}[\zeta] : \mathbb{Q}] = \phi(n)$.

A prova deste resultado é não trivial e precisa antes de mais nada determinar o polinômio mínimo de ζ. Tal polinômio é chamado o n-ésimo polinômio ciclotômico e denotado por $\Phi_n(x)$.
Se $\zeta = \exp^{\frac{2\pi i}{n}}$ é uma n-ésima raiz da unidade então $\zeta^n = \exp^{2\pi i} = 1$ donde ζ é raiz do polinômio $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots x + 1)$. Se $\zeta \neq 1$ então ζ é raiz do polinômio $x^{n-1} + x^{n-2} + \cdots x + 1$. Quando $n = p$ é primo, $q(x) = x^{p-1} + x^{p-2} + \cdots x + 1$ é irredutível sobre $\mathbb{Q}$ e portanto é o p-ésimo polinômio ciclotômico $\Phi_p(x)$. De fato, $\dfrac{x^p - 1}{x - 1} = q(x)$. Assim,

$$\begin{aligned} q(x+1) &= \frac{(x+1)^p - 1}{x+1-1} \\ &= \frac{x^p + \begin{pmatrix} p \\ p-1 \end{pmatrix} x^{p-1} + \cdots + \begin{pmatrix} p \\ 1 \end{pmatrix} x + 1 - 1}{x} \\ &= \frac{x^p + \begin{pmatrix} p \\ p-1 \end{pmatrix} x^{p-1} + \cdots + \begin{pmatrix} p \\ 1 \end{pmatrix} x}{x} \\ &= x^{p-1} + \begin{pmatrix} p \\ p-1 \end{pmatrix} x^{p-2} + \cdots + \begin{pmatrix} p \\ 1 \end{pmatrix} \end{aligned}$$

Como p divide $\begin{pmatrix} p \\ r \end{pmatrix}$ para todo r, $0 < r < p$, segue pelo critério de Eisenstein que $q(x) = x^{p-1} + x^{p-2} + \cdots x + 1$ é irredutível.

5.6 Conclusão

Embora não exista um método geral para determinar irredutibilidade em $\mathbb{Q}[x]$, conseguimos, por meio dos critérios elaborados nesta aula, caracterizar a irredutibilidade de certos tipos de polinômios. O principal critério é o de Eisenstein. Eles são de extrema utili-

dade tanto na teoria dos corpos quanto na teoria de Galois.

RESUMO

Critério de Eisenstein

Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ não constante. Se existe um primo $p \in \mathbb{Z}$ tal que $p|a_0, \ldots, p|a_{n-1}$, $p \nmid a_n$ e $p^2 \nmid a_0$ então $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Critério $\mathbb{Z}_p[x]$

Seja $f(x) \in \mathbb{Z}[x]$ um polinômio não constante e seja p um primo que não divida o coeficiente líder de $f(x)$. Se $\phi_p(f(x))$ é irredutível em $\mathbb{Z}_p[x]$ então $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Critério $f(x+c)$

Seja $f(x) \in k[x]$, k corpo, e $c \in k$. Se $f(x+c)$ é irredutível em $k[x]$ então $f(x)$ é irredtível em $k[x]$.

O polinômio ciclotômico $\Phi_p(x)$, p primo

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

PRÓXIMA AULA

Na próxima aula iniciaremos a segunda fase do curso. Será uma aula de transição entre o estudo de polinômios e a teoria de corpos. Estudaremos os anéis quocientes obtidos por meio de ideais em

$k[x]$. É muito importante que você ganhe maturidade na estrutura de tais anéis, pois será a teoria que dará suporte à toda teoria dos corpos vista neste curso.

ATIVIDADES

ATIV. 5.1. Mostre que os seguintes polinômios $f(x) \in \mathbb{Z}[x]$ são irredutíveis sobre $\mathbb{Q}[x]$.

a) $f(x) = x^4 + 2x^3 + 2x^2 + 2x + 2$.

b) $f(x) = x^7 - 31$.

c) $f(x) = x^6 + 15$.

d) $f(x) = x^3 + 6x^2 + 5x + 25$.

e) $f(x) = x^4 + 8x^3 + x^2 + 2x + 5$.

f) $f(x) = x^4 + 10x^3 + 20x^2 + 30x + 22$.

ATIV. 5.2. Determine quais dos seguintes polinômios são irredutíveis sobre $\mathbb{Q}$.

a) $x^3 - x + 1$ *b*) $x^3 + 2x + 10$

c) $x^3 - 2x^2 + x + 15$ *d*) $x^4 + 2$

e) $x^4 - 2$ *f*) $x^4 - x + 1$

ATIV. 5.3. Determine quais dos seguintes polinômios sobre os seguintes corpos K são irredutíveis:

a) $x^7 + 22x^3 + 11x^2 - 44x + 33$, $K = \mathbb{Q}$

b) $x^3 - 7x^2 + 3x + 3$, $K = \mathbb{Q}$

c) $x^4 - 5$, $K = \mathbb{Z}_{17}$

d) $x^3 - 5$, $K = \mathbb{Z}_{11}$

LEITURA COMPLEMENTAR

CLARK, Allan, Elements of abstract algebra. Dover, 1984

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.

AULA

Anéis quocientes $k[x]/I$

6

META:

Determinar as possíveis estruturas definidas sobre o conjunto das classes residuais do quociente entre o anel de polinômios e seus ideais.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Reconhecer as estruturas de anel e espaço vetorial do conjunto quociente $k[x]/I$.

Caracterizar uma base de $k[x](f(x))$ como um espaço vetorial sobre o corpo k.

Reconhecer a classe $\overline{x}$ em $k[x]/(f(x))$ como uma raiz do polinômio $f(x)$.

Usar o processo de adjunção de raízes para determinar corpos de raízes de alguns polinômios.

PRÉ-REQUISITOS

As seguintes noções de álgebra linear: espaço vetorial, dependência e independênica linear, base e dimensão.

6.1 Introdução

Seja A um anel e $I \subset A$ um ideal. A relação de congruência módulo o ideal I ($a \equiv b \Leftrightarrow a - b \in I$) define uma relação de equivalência em A. A classe de equivalência de um elemento a é o conjunto $\overline{a} = \{a + b : b \in I\} = a + I$. O importante na definição de congruência é que usa apenas a estrutura aditiva de A. Sendo $(A, +)$ um grupo abeliano, $(I, +)$ é um subgrupo normal de A. Assim, o quociente A/I é grupo aditivo com a operação $\overline{a} + \overline{b} = \overline{a + b}$. A operação $\overline{a}.\overline{b} = \overline{a.b}$ define uma multiplicação em A/I. O anel $(A/I, +, .)$ é chamado anel quociente ou anel de classes residuais módulo I. Se A é comutativo com identidade 1_A então A/I é comutativo com identidade $\overline{1}_A$. São fundamentais os seguintes resultados:

1. A/I é domínio se e somente se I é ideal primo.
2. A/I é corpo se e somente se I é ideal maximal.
3. Em um domínio de ideais principais (DIP), ideais primos são máximos.

6.2 Exemplos

Exemplo 6.1. Em $\mathbb{Z}[x]$,

$$x^2 + x + 1 \equiv x + 3 \mod x + 2$$

pois $x^2 + x + 1 - (x + 3) = x^2 - 4 = (x - 2)(x + 2) \in I$, $I = (x + 2)$.

Exemplo 6.2. Vamos mostrar que $\mathbb{Z}_2[x]/(x^2 + x + 1)$ é um anel com exatamente 4 elementos. Seja $\overline{f(x)} \in \mathbb{Z}_2[x]/(x^2 + x + 1)$. Então $f(x) \in \mathbb{Z}_2[x]$ e pelo algoritmo da divisão existem únicos $q(x), r(x) \in \mathbb{Z}_2[x]$ tais que $f(x) = q(x)(x^2 + x^1) + r(x)$ onde $r(x) =$

0 ou $0 \leq \deg r(x) < 2$. Assim, $r(x) = ax + b$ para $a, b \in \mathbb{Z}_2$. Deste modo, para toda classe $\overline{f(x)}$ existe um representante de grau 1 $ax + b \in \mathbb{Z}_2[x]$ tal que $\overline{f(x)} = \overline{ax + b}$. Vamos mostrar que este representante é único. De fato, $\overline{ax + b} = \overline{cx + d}$ implica $ax + b - (cx + d) = (a - c)x + b - d = q(x)(x^2 + x + 1)$. Se $ax + b \neq cx + d$ então segue da última igualdade que $1 \geq \deg((a - c)x + b - d) = \deg q(x)(x^2 + x + 1) \geq 2$, contradição. Logo, $ax + b = cx + d$. Assim, $\mathbb{Z}_2[x]/(x^2 + x + 1) = \{\overline{ax + b} \ : \ a, b \in \mathbb{Z}_2\}$. Pela unicidade da representação de uma classe por polinômios de grau 1 podemos omitir as barras e simplesmente escrever $\mathbb{Z}_2[x]/(x^2 + x + 1) = \{ax + b \ : \ a, b \in \mathbb{Z}_2\}$ que é um anel com 4 elementos: 0, 1, x e $1 + x$. Note que $x(x + 1) = x^2 + x = x + 1 + x = 1$, pois $x^2 \equiv x + 1$ em $\mathbb{Z}_2[x]/(x^2 + x + 1)$. Assim, toda classe não nula possui inverso multiplicativo e, portanto, $\mathbb{Z}_2[x]/(x^2 + x + 1)$ é um corpo. Prezado aluno, se você não percebeu, x^2+x+1 é irredutível em $\mathbb{Z}_2[x]$ logo gera um ideal primo. Sendo $\mathbb{Z}_2$ corpo, $\mathbb{Z}_2[x]$ é DIP e, portanto, primos são maximais. Logo, $(x^2 + x + 1)$ é maximal donde $\mathbb{Z}_2[x]/(x^2 + x + 1)$ é corpo.

6.3 O anel quociente $k[x]/I$

Seja $I \subset k[x]$ um ideal não nulo. Sendo $k[x]$ um DIP então $I = (f(X))$ para algum $f(x) = x^n + a_{n-1}x^{n-1} + \cdots a_1x + a_0$ (por quê mônico?). Se I é trivial, isto é, nulo ou gerado por uma unidade (constantes não nulas) então $k[x]/(0) = k[x]$ ou $k[x]/(1) = (0)$ (anel nulo). Vejamos o caso não trivial. Neste caso,

$$n = \deg f(x) > 0$$

e o exemplo 6.2 nos diz como procedermos. Por definição de anéis quocientes,

$$k[x]/(f(x)) = \{\overline{g(x)} \ : \ g(x) \in k[x]\}$$

onde $\overline{g(x)} = \{g(x) + h(x) : h(x) \in I\} = g(x) + I$.

1. Dado $\overline{g(x)} \in k[x]/I$, o algoritmo da divisão em $k[x]$ nos fornece únicos $q(x), r(x) \in k[x]$ tais que

   $$g(x) = q(x)f(x) + r(x)$$

   com $r(x) = 0$ ou $0 \leq \deg r(x) < n$. Assim,

   $$r(x) = b_{n-1}x^{n-1} + \cdots + b_1x + b_0$$

   é um polinômio de grau $\leq n-1$ e

   $$\begin{aligned} \overline{g(x)} = \overline{q(x)f(x) + r(x)} & \\ &= \overline{q(x)f(x)} + \overline{r(x)} \\ &= \overline{r(x)} \end{aligned}$$

   Portanto, toda classe $\overline{g(x)} \in k[x]/I$ possui um representante de grau $\leq n-1$.

2. Suponhamos que $r_1(x), r_2(x) \in k[x]$ sejam dois representantes de grau $\leq n-1$ para uma mesma classe $\overline{g(x)} \in k[x]/I$. Então $\overline{r_1(x)} = \overline{g(x)} = \overline{r_2(x)}$ donde $\overline{r_1(x)} - \overline{r_2(x)} = \overline{r_1(x) - r_2(x)} = \overline{0}$. Se $r_1(x) \neq r_2(x)$ então

   $$r_1(x) - r_2(x) = q(x)f(x)$$

   e isto é uma contradição, pois o grau à esquerda é sempre $\leq n-1$ e o grau à direita é sempre $\geq n$. Assim, $r_1(x) = r_2(x)$.

3. Seja $\overline{k} = \{\overline{a} : a \in k\} \subset k[x]/I$ o conjunto das classes dos polinômios constantes em $k[x]$. A aplicação

$$\pi_{|_k} : k \to k[x]/I, \quad a \mapsto \overline{a}$$

define um homomorfismo de núcleo nulo (verifique isto!) cuja imagem é o conjunto $\overline{k}$. Pelo teorema fundamental do isomorfismo, $k \simeq \overline{k}$. Deste modo, podemos fazer a identificação $\overline{a} := a$ para cada $a \in k$ e obtermos a inclusão $k \subset k[x]/I$. Tal inclusão preserva toda a estrutura do corpo k dentro de $k[x]/I$ e isto caracteriza uma extensão de anéis. Assim, $k[x]/I$ é uma extensão do corpo k (de anéis!) na qual a classe $\overline{x}$ satisfaz a relação

$$\overline{x}^n + a_{n-1}\overline{x}^{n-1} + \cdots + a_1\overline{x} + a_0 = 0 \tag{6.6}$$

Para ver isto, observe a seguinte sequência de igualdades:

$$\begin{aligned} \overline{x}^n + a_{n-1}\overline{x}^{n-1} + \cdots + a_1\overline{x} + a_0 &= \overline{x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0} \\ &= \overline{f(x)} = \overline{0} = 0. \end{aligned}$$

OBS 6.1. De 1) e 2) acima segue que

$$\begin{aligned} k[x]/(f(x)) &= \{\overline{r(x)} \ : \ \deg r(x) \leq n-1\} \\ &= \{\overline{b_0 + \cdots + c_{n-1}x^{n-1}} \ : \ b_i \in k\} \\ &= \{\overline{b}_0 + \overline{b}_1\overline{x} + \cdots + \overline{b}_{n-1}\overline{x}^{n-1} \ : \ b_i \in k\} \end{aligned}$$

Por 3), podemos omitir as barras sobre as classes dos elementos de k e assim obtemos:

$$k[x]/I = \{b_0 + b_1\overline{x} + \cdots + b_{n-1}\overline{x}^{n-1} : b_i \in k\}$$

Note que as expressões

$$b_0 + b_1\overline{x} + \cdots + b_{n-1}\overline{x}^{n-1}$$

são combinações lineares de $1, \overline{x}, \ldots, \overline{x}^{n-1} \in k[x]/I$ com coeficientes em k. Além disso, $(k[x]/I, +)$ é um grupo aditivo abeliano (é anel!) e com respeito à multiplicação por elementos de k é distributivo, associativo e $1.\overline{g(x)} = \overline{g(x)}$. Isto define uma estrutura de espaço vetorial de $k[x]/I$ sobre k tendo $1, \overline{x}, \ldots, \overline{x}^{n-1}$ como conjunto de geradores. Pela unicidade das expressões em grau $n-1$ segue a independência linear de tal conjunto. Assim,

$$1, \overline{x}, \ldots, \overline{x}^{n-1}$$

é um conjunto de geradores linearmente independentes. Logo, é uma base de $k[x]/I$ como um espaço vetorial sobre k com n elementos. Então,

$$\dim_k k[x]/I = n = \text{ deg } f(x)$$

onde a expressão acima denota a dimensão de $k[\overline{x}]$ sobre k.

OBS 6.2. Este procedimento é uma forma de construir espaços vetoriais de dimensão finita arbitrária tendo ainda uma estrutura adicional de anéis. Tal estrutura híbrida é o que se chama de k-álgebra. Sobe tal aspecto, $k[x]/I$ é uma k-álgebra gerada por $\overline{x}$ e isto é denotado por $k[\overline{x}]$. Assim, temos a igualdade de notações $k[x]/I = k[\overline{x}]$. Em geral, uma k-álgebra finitamente gerada por $g_1, \ldots, g_r$ é denotada por $k[g_1, \ldots, g_r]$ e chamada k-álgebra de tipo finito. Tal linguagem significa dizer que $k[g_1, \ldots, g_r]$ é um anel contendo k como subanel e tendo adicionalmente uma estrutura de k-espaço vetorial. Um elemento em $k[g_1, \ldots, g_r]$ é uma expressão polinomial em $g_1, \ldots, g_r$ com coeficientes em k.

OBS 6.3. A relação 6.6 não somente nos fornece uma dependência linear de $1, \overline{x}, \ldots, \overline{x}^{n-1}$ sobre k como também nos diz que $f(\overline{x}) = 0$. Assim, $\overline{x}$ é uma raiz do polinômio $f(x)$. Deste modo $k[x]/I = k[\overline{x}]$ é uma extensão de k contendo uma raiz de $f(x) \in k[x]$. No caso em

que $k[\overline{x}]$ é um corpo, este procedimento de construção de raízes de polinômios chama-se adjunção de raízes. Isto constituirá o cerne da teoria de extensões de corpos nas aulas subsequentes. Por isso, precisamos saber quando $k[x]/I$ é corpo e isto é o que nos motiva para a próxima seção.

6.4 A estrutura de $k[x]/(p(x))$ quando $p(x)$ é irredutível

Considere os seguintes fatos já vistos:

1. $k[x]$ é DIP (teorema 3.3).
2. Polinômios irredutíveis em $k[x]$ são elementos primos (Lema 3.2).
3. Elementos primos geram ideais primos.
4. Em um DIP ideais primos são ideais maximais.
5. O anel quociente A/I é corpo se e somente se I e ideal maximal.

Conclusão:

$p(x) \in k[x]$ irredutível $\Rightarrow$ $k[x]/(p(x))$ corpo.

OBS 6.4. Vale a recíproca da implicação acima. Veja atividade 6.1.

Exemplo 6.3. O polinômio $p(x) = x^2 + 1$ é irredutível em $\mathbb{R}[x]$, pois é de grau 2 e não tem raízes reais ($\mathbb{R}$ é um corpo ordenado). Assim, o anel quociente $\mathbb{R}[x]/(x^2+1)$ é corpo. Pela observação 6.1, $\mathbb{R}[x]/(x^2+1) = \{a + b\overline{x} : a, b \in \mathbb{R}\}$ com $a + b\overline{x} = 0$ se e somente se $a = b = 0$. Em $\mathbb{R}[\overline{x}]$, $\overline{x}^2 + 1 = 0$ donde $\overline{x}^2 = -1$. Deste modo, a aplicação $\varphi : \mathbb{R}[\overline{x}] \to \mathbb{C}$, $a + b\overline{x} \mapsto a + bi$ define um isomorfismo de corpos com $\varphi(a) = a$ para todo $a \in \mathbb{R}$.

6.5 Adjunção de raízes

Na seção 6.3, mais precisamente na observação 6.3, foi exibida a noção de adjunção de raízes. Seja dado um polinômio $f(x) \in k[x]$. O método de adjunção de raízes consiste nos seguintes passos:

Passo 1 Considere um fator irredutível $p(x)$ de $f(x)$ em $k[x]$ (existe, pois $k[x]$ é DFU).

Passo 2 O anel quociente $k[x]/(p(x)) = k[\overline{x}]$ é um corpo contendo k (extensão de k) tendo $\overline{x}$ como raiz de $p(x)$ (ver observação 6.3). Como $p(x)|f(x)$ então $\overline{x}$ é também raiz de $f(x)$.

Passo 3 Denotando $\overline{x} := \alpha_1$ temos $k \subset k[\alpha_1]$ com α_1 raiz de $f(x) \in (k[\alpha_1])[x]$ (os coeficientes de $f(x)$ estão em $k[\alpha_1]$). Pelo teorema do fator, podemos escrever $f(x) = (x-\alpha_1)^{a_1} q_1(x)$ com $q_1(x) \in k[\alpha_1][x]$ de grau $< f(x)$ e $q_1(\alpha_1) \neq 0$. Aplicando os Passos 1 e 2 agora para $q_1(x)$ obtemos um fator irredutível $p_2(x) \in (k[\alpha_1])[x]$ de modo que o corpo $(k[\alpha_1])[x]/(p_2(x))$ contém $k[\alpha_1]$ com $\overline{x} := \alpha_2$ uma raiz de $p_2(x)$. Logo, $k[\alpha_1][\alpha_2] = k[\alpha_1, \alpha_2]$ é um corpo contendo $k[\alpha_1]$ (logo k) e as raízes α_1, α_2 de $f(x)$.

Passo 4 Em $k[\alpha_1, \alpha_2]$ temos $f(x) = (x - \alpha_1)^{a_1}(x - \alpha_2)^{a_2} q_2(x)$, com $q_2(\alpha_i) \neq 0$, $i = 1, 2$. Repetindo o Passo 3 obtemos um polinômio irredutível $p_3(x) \in k[\alpha_1, \alpha_2][x]$, com $\deg p_3(x) < \deg q_2(x) < \deg p_2(x)$ tal que $f(x) = (x-\alpha_1)^{a_1}(x-\alpha_2)^{a_2}(x-\alpha_3)^{a_3} q_3(x) \in k[\alpha_1, \alpha_2][x]/(p_3(x)) = k[\alpha_1, \alpha_2, \alpha_3]$, $\alpha_3 = \overline{x}$ em $k[\alpha_1, \alpha_2][x]/(p_3(x))$ e $q_3(\alpha_i) \neq 0$, $i = 1, 2, 3$.

O procedimento acima termina após um número finito de passos (no máximo em n passos) com

$$f(x) = (x - \alpha_1)^{a_1} \cdots (x - \alpha_r)^{a_r} \in k[\alpha_1, \alpha_2, \cdots, \alpha_r][x].$$

OBS 6.5. O corpo $k[\alpha_1, \alpha_2, \cdots, \alpha_r]$ é o menor corpo contendo todas as raízes de $f(x)$ e é chamado o corpo de raízes de $f(x)$. As raízes $\alpha_1, \cdots, \alpha_r$ são todas distintas e os expoentes a_i's são chamados multiplicidades da raiz α_i. Além disso, em geral não são necessários n passos para se chegar ao corpo de raízes de um polinômio de grau n. Às vezes, apenas um é necessário.

Exemplo 6.4. Seja $p \in \mathbb{Z}$ um primo. Então, $f(x) = x^2 - p$ é irredutível em $\mathbb{Q}[x]$. Assim, $\mathbb{Q}[x]/(x^2 - p) = \mathbb{Q}[\alpha]$, $\alpha = \overline{x} \in \mathbb{Q}[x]/(x^2 - p)$ é uma raíz de $x^2 - p$. Como $-\alpha \in \mathbb{Q}[\alpha]$ é a outra raiz de $x^2 - p$ segue que $x^2 - p = (x - \alpha)(x + \alpha) \in \mathbb{Q}[\alpha][x]$. Denotando α por $\sqrt{p}$, segue da observação 6.1 a seguinte igualdade:

$$\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} \ : \ a, b \in \mathbb{Q}\}.$$

$\mathbb{Q}[\sqrt{p}]$ é o corpo de raízes de $x^2 - p$ sobre $\mathbb{Q}$ pois $\mathbb{Q}[\sqrt{p}] = \mathbb{Q}[\sqrt{p}, -\sqrt{p}]$ é o menor corpo contendo Q e as raízes de $x^2 - p$.

6.6 Conclusão

O anel quociente $k[x]/I$, $I \neq (0)$, possui uma estrutura de espaço vetorial sobre k de dimensão finita e igual ao grau do polinômio gerador de I. Isto possibilita a integração da teoria dos anéis com álgebra linear. Subjacente à estas duas está a estrutura de corpo do anel $k[x]/I$ quando I é gerado por um polinômio irredutível. Toda esta confluência de estruturas em um só objeto algébrico, já tornaria o anel quociente $k[x]/I$ interessante por si só. Mas, o fato de conter uma raiz do polinômio gerador do ideal I confere ao mesmo o estatus de principal objeto algébrico.

RESUMO

Dado $f(x) \in k[x]$ não constante, eis o que se pode dizer a respeito do anel quociente $k[x]/(f(x))$:

1. $k[x]/(f(x))$ é um anel contendo o corpo k.

2. $k[x]/(f(x)) = k[\overline{x}]$ é espaço vetorial sobre k de dimensão finita $n = \deg f(x)$ com base $1, \overline{x}, \overline{x}^2, \ldots, \overline{x}^{n-1}$.

3. A classe $\overline{x} \in k[x]/(f(x))$ é uma raiz do polinômio $f(x)$.

4. Se $f(x)$ é irredutível sobre $k[x]$ então $k[x]/(f(x))$ é um corpo contendo k e a raiz $\overline{x}$ de $f(x)$.

5. Se $f(x)$ é irredutível então $k[x]/(f(x)) = k[\overline{x}]$ é o menor corpo contendo k e a raiz $\alpha = \overline{x}$ de $f(x)$.

6. O processo acima de passar ao quociente $k[x]/(f(x))$ para determinar o menor corpo contendo k e uma raiz de $f(x)$ é chamado de adjunção da raiz $\overline{x}$ ao corpo k.

7. A iteração do processo de adjunção de raízes determina o menor corpo contendo k e todas as raízes do polinômio $f(x)$. O corpo assim obtido é chamado *corpo de raízes* de $f(x)$.

PRÓXIMA AULA

Iniciaremos o estudo de teoria dos corpos, pré-âmbulo à teoria de Galois. Usaremos os conhecimentos obtidos nesta aula sobre os anéis quocientes para nos auxiliar nesta tarefa.

ATIVIDADES

ATIV. 6.1. Seja k um corpo. Mostre a equivalência entre as seguintes afirmações:

i) $p(x)$ é irredutível em $k[x]$.

ii) $k[x]/(p(x))$ é um corpo.

iii) $k[x]/(p(x))$ é um domínio de integridade.

Sugestão: Use os seguintes fatos conhecidos:

a) Corpos são domínios.

b) A/I é domínio $\Leftrightarrow$ I é ideal primo.

b) A/I é corpo $\Leftrightarrow$ I é maximal.

c) A DIP $\Rightarrow$ (I ideal primo $\Leftrightarrow$ I ideal maximal).

d) k corpo $\Rightarrow$ $k[x]$ DIP.

e) k corpo $\Rightarrow$ irredutíveis em $k[x]$ são elementos primos (logo, geram ideais primos).

ATIV. 6.2. Seja $p \in \mathbb{Z}$ primo. Mostre que se $p(x) \in \mathbb{Z}_p[x]$ é irredutível de grau n então $\mathbb{Z}_p[x]/(p(x))$ é um corpo contendo $\mathbb{Z}_p$ com p^n elementos.

ATIV. 6.3. Considere o conjunto

$$\mathbb{Q}[\sqrt{2}] = \{a_0 + a_1\sqrt{2} + \cdots + a_n(\sqrt{2})^n \ : \ a_i \in \mathbb{Q}, n \in \mathbb{Z}_{\geq 0}\}.$$

Mostre que $\mathbb{Q}[\sqrt{2}]$ é um subcorpo de $\mathbb{R}$ como segue. Defina a função

$$\varphi : \mathbb{Q}[x] \to \mathbb{R},\ f(x) \mapsto \varphi(f(x)) = f(\sqrt{2}).$$

i) Mostre que φ é um homomorfismo com conjunto imagem $\mathbb{Q}[\sqrt{2}]$.

ii) Mostre que Ker $\varphi = (x^2 - p)$.

iii) Use o teorema fundamental do isomorfismo para concluir que $\mathbb{Q}[x]/(x^2 - p) \cong \mathbb{Q}[\sqrt{2}]$.

iv) Caracterize a irredutibilidade de $x^2 - 2$ e conclua que o anel quociente $\mathbb{Q}[x]/(x^2 - p)$ é corpo. Do isomorfismo acima, $\mathbb{Q}[\sqrt{2}]$ é um corpo contido em $\mathbb{R}$.

v) Mostre que se K é um subcorpo de $\mathbb{R}$ contendo $\mathbb{Q}$ e $\sqrt{2}$ então K contém $\mathbb{Q}[\sqrt{2}]$. Conclua que $\mathbb{Q}[\sqrt{2}]$ é o corpo de raízes de $x^2 - 2$ sobre $\mathbb{Q}$.

vi) Mostre que todo elemento de $\mathbb{Q}[\sqrt{2}]$ se escreve de maneira única na forma $a + b\sqrt{2}$, com $a, b \in \mathbb{Q}$ e, portanto,

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \ : \ a, b \in \mathbb{Q}\}$$

vii) Determine o inverso de um elemento não nulo $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

viii) Determine a dimensão de $\mathbb{Q}[\sqrt{2}]$ como um espaço vetorial sobre $\mathbb{Q}$.

ATIV. 6.4. Mesma questão anterior para

$$\mathbb{Q}[\sqrt{3}] = \{a_0 + a_1\sqrt{3} + \cdots + a_n(\sqrt{3})^n \ : \ a_i \in \mathbb{Q}, n \in \mathbb{Z}_{\geq 0}\}.$$

ATIV. 6.5. Mostre que $\mathbb{Q}[\sqrt{2}]$ e $\mathbb{Q}[\sqrt{3}]$ não são corpos isomorfos.

Sugestão: Suponha que exista um isomorfismo $\varphi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$. Mostre que $\varphi(\frac{a}{b}) = \frac{a}{b}$ para todo $\frac{a}{b} \in \mathbb{Q}$. Conclua que $\varphi(\sqrt{2}) = \sqrt{2} \in \mathbb{Q}[\sqrt{3}]$. Mostre que isto é uma contradição por mostrar que $\sqrt{2} \notin \mathbb{Q}[\sqrt{3}]$.

ATIV. 6.6. Mostre que $\mathbb{Z}_2[x]/(x^3 + x + 1)$ é um corpo contendo todas as três raízes de $x^3 + x + 1$.

ATIV. 6.7. Racionalize a fração $\dfrac{1}{1 + \sqrt[3]{2} + \sqrt[3]{4}}$.

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.

AULA

Extensões de Corpos

7

META:

Determinar as noções e fatos básicos da teoria dos corpos.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Definir: Característica de corpos, extensão de corpos, grau de uma extensão, extensão finita, extensão finitamente gerada, extensão simples, elemento algébrico e transcendente, polinômio mínimo, corpo de raízes de um polinômio, extensão algébrica e corpo algebricamente fechado.

Determinar a característica de um corpo.

Expressar uma extensão simples $k[\alpha]$ como um quociente $k[x]/(p(x))$ em que $p(x)$ é o polinômio mínimo de α.

Determinar uma base vetorial de uma extensão algébrica simples.

Determinar as operações adição e multiplicação para extensão algébricas simples.

Determinar o inverso de um elemento dado em uma extensão algébrica simples.

PRÉ-REQUISITOS

Observação 6.1 e seção 6.4 da aula 6.

7.1 Introdução

Iniciaremos o estudo de extensões de corpos. Na primeira seção, são listadas todas as definições básicas que iremos precisar. É muito importante que você interiorize tais definições. Sem elas em mente fica impossível acompanhar o restante do curso.
Nas seções que seguem, veremos alguns exemplos e os principais fatos sobre o tema.
A fim de tornar mais dinâmica a exposição do assunto, as provas dos fatos são dadas em uma seção à parte em forma de exercícios resolvidos. Desta maneira, os resultados tornam-se problemas teóricos que precisam ser resolvidos e você está convidado à resolvê-los antes mesmos de ver a solução. Este modo ativo de estudo forçará você a relacionar as idéias sobre os assuntos anteriores. Bons estudos!

7.2 Glossário

Ao longo desta seção, F denotará um corpo.

Característica de corpos A característica de um corpo F, denotado por $Ch\ F$, é o gerador não negativo do homomorfismo de grupos (anéis)

$$\varphi : \mathbb{Z} \to F, n \mapsto n.1_F = \underbrace{1_F + \cdots 1_F}_{n \text{ parcelas}}.$$

Em outras palavras, a característica de um corpo é zero ou o menor inteiro positivo n tal que $n.1_F = 0$.

Subcorpo primo O subcorpo primo de um corpo F é o subcorpo de F gerado pela identidade multiplicativa 1_F.

Extensão de um corpo Um corpo K é dito uma extensão de F se K contém F como um subcorpo. Notação: $F \subset K$. O corpo F é chamado de corpo base da extensão $F \subset K$.

Grau de uma extensão O grau de uma extensão de corpos $F \subset K$, denotado por $[K : F]$, é a dimensão de K considerado como um espaço vetorial sobre F.

Extensão finita Uma extensão $F \subset K$ é chamada finita se $[K : F]$ é finito. Caso contrário, a extensão é dita infinita.

Corpos finitamente gerados O corpo gerado sobre F por uma coleção finita de elementos $\alpha_1, \ldots, \alpha_r \in K$, denotado por $F(\alpha_1, \ldots, \alpha_r)$, é o menor subcorpo de K contendo F e $\alpha_1, \ldots, \alpha_r$.

Extensão finitamente gerada Extensão $F \subset K$ na qual existem finitos elementos $\alpha_1, \ldots, \alpha_r \in K$ tais que $K = F(\alpha_1, \ldots, \alpha_r)$.

Extensão simples Extensão $F \subset K$ na qual existe $\alpha \in K$ tal que $K = F(\alpha)$.

Elemento algébrico Seja $F \subset K$ uma extensão de corpos. Um elemento $\alpha \in K$ é dito algébrico sobre F se existe um polinômio não nulo $f(x) \in F[x]$ tal que $f(\alpha) = 0$. Em outras palavras, o núcleo do homomorfismo $\varphi_\alpha : F[x] \to K$, $f(x) \mapsto \varphi_\alpha(f(x)) = f(\alpha)$ é não nulo.

Elemento transcendente Elemento não algébrico.

Polinômio mínimo Seja $F \subset K$ uma extensão de corpos e $\alpha \in K$ algébrico sobre F. O polinômio mínimo de α sobre F, denotado por $m_{\alpha,F}(x)$, é o polinômio de menor grau em $F[x]$

tendo α como raiz. Em outras palavras, $m_{\alpha,F}(x)$ é o gerador do núcleo do homomorfismo entre $F[x]$ e K definido por $f(x) \mapsto f(\alpha)$.

Corpo de raízes de um polinômio Chama-se corpo de raízes de um polinômio $f(x) \in F[x]$ ao menor corpo contendo F e todas as raízes de $f(x)$.

Extensão algébrica Um corpo K é dito uma extensão algébrica de F se todo elemento de K é algébrico sobre F.

Fecho algébrico O fecho algébrico de um corpo F é um corpo, denotado por $\overline{F}$, algébrico sobre F e satisfazendo a condição em que todo polinômio $f(x) \in F[x]$ fatora-se completamente em $\overline{F}$.

Corpo algebricamente fechado Corpo K no qual todo polinômio com coeficientes em K possui uma raiz em K. Em símbolos, $\overline{K} = K$.

Extensão normal Extensão $F \subset K$ na qual todo polinômio irredutível em $F[x]$ possuindo um raiz em K fatora-se completamente em K.

Extensão de um isomorfismo Sejam $F \subset L$ e $E \subset K$ duas extensões de corpos e $\varphi : F \to E$ um homomorfismo de corpos. Um homomorfismo $\tilde{\varphi} : L \to K$ é dito uma extensão de φ se $\tilde{\varphi}(c) = \varphi(c)$ para todo $c \in F$.

Polinômio separável Polinômio sem raízes múltiplas. Se $f(x) \in F[x]$ é separável de grau n então $f(x)$ possui n raízes distintas em seu corpo de raízes.

Elemento separável Um elemento α em uma extensão K de F é dito separável sobre F se α é raiz de um polinômio sepa-

rável em $F[x]$. Equivalentemente, α é dito separável sobre F se é algébrico sobre F e seu polinômio mínimo $m_{\alpha,F}(x)$ é separável.

Extensão separável Extensão $F \subset K$ na qual todo elemento em K é separável sobre F.

7.3 Exemplos

1. O corpo dos números racionais $\mathbb{Q}$ tem característica *zero*. De fato, o subgrupo abeliano aditivo de $\mathbb{Q}$ gerado pela identidade 1 é o conjunto $\mathbb{Z}$ dos inteiros. Logo, $n.1 \neq 0$ para todo inteiro positivo n. Assim, todo corpo contendo um subanel isomorfo à $\mathbb{Z}$ é de característica zero.

2. Se p é primo então $\mathbb{F}_p = \mathbb{Z}_p$ é um corpo de característica positiva p. De fato,

$$p.1_{\mathbb{F}_p} = \underbrace{1_{\mathbb{F}_p} + \cdots + 1_{\mathbb{F}_p}}_{p \text{ parcelas}} = \overline{p} = \overline{0}.$$

3. A relação entre característica de um corpo F e seu corpo primo é como segue. Todo corpo F contém um elemento identidade 1_F. Da estrutura de corpo, F contém o grupo abeliano aditivo gerado por 1_F, aqui denotado por $< 1_F >$. A aplicação $\varphi : \mathbb{Z} \to F$, $n \mapsto n.1_F$, define um homomorfismo não somente de grupos mas também de anéis. Temos Im φ $= < 1_F >$. Existem dois casos:

   Caso 1: Ker $\varphi = 0$. Neste caso, $n \neq 0$ implica $\varphi(n) = n.1_F \neq 0$. Assim, não existe $n \neq 0$ tal que $n.1_F = 0$. Isto significa ch $F = 0$. Pelo teorema fundamental do isomorfismo, $\mathbb{Z} \cong < 1_F >$. Desde que corpos de frações

de domínios isomorfos são também isomorfos então F contém um corpo K isomorfo à $\mathbb{Q}$. Por construção e definição de corpo primo, $K \cong \mathbb{Q}$ é o corpo primo de F.

Caso 2: Ker $\varphi \neq 0$. Sendo $\mathbb{Z}$ DIP, o núcleo Ker φ é principal, Ker $\varphi = (p)$. Podemos supor $p > 0$. Lembramos que p, na condição de gerador do ideal, é o menor inteiro positivo em Ker φ. Por definição de núcleo, p é o menor inteiro positivo tal que $\varphi(p) = p.1_F = 1_F + \cdots 1_F = 0$. Isto é justamente a definição de característica. Assim, ch $F = p$. O anel quociente $\mathbb{Z}/(p)$ é domínio (isomorfo à um subanel de um corpo). Logo, p é primo. Assim, $F_P \cong \mathbb{Z}_p = \mathbb{Z}/(p)$ é o corpo primo de F.

4. O polinômio x^2+1 é irredutível sobre $\mathbb{R}$, logo o anel quociente $\mathbb{R}[x]/(x^2+1)$ é um corpo. À esta altura eis o que devemos saber sobre um corpo:

   (a) A expressão de um elemento genérico do corpo. Neste caso, um elemento típico de $\mathbb{R}[x]/(x^2+1)$ é unicamente escrito na forma $a + b\overline{x}$, $a, b \in \mathbb{R}$ com $\overline{x}$ satisfazendo a relação $\overline{x}^2 + 1 = 0$ (ver exemplo 6.3).

   (b) Efetuar a adição e a multiplicação. Neste caso:

   Adição: $(a + b\overline{x}) + (c + d\overline{x}) = (a + b) + (c + d)\overline{x}$.

   Multiplicação:

$$\begin{aligned}(a + b\overline{x}).(c + d\overline{x}) &= ac + ad\overline{x} + bc\overline{x} + bd\overline{x}^2 \\ &= (ac - bd) + (ad + bc)\overline{x}\end{aligned}$$

   onde temos feito a substituição $\overline{x}^2 = -1$.

   (c) Expressar, se possível, por meio de um isomorfismo o corpo como um corpo já conhecido. Neste caso, $\mathbb{R}[\overline{x}] \cong$

$\mathbb{C}$ pois a aplicação $\varphi : \mathbb{R}[\overline{x}] \to \mathbb{C}$, $a + b\overline{x} \mapsto a + bi$ define um isomorfismo de corpos.

(d) Exibir, se possível, o inverso de um elemento não nulo geral. Neste caso, para $a, b \in \mathbb{R}$ não simultaneamente nulos:

$$\begin{aligned}(a+b\overline{x})^{-1} &= \frac{1}{a+b\overline{x}} \\ &= \frac{1}{a+b\overline{x}}.\frac{a-b\overline{x}}{a-b\overline{x}} \\ &= \frac{a-b\overline{x}}{a^2-(b\overline{x})^2} \\ &= \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}\overline{x}\end{aligned}$$

5. Determinar o grau da extensão $\mathbb{R} \subset \mathbb{R}[\overline{x}]$. A dimensão de um espaço vetorial é a cardinalidade de uma base qualquer. Assim, devemos determinar uma base de $\mathbb{R}[\overline{x}]$ sobre $\mathbb{R}$. Lembramos que uma base é um conjunto de geradores linearmente independentes.

   (a) Conjunto de geradores: $1, \overline{x}$. De fato, todo elemento de $\mathbb{R}[\overline{x}]$ se escreve na forma $a + b\overline{x} = a.1 + b.\overline{x}$.

   (b) Independência linear: $a + b\overline{x} = 0 \Leftrightarrow \overline{a + bx} = \overline{0} \in \mathbb{R}[x]/(x^2+1) \Leftrightarrow a+bx \in (x^2+1) \Leftrightarrow a+bx = q(x)(x^2+1)$. Se $a + bx \neq 0$ então, $1 \geq \deg(a + bx) = \deg q(x) + \deg(x^2+1) \geq 2$, contradição. Logo, $a+bx = 0$ implica $a = b = 0$.

6. Considere o corpo $\mathbb{Q}[\sqrt{p}] \cong \mathbb{Q}[x]/(x^2 - p)$ obtido no exemplo 6.4. Como no exemplo anterior, as características básicas da extensão $\mathbb{Q} \subset \mathbb{Q}[\sqrt{p}]$ são:

   (a) Elemento genérico:

   $$a + b\sqrt{p} \quad (\text{ tal expressão é única}).$$

(b) Operações:

Adição:

$$(a + b\sqrt{p}) + (c + d\sqrt{p}) = (a + b) + (c + d)\sqrt{p}$$

Multiplicação:

$$(a + b\sqrt{p}).(c + d\sqrt{p}) \quad = \quad (ac + p.bd) + (ad + bc)\sqrt{p}$$

(c) A aplicação $\varphi : \mathbb{Q}[x] \to \mathbb{R}$, $f(x) \mapsto f(\sqrt{p})$, define um homomorfismo de anéis de núcleo Ker $\varphi = (x^2 - p)$ (prove isto!). Assim,

$$\mathbb{Q}[x]/(x^2 - p) \cong \quad \text{Im } \varphi$$

com

$$\text{Im } \varphi = \{\mathrm{a_0}+\mathrm{a_1}\sqrt{\mathrm{p}}+\cdots+\mathrm{a_n}\sqrt{\mathrm{p}}^{\mathrm{n}} : \mathrm{a_i} \in \mathbb{Q},\ \mathrm{n} \in \mathbb{Z}_{\geq 0}\} \subset \mathbb{R}$$

onde o conjunto à direita é denotado por $\mathbb{Q}[\sqrt{p}]$. Neste caso, temos mostrado que

$$\mathbb{Q}[\sqrt{p}] = \{a + b\sqrt{p} \ : \ a, b \in \mathbb{Q}\}.$$

(d) Inverso multiplicativo:

$$(a + b\sqrt{p})^{-1} \quad = \quad \frac{a}{a^2 - pb^2} - \frac{b}{a^2 - pb^2}\sqrt{p}$$

7. $\left[\mathbb{Q}[\sqrt{p}] : \mathbb{Q}\right] = 2$, pois $1, \sqrt{p}$ é uma base de $\mathbb{Q}[\sqrt{p}]$ sobre $\mathbb{Q}$. De fato,

   (a) Geradores: Todo elemento de $\mathbb{Q}[\sqrt{p}]$ se escreve na forma $a + b\sqrt{p} = a.1 + b.\sqrt{p}$.

   (b) Independência linear: Da unicidade da expressão $a + b\sqrt{p}$ segue que $a + b\sqrt{p} = 0 \Leftrightarrow a = b = 0$.

Daqui por diante, se $F[\overline{x}]$ é o anel quociente $F[x]/(p(x))$, usaremos o grau de $p(x)$ para determinar o grau da extensão. Em símbolos: $[F[\overline{x}] : F] = n = \deg p(x)$ (ver exemplo 6.1).

8. Em $\mathbb{Z}_2[x]$, $p(x) = x^2 + x + 1$ é irredutível. Segue as características do corpo $\mathbb{Z}_2[\overline{x}] = \mathbb{Z}_2[x]/(x^2 + x + 1)$:

   (a) Elemento genérico:

   $$a + b\alpha$$

   com $\alpha^2 + \alpha + 1 = 0$, isto é, $\alpha^2 = -\alpha - 1 = \alpha + 1$. A expressão acima é única.

   (b) Operações:

   Adição:

   $$(a + b\alpha) + (c + d\alpha) = (a + b) + (c + d)\alpha$$

   Multiplicação:

   $$\begin{aligned}(a + b\alpha).(c + d\alpha) &= ac + (ad + bc)\alpha + bd\alpha^2 \\ &= ac + (ad + bc)\alpha + bd(\alpha + 1) \\ &= (ac + bd) + (ad + bc + bd)\alpha\end{aligned}$$

   (c) Inverso multiplicativo:

   $$(a + b\alpha)^{-1} = (a + b) + b\alpha$$

   (d) $[\mathbb{Z}_2[\alpha] : \mathbb{Z}_2] = \deg (x^2 + x + 1) = 2$. Logo, $\mathbb{Z}_2[\alpha]$ é um corpo com 4 elementos.

   OBS 7.1. Em geral, se $p(x)$ é irredutível em $\mathbb{Z}_p[x]$, p primo, então $\mathbb{Z}_p[\alpha] = \mathbb{Z}_p[x]/(p(x)$ é um corpo de característica p com p^n elementos.

9. Seja $F = \mathbb{Q}$ e $p(x) = x^3 - 2$ irredutível em $\mathbb{Q}[x]$ (Eisenstein, $p = 2$). As características básicas do corpo $\mathbb{Q}[x]/(x^3 - 2)$ são:

(a) Elemento genérico:

$$a + b\alpha + c\alpha^2$$

com $\alpha^3 - 2 = 0$, isto é, $\alpha^3 = 2$ ($\alpha = \overline{x}$). A expressão acima é única.

(b) Operações:

Adição:

$$\begin{aligned}(a_1 + b_1\alpha + c_1\alpha^2) + (a_2 + b_2\alpha + c_2\alpha^2) \quad &= \\ (a_1 + a_2) + (b_1 + b_2)\alpha + (c_1 + c_2)\alpha^2 &\end{aligned}$$

Multiplicação:

$$(a_1 + b_1\alpha + c_1\alpha^2)(a_2 + b_2\alpha + c_2\alpha^2) \quad = \quad r(\alpha)$$

onde $r(x) \in \mathbb{Q}[x]$ é o resto da divisão do produto $(a_1 + b_1x + c_1x^2)(a_2 + b_2x + c_2x^2)$ por $x^3 - 2$.

(c) Inverso multiplicativo: Dado $g(\alpha) = a+b\alpha+c\alpha^2 \in \mathbb{Q}[\alpha]$ considere o polinômio $g(x) = a+bx+cx^2 \in \mathbb{Q}[x]$. Pode-se mostrar que $\text{MDC}(x^3 - 2, g(x)) = 1$, (mostre isto usando o fato de $x^3 - 2$ ser irredutível em $\mathbb{Q}[x]$ e deg $g(x) <$ deg $x^3 - 2$). Pelo teorema de Bezout, existem $a(x), b(x) \in \mathbb{Q}[x]$ que verificam a igualdade

$$a(x)g(x) + b(x)(x^3 - 2) = 1$$

Passando às classes e lembrando que $\overline{x} = \alpha$, obtemos $a(\alpha)g(\alpha) = 1$ donde $a(\alpha) = g(\alpha)^{-1}$ (isto resolve a atividade 6.7).

(d) $[\mathbb{Q}[\alpha] : \mathbb{Q}] = \text{deg } (x^3 - 2) = 3$.

7.4 Fatos

1. Multiplicatividade dos graus: Se $F \subset K$ e $K \subset L$ são extensões finitas então $F \subset L$ é finita e $[L : F] = [L : K]\,[K : F]$.

2. Sejam K, L extensões finitas do corpo F e $\varphi : K \to L$ um isomorfismo de corpos tal que $\varphi(c) = c$ para todo $c \in F$. Então, $[K : F] = [L : F]$.

3. Seja F um corpo e seja $p(x) \in F[x]$ um polinômio irredutível sobre $F[x]$. Então,

   (a) Existe uma extensão K de F contendo uma raiz de $p(x)$.

   (b) Suponha K uma extensão de F contendo uma raiz α de $p(x)$. Seja $F(\alpha)$ o subcorpo de K gerado por F e α. Então,

   $$F(\alpha) \cong F[x]/(p(x)).$$

   Em particular, $F(\alpha) = F[\alpha]$.

4. Seja K uma extensão de F e $\alpha \in K$. São equivalentes as afirmações abaixo a respeito de um polinômio $p(x) \in F[x]$:

   (a) $p(x)$ gera o núcleo do homomorfismo $\varphi_\alpha : F[x] \to F[\alpha]$, $f(x) \mapsto f(\alpha)$.

   (b) $p(x)$ é irredutível em $F[x]$ e tem α como raiz.

   (c) $p(x)$ é o polinômio de menor grau em $F[x]$ tendo α como raiz.

   OBS 7.2. Se $q(x) \in F[x]$ é um outro polinômio em $F[x]$ satisfazendo uma das condições acima então $(q(x)) = (p(x))$ donde $q(x) \sim p(x)$. Assim, existe um único polinômio mônico nesta classe de polinômios associados satisfazendo tais condições. Este polinômio, denotado por $m_{\alpha,F}(x)$, é chamado *polinômio mínimo* de α.

5. Sejam K uma extensão de F e $\alpha \in K$ algébrico sobre F com polinômio mínimo $m_{\alpha,F}(x) \in F[x]$ de grau n. Então,

   (a) $F(\alpha) \cong F[\alpha] = F[x]/(m_{\alpha,F}(x))$.

   (b) $\{1_F, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base de $F(\alpha)$ sobre F.

   (c) $[F(\alpha) : F] = n$.

7.5 Exercícios Resolvidos

A menos que seja dito o contrário, K é uma extensão do corpo F.

1. Prove o fato 1: $F \subset K$ e $K \subset L$ finitas $\Rightarrow F \subset L$ finita e $[L : F] = [L : K][K : F]$.

   Solução: Suponha $[L : K] = n$ e $[K : F] = m$. Por definição de grau, seja

   $$\alpha = \{\alpha_1, \ldots, \alpha_n\}$$

   uma base de L sobre K e seja

   $$\beta = \{\beta_1, \ldots, \beta_m\}$$

   uma base de K sobre F. Considere o conjunto

   $$\gamma = \{\alpha_i\beta_j : 1 \leq i \leq n, 1 \leq j \leq m\} \subset L$$

   com nm elementos. Basta mostrar que γ é uma base de L sobre F.

   i) γ é um conjunto de geradores de L sobre F: Seja $u \in L$. Por definição de base, existem escalares $a_1, \ldots, a_n \in K$ tais que

   $$u = a_1\alpha_1 + \cdots + a_n\alpha_n \tag{7.7}$$

Desde que β é base de K sobre F e $a_1, \ldots, a_n$ são elementos de K então, para cada $i = 1, \ldots, n$, existem escalares $b_{1i}, \ldots, b_{mi} \in F$ tais que

$$\begin{aligned} a_1 &= b_{11}\beta_1 + \cdots b_{1m}\beta_m \\ a_2 &= b_{21}\beta_1 + \cdots b_{2m}\beta_m \\ &\vdots \\ a_n &= b_{n1}\beta_1 + \cdots b_{nm}\beta_m \end{aligned}$$

Substituindo as igualdades acima na igualdade 7.7 obtemos

$$\begin{aligned} u &= (b_{11}\beta_1 + \cdots + b_{1m}\beta_m)\alpha_1 + \cdots + \\ &= (b_{n1}\beta_1 + \cdots + b_{nm}\beta_m)\alpha_n \\ &= \sum_{1 \le i \le n, 1 \le j \le m} b_{ij}\alpha_i\beta_j. \end{aligned}$$

ii) γ é um conjunto linearmente independente: Seja dada uma combinação linear nula

$$\sum_{1 \le i \le n, 1 \le j \le m} b_{ij}\alpha_i\beta_j = 0$$

com $b_{ij} \in F$. Podemos escrever a igualdade acima na forma:

$$(b_{11}\beta_1 + \cdots + b_{1m}\beta_m)\alpha_1 + \cdots + (b_{n1}\beta_1 + \cdots + b_{nm}\beta_m)\alpha_n = 0.$$

em que $b_{i1}\beta_1 + \cdots + b_{im}\beta_m \in K$ para todo $i = 1, \ldots, n$. Mas, $\alpha_1, \ldots, \alpha_n$ são linearmente independentes sobre K

donde

$$\begin{aligned} b_{11}\beta_1 + \cdots b_{1m}\beta_m &= 0 \\ b_{21}\beta_1 + \cdots b_{2m}\beta_m &= 0 \\ &\vdots \\ b_{n1}\beta_1 + \cdots b_{nm}\beta_m &= 0 \end{aligned}$$

com $b_{ij} \in F$. Como $\beta_1, \ldots, \beta_m$ são linearmente independentes sobre F segue que $b_{ij} = 0$ para todo $i = 0 \ldots, n$ e para todo $j = 0, \ldots, m$.

2. Seja $\{E_i : i \in I\}$ uma família de subcorpos de um corpo K. Mostre que a interseção $\cap_{i\in I} E_i$ é um subcorpo de K.

   Solução: Os elementos 0_K e 1_K estão em cada E_i, $i \in I$, por definição de subcorpo. Logo, $0_K, 1_K \in \cap_{i\in I} E_i$. Dados $a, b \in \cap_{i\in I} E_i$, por definição de interseção, $a, b \in E_i$ para todo $i \in I$. Logo, $a \pm b, ab, a_{-1}$ (se $a \neq 0$) estão em cada E_i para todo $i \in I$ donde também estão em $\cap_{i\in I} E_i$. Como $\cap_{i\in I} E_i \subset K$, K corpo, então $\cap_{i\in I} E_i$ não possui divisores de zero. Assim, $\cap_{i\in I} E_i$ é corpo.

3. Se $u \in K$ mostre que $F(u^n) \subset F(u)$.

   Solução: Por definição, $F(u^n)$ é o menor corpo contendo F e u^n. Como $F(u)$ é o menor corpo contendo F e u segue que $F(u)$ contém F e toda potência u^n. Por minimalidade, $F(u^n) \subset F(u)$.

4. Se $v \in K$ e $c \in F$, mostre que $F(c + v) = F(v) = F(cv)$.

   Solução: Por definição, $F(c + v)$ contém F e $c + v$. Temos $v = c + v - c \in F(c+v)$ desde que $c, c+v \in F(c+v)$. Assim,

$F(c+v)$ é um corpo contendo F e v. Por minimalidade, $F(v) \subset F(c+v)$. Por outro lado, $F(v)$ contém c e v donde $c+v \in F(v)$. Daí, $F(c+v) \subset F(v)$ por minimalidade. Logo, $F(c+v) = F(v)$.

5. Mostre o fato 2: Sejam K, L extensões finitas do corpo F e $\varphi : K \to L$ um isomorfismos de corpos tal que $\varphi(c) = c$ para todo $c \in F$. Então, $[K : F] = [L : F]$.

   Solução: Com a hipótese $\phi(c) = c$ para todo $c \in F$, ϕ pode ser considerado como um isomorfismo de espaços vetoriais. Assim, L e K são espaços vetoriais sobre F isomorfos. Logo, têm a mesma dimensão.

6. Mostre que $\sqrt{i-\sqrt{2}} \in \mathbb{C}$ é algébrico sobre $\mathbb{Q}$.

   Solução: Denotando $\alpha = \sqrt{i-\sqrt{2}}$ e eliminando os radicais mostra-se que

   $$\alpha^8 - 2\alpha^4 - 3 = 0.$$

   Assim, $f(x) = x^8 - 2x^4 - 3 \in \mathbb{Q}[x]$ é não nulo e

   $$f(\sqrt{i-\sqrt{2}}) = f(\alpha) = \alpha^8 - 2\alpha^4 - 3 = 0.$$

7. Se $u, v \in K$ e $u+v$ é algébrico sobre F mostre que u é algébrico sobre $F(v)$.

   Solução: Por definição de elemento algébrico, existe um polinômio $f(x) \in F[x]$, não nulo, tal que $f(u+v) = 0$. Seja $f(x) = a_0 + a_1x + \cdots + x^n$, $a_i \in F$ e $n > 0$ (podemos supor $f(x)$ mônico). Então,

   $$f(u+v) = a_0 + a_1(u+v) + \cdots + (u+v)^n = 0.$$

   Efetuando as operações na equação acima obtemos

   $$f(u+v) = f(v) + b_1u + \cdots + b_{n-1}u^{n-1} + u^n = 0$$

em que $f(v), b_1, \ldots, b_{n-1} \in F(v)$. Assim,

$$g(x) = f(v) + b_1 x + \cdots + b_{n-1}x^{n-1} + x^n \in F(v)[x]$$

é não nulo e tem u como raiz. Logo, u é algébrico sobre $F(v)$.

8. Prove o fato 3: Seja F um corpo e seja $p(x) \in F[x]$ um polinômio irredutível sobre $F[x]$. Então,

   (a) Existe uma extensão K de F contendo uma raiz de $p(x)$.

   (b) Suponha K uma extensão de F contendo uma raiz α de $p(x)$. Seja $F(\alpha)$ o subcorpo de K gerado por F e α. Então,

   $$F(\alpha) \cong F[x]/(p(x)).$$

   Em particular, $F(\alpha) = F[\alpha]$.

   Solução:

   i) Se $p(x) \in F[x]$ é irredutível então $K = F[x]/(p(x))$ é uma extensão de F (pois $F \subset K$) na qual o elemento $\alpha = \overline{x}$ é raiz de $p(x) \in F[x] \subset K[x]$.

   ii) A função $\varphi_\alpha : F[x] \to K$, $\varphi_\alpha(f(x)) = f(\alpha)$, define um homomorfismo em que $p(x) \in \text{Ker } \varphi_\alpha$. Sendo $p(x)$ irredutível, o ideal $(p(x)) \subset F[x]$ é maximal e $(p(x)) \subset \text{Ker } \varphi_\alpha \subset F[x]$. Como Ker $\varphi_\alpha \subsetneq F[x]$ (as constantes não pertencem ao núcleo) segue da maximalidade de $(p(x))$ que Ker $\varphi_\alpha = (p(x))$. Assim,

$$\begin{aligned} F[x]/(p(x)) &\cong \text{Im } \varphi_\alpha \\ &= F[\alpha] \\ &= \{a_o + a_\alpha + \cdots + a_n\alpha^r : a_i \in F\} \\ &= \{a_o + a_\alpha + \cdots + a_{n-1}\alpha^{n-1} : \\ &\qquad a_i \in F,\ n = \deg p(x)\} \end{aligned}$$

(com tal expressão na última igualdade única). Mas, $F(\alpha)$ é corpo e contém F e α. Logo, contém todo elemento na forma $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}$. Assim, $F[\alpha] \subset F(\alpha)$. Por outro lado,

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

é corpo contendo F e α. Pela definição de $F(\alpha)$ como menor corpo contendo F e α temos $F(\alpha) \subset F[\alpha]$. Assim, $F(\alpha) = F[\alpha] \cong F[x]/(p(x))$.

9. Prove o fato 4: Seja K uma extensão de F e $\alpha \in K$. São equivalentes as afirmações abaixo a respeito de um polinômio $p(x) \in F[x]$:

   (a) $p(x)$ gera o núcleo do homomorfismo $\varphi_\alpha : F[x] \to F[\alpha]$, $f(x) \mapsto \varphi_\alpha(f(x)) = f(\alpha)$.

   (b) $p(x)$ é irredutível em $F[x]$ e tem α como raiz.

   (c) $p(x)$ é o polinômio de menor grau em $F[x]$ tendo α como raiz.

   Solução:

   (i) $\Leftrightarrow$ (ii) Por hipótese, Ker $\varphi_\alpha = (p(x))$. Por definição de núcleo, $p(\alpha) = 0$. Pelo teorema fundamental do isomorfismo, $F[x]/(p(x)) \cong F[\alpha] \subset K$. Assim, o anel quociente $F[x]/(p(x))$ é subanel do corpo K, logo é domínio. Isto mostra que o ideal $(p(x))$ é primo donde $p(x)$ é irredutível.

   (ii) $\Leftrightarrow$ (iii) A hipótese $p(x)$ irredutível em $F[x]$ implica $(p(x))$ ideal maximal em $F[x]$. A hipótese $p(\alpha) = 0$ implica

   $$(p(x)) \subset \text{ Ker } \varphi_\alpha \subsetneq F[x].$$

Isto mostra que $(p(x)) = \text{Ker } \varphi_\alpha$. Deste modo,

$f(\alpha) = 0 \Rightarrow f(x) \in \text{Ker } \varphi_\alpha = (p(x)) \Rightarrow f(x) = g(x)p(x)$, para algum $g(x) \in F[x] \Rightarrow \deg f(x) \geq \deg p(x)$.

(iii) ⇒ (i) Seja $\text{Ker } \varphi_\alpha = (q(x))$. Então, $p(\alpha) = 0 \Rightarrow p(x) \in \text{Ker } \varphi_\alpha \Rightarrow p(x) = q(x)g(x)$ para algum $g(x) \in F[x] \Rightarrow \deg p(x) \geq \deg q(x)$. Mas, $q(x)$ tem α como raiz e $p(x)$ é o polinômio de menor grau tendo α como raiz. Logo, $\deg q(x) \geq \deg p(x)$. Assim, $\deg q(x) = \deg p(x)$ e temos $\deg g(x) = 0$. Logo, $p(x) \sim q(x)$ donde $(p(x)) = (q(x)) = \text{Ker } \varphi_\alpha$.

10. Prove o fato 5: Sejam K uma extensão de F e $\alpha \in K$ algébrico sobre F com polinômio mínimo $m_{\alpha,F}(x) \in F[x]$ de grau n. Então,

    i) $F(\alpha) \cong F[\alpha] = F[x]/(m_{\alpha,F}(x))$.

    ii) $\{1_F, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base de $F(\alpha)$ sobre F.

    iii) $[F(\alpha) : F] = n$.

    Solução:

    i) Segue da implicação (iii) ⇒ (i) no fato 4.

    ii) Foi provado na observação 6.1 da aula 6.

    iii) Definição de grau de uma extensão e do item anterior.

11. Determine $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}]$.

    Solução: O polinômio $x^6 - 2 \in \mathbb{Q}[x]$ é irredutível (Eisenstein, $p = 2$) e tem $\sqrt[6]{2}$ como raiz. Então, $m_{\sqrt[6]{2},\mathbb{Q}}(x) = x^6 - 2$ donde $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = \deg m_{\sqrt[6]{2},\mathbb{Q}}(x) = 6$.

12. Determine o polinômio mínimo de $\sqrt{2} + i$ sobre $\mathbb{Q}$ e sobre $\mathbb{R}$.

Solução: Denotando $\alpha = \sqrt{2} + i$ e eliminando os radicais obtemos

$$\alpha^4 - 2\alpha^2 + 9 = 0.$$

Se $p(x) = x^4 - 2x^2 + 9 \in \mathbb{Q}[x]$ então $p(\alpha) = 0$. As possíveis raízes racionais de $p(x)$ são $\pm 1, \pm 3 \pm 9$. Mas, $p(\pm 1) = -10$, $p(\pm 3) = 54$ e $p(\pm 9) = 6.390$. Deste modo, $p(x)$ pode ser fatorado em $\mathbb{Q}[x]$ somente como um produto $p(x) = (x^2 + ax + b)(x^2 + cx + d)$ com $a, b, c, d \in \mathbb{Q}$. Tal igualdade acarreta nas equações:

$$\begin{aligned} a + c &= 0 && (7.8)\\ b + ad + d &= -2 && (7.9)\\ ad + bc &= 0 && (7.10)\\ bd &= -9. && (7.11) \end{aligned}$$

As equações 7.8 e 7.10 implica $a(d - b) = 0$ donde $a = 0$ ou $d = b$. Se $a = 0$ obtemos, usando as equações 7.9 e 7.11, a equação quadrática $b^2 + 2b - 9 = 0$ cujo discriminante é $\Delta = 40$. Logo, não possui soluções racionais. Por outro lado, se $b = d$, obtemos $b^2 = -9$. Assim, o sistema acima não admite soluções racionais e, portanto, $p(x)$ é mônico e irredutível em $\mathbb{Q}[x]$. Então $m_{\alpha,\mathbb{Q}}(x) = x^4 - 2x^2 + 9$. Vejamos sobre os reais. Como acima, $\alpha = \sqrt{2} + i$ implica $\alpha^2 - 2\sqrt{2}\alpha + 3 = 0$. Assim, $p(x) = x^2 - 2\sqrt{2}x + 3 \in \mathbb{R}[x]$ e tem discriminante $\Delta = -4$. Logo, $p(x) \in \mathbb{R}[x]$ é mônico e irredutível sobre $\mathbb{R}[x]$ donde $m_{\alpha,\mathbb{R}}(x) = x^2 - 2\sqrt{2}x + 3$.

13. Seja $\alpha \in K$ um elemento algébrico sobre F de grau ímpar. Mostre que $F(\alpha) = F(\alpha^2)$.

Solução: Suponha $F(\alpha) \neq F(\alpha^2)$. Desde que $F(\alpha) = F(\alpha^2)$ se e somente se $\alpha \in F(\alpha^2)$ temos $\alpha \notin F(\alpha^2)$. Então, o polinômio quadrático $x^2 - \alpha^2 \in F(\alpha^2)$ é mônico e tem raízes $\pm\alpha$ não pertencentes à $F(\alpha^2)$. Isto implica $x^2-\alpha^2$ irredutível sobre $F(\alpha^2)[x]$. Logo, $m_{\alpha,F(\alpha^2)}(x) = x^2 - \alpha^2$ e, portanto, $[F(\alpha) : F(\alpha^2)] = 2$. Daí,

$$[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)]F(\alpha^2) : F] = 2.[F(\alpha^2) : F]$$

donde $[F(\alpha) : F]$ é par, contradição.

7.6 Conclusão

A estrutura de espaço vetorial subjacente à uma extensão de corpos é fundamental no estudo de extensões de corpos. Destaca-se a noção do grau de uma extensão. Tal noção juntamente com a de polinômio mínimo nos fornece toda a estrutura de uma extensão simples.

RESUMO

Seja $F \subset K$ uma extensão de corpos.

Grau da extensão $F \subset K$:
$[K : F] = \dim_F K$ (dimensão de espaços vetoriais).

Multiplicatividade dos graus:
$F \subset K$ e $K \subset L$ finitas $\Rightarrow [L : F] = [L : K][K : F]$.

Caracterização do polinômio mínimo:
Seja $\alpha \in K$ algébrico sobre F e considere o homomorfismo

$$\varphi : F[x] \to K, f(x) \mapsto f(\alpha)$$

Dado $p(x) \in F[x]$, tem-se:

$$\begin{aligned} p(x) = m_{\alpha,F}(x) &\Leftrightarrow \text{Ker } \varphi = (p(x)) \\ &\Leftrightarrow p(x) \text{ irredutível e } p(\alpha) = 0 \end{aligned}$$

Estrutura de uma extensão algébrica simples:
Sejam K uma extensão de F e $\alpha \in K$ algébrico sobre F com polinômio mínimo $m_{\alpha,F}(x) \in F[x]$ de grau n. Então,

a) $F(\alpha) \cong F[\alpha] = F[x]/(m_{\alpha,F}(x))$.

b) $\{1_F, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ é uma base de $F(\alpha)$ sobre F.

c) $[F(\alpha) : F] = n$.

PRÓXIMA AULA

Estudaremos a noção de extensões de isomorfismo. Será de muita utilidade na determinação do grupo de Galois de uma extensão de corpos. No momento, será contextualizada para dar uma condição suficiente para caracterizar isomorfismo entre duas extensões simples.

ATIVIDADES

ATIV. 7.1. Mostre que $[K : F] = 1$ se e somente se $K = f$.

ATIV. 7.2. Mostre que $\{1, \overline{x}\}$ é uma base de $\mathbb{Z}_2[x]/(x^2 + x + 1)$ sobre $\mathbb{Z}_2$.

ATIV. 7.3. Se F, K, L são corpos tais que $F \subset K \subset L$ e $[L : F]$ é finita, mostre que $[K : F]$ é finita e $[K : L] \leq [L : F]$.

ATIV. 7.4. Se $[K : F] = p$, p primo, mostre que não existe corpo E tal que $F \subsetneq E \subsetneq K$.

ATIV. 7.5. Mostre que $\mathbb{Q}(2 - 3i) = \mathbb{Q}(1 + i)$.

ATIV. 7.6. Determine $[\mathbb{Q}(\sqrt[5]{7}) : \mathbb{Q}]$.

ATIV. 7.7. Se L é um corpo tal que $F \subset K \subset L$ e $v \in L$ é algébrico sobre F, mostre que v é algébrico sobre K.

ATIV. 7.8. Determine o polinômio mínimo de cada elemento a seguir sobre o corpo especificado:

a) $\sqrt{1 + \sqrt{5}}$ sobre $\mathbb{Q}$.

b) $\sqrt{3}i + \sqrt{2}$ sobre $\mathbb{Q}$.

c) $\sqrt{2} + i$ sobre $\mathbb{Q}$.

d) $\sqrt{2} + i$ sobre $\mathbb{R}$.

e) $\sqrt{5}$ sobre $\mathbb{Q}(\sqrt{3})$.

ATIV. 7.9. Se K é uma extensão de corpo de $\mathbb{Q}$ de grau 2, mostre que $K = \mathbb{Q}(\sqrt{d})$ para algum inteiro livre de quadrado d (livre de quadrado significa d não divisível por p^2 para todo primo p).

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.

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

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

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,

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

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

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

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 $\varphi : F \rightarrow F'$ 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

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

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

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

onde

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

A composição acima é um homomorfismo sobrejetivo, pois composição de homomorfimos sobrejetivos é homomorfismo sobreje-

tivo. 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:

$$F(\alpha) \xleftarrow{\pi} F[x]/(m_{\alpha,F}(x)) \xrightarrow{\Theta} F'(\alpha').$$

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

$$\begin{array}{rccc}
\sigma : & F(\alpha) & \xrightarrow{\sim} & F'(\alpha') \\
& \uparrow & & \uparrow \\
\varphi : & F & \xrightarrow{\sim} & F'
\end{array}$$

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

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

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

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

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

- 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.

AULA

Extensões algébricas

9

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 ⇒ 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 $1, \alpha, \alpha^2, \ldots, \alpha^n$ 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 $a_0, a_1, \ldots, a_n \in F$, 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 ⇒ algébrica ?

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

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

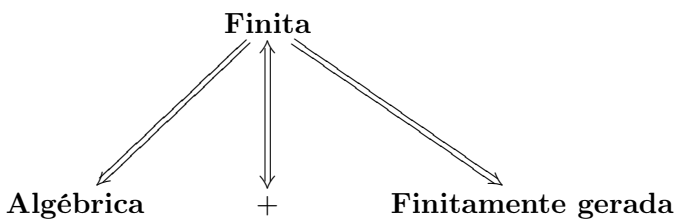
algébricos, isto é, transcendentes sobre $\mathbb{Q}$. Temos a inclusão própria $\overline{\mathbb{Q}}_{\mathbb{R}} \subsetneq \mathbb{R}$ donde $\overline{\mathbb{Q}}_{\mathbb{R}} \subsetneq \mathbb{C}$. Segue também que $\mathbb{R}$ é uma extensão infinita dos racionais.

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



Contra-exemplos:

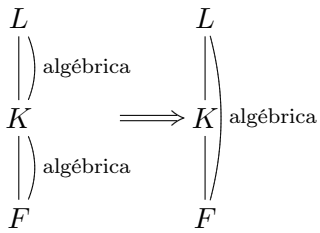
Algébrica $\not\Rightarrow$ Finita: $\overline{\mathbb{Q}}_{\mathbb{R}}$ sobre $\mathbb{Q}$.

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



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

ATIV. 9.2. Se $F \subset K$ é uma extensão finita e α é algébrico sobre K prove que $[K(\alpha) : K] \leq [F(\alpha) : F]$.

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.

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

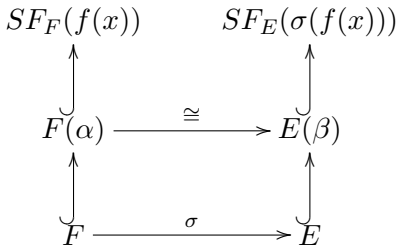
Teorema 10.2. *Seja $\sigma : F \to E$ um isomorfismo de corpos, $f(x) \in F[x]$ não constante, e $\sigma(f(x)) \in E[x]$. Então, σ estende-se à um isomorfismo $SF_F(f(x)) \cong SF_E(\sigma(f(x)))$.*

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 $SF_F(f(x)) \cong SF_E(\sigma(f(x)))$. □.

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). □

10.5 Corpo de raízes $\Leftrightarrow$ 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

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

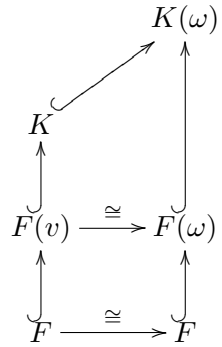
Assim, toda extensão normal e finita é o corpo de raízes de um polinômio. O resultado a seguir mostra que a recíproca é também verdadeira.

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.

AULA

Separabilidade

11

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 $\Leftrightarrow \text{MDC}(f, f') = 1$.

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.

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.

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 $Gal_{\mathbb{R}}\mathbb{C} = \{\iota, \tau\}$.

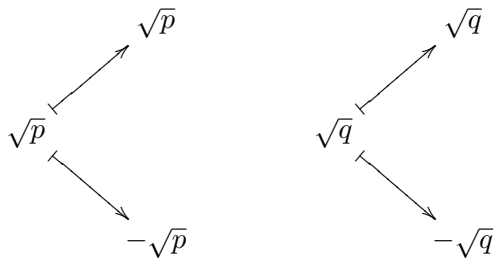
4. Finalmente, o fato 4 afirma que o grupo de Galois do corpo de raízes de um polinômio separável de grau n é um subgrupo de S_n. Neste caso, temos o isomorfismo $\phi : Gal_{\mathbb{R}}\mathbb{C} \to S_2$ definido por $\iota \mapsto \iota$ e $\tau \mapsto (12)$. Note que ambos os grupos são isomorfos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

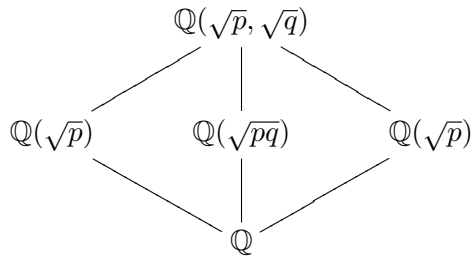
$$\begin{aligned} a+b\sqrt{p}+c\sqrt{q}+d\sqrt{pq} &= \sigma_3(a+b\sqrt{p}+c\sqrt{q}+d\sqrt{pq}) \\ &= a-b\sqrt{p}-c\sqrt{q}+d\sqrt{pq} \end{aligned}$$

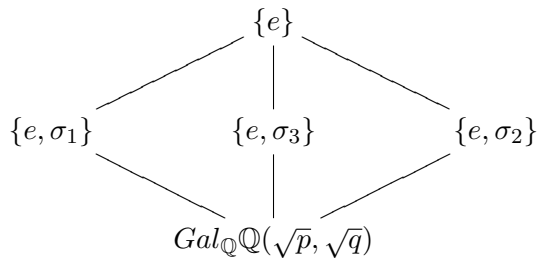
se e somente se $b=c=0$. Assim, $\Phi(<\sigma_2>)=\{a+d\sqrt{pq} \ : \ a,d\in\mathbb{Q}\}=\mathbb{Q}(\sqrt{pq})$. Temos mostrado a seguinte correspondência:

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.

AULA

13

O teorema fundamental da teoria de Galois

META:

Demonstrar o teorema fundamental da teoria de Galois.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Enunciar o teorema fundamental da teoria de Galois.

Determinar e exibir a correspondência de Galois de certas extensões.

PRÉ-REQUISITOS

Aula 12.

13.1 Introdução

Todo o esforço de nossos estudos serão compensados após apreciarmos os resultados desta aula. Na aula anterior, estabelecemos a correspondência de Galois $E \overset{\Gamma}{\longmapsto} \Gamma(E)$ e $H \overset{\Phi}{\longmapsto} \Phi(H)$ entre o conjunto de corpos intermediários de uma extensão $F \subset K$ e os subgrupos do grupo de Galois $Gal_F K = \Gamma(F)$. O teorema fundamental da teoria de Galois mostra que esta correspondência é biunívoca quando a extensão é finita, normal e separável. Uma extensão reunindo estas três propriedades é chamada extensão de Galois.

13.2 O Lema Principal

Lema 13.3. *Se $F \subset K$ é finita então K é simples, normal e separável sobre o corpo fixado de qualquer subgrupo H de $Gal_F K$.*

Prova: Esboço:
Seja H um subgrupo de $Gal_F K$ e $\Phi(H)$ seu corpo fixado.

1. K é algébrico sobre $\Phi(H)$.
2. Para cada $\alpha \in K$ e $\sigma \in H$, $\sigma(\alpha)$ é raiz do polinômio mínimo de α sobre $\Phi(H)$, $m_{\alpha,\Phi(H)}(x)$.
3. O conjunto das imagens de α por automorfismo em H é finito.
4. Sejam
$$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_t \in K$$
todas as imagens distintas de α por elementos em H. Então,
$$\sigma(\alpha_i) \in \{\alpha_1, \alpha_2, \ldots, \alpha_t\}$$
para todo $i = 1, 2, \ldots, t$ e a aplicação restrição
$$\sigma : \{\alpha_1, \alpha_2, \ldots, \alpha_t\} \to \{\alpha_1, \alpha_2, \ldots, \alpha_t\}$$

define uma permutação no conjunto $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ qualquer que seja $\sigma \in H$.

5. O polinômio

$$f(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_t)$$

é separável, tem α como raiz e $\sigma(f(x)) = f(x)$ para todo $\sigma \in H$. Logo, $f(x) \in \Phi(H)[x]$.

6. K é uma extensão separável de $\Phi(H)$ e finitamente gerada sobre $\Phi(H)$.

7. Pelo teorema do elemento primitivo, $K = \Phi(H)(\theta)$ para algum $\theta \in K$.

8. $K = \Phi(H)(\theta)$ é o corpo de raízes de $f(x)$ sobre $\Phi(H)$, logo, normal sobre $\Phi(H)$. $\square$

13.3 Sobrejetividade

Teorema 13.1. *Se $F \subset K$ é finita então $H = \Gamma(\Phi(H))$ e $|H| = [K : \Phi(H)]$ para todo subgrupo H de $Gal_F K$.*

Prova: $K = \Phi(H)(\theta)$ é normal e separável, pelo lema fundamental. Então,

$$[K : \Phi(H)] = \text{ deg } m_{\theta,\Phi(H)}(x) = n$$

com $m_{\theta,\Phi(H)}(x)$ separável e fatorando-se completamente sobre K. Se $\sigma \in \Gamma(\Phi(H))$ então σ fixa todos os elementos do corpo $\Phi(H)$. Em particular, fixa todos os coeficientes do polinômio $m_{\theta,\Phi(H)}(x)$. Então, para todo $\sigma \in \Gamma(\Phi(H))$, σ leva θ numa das n raízes distintas de $m_{\theta,\Phi(H)}(x)$. Desde que um automorfismo $\sigma \in \Gamma(\Phi(H))$ fica

completamente determinado pela imagem em θ, existem no máximo n elementos em $\Gamma(\Phi(H))$. Da inclusão $H \subset \Gamma(\Phi(H))$, segue as desigualdades

$$|H| \leq |\Gamma(\Phi(H))| \leq n = [K : \Phi(H)].$$

Seja

$$f(x) = (x - \theta)(x - \theta_2) \cdots (x - \theta_t)$$

como no esboço da prova do lema fundamental com $\alpha = \theta$. Então, existem ao menos t elementos em H, pela definição de $f(x)$. Além disso, $f(x) \in \Phi(H)[x]$ e tem θ como raiz. Então, $m_{\theta,\Phi(H)}(x)$ divide $f(x)$. Daí,

$$|H| \geq t = \text{ deg } f(x) \geq \text{ deg } m_{\theta,\Phi(H)}(x) = n = [K : \Phi(H)]$$

Combinando todas as desigualdades obtidas, temos

$$|H| \leq |\Gamma(\Phi(H))| \leq [K : \Phi(H)] \leq |H|.$$

Assim, $|H| = |\Gamma(\Phi(H))| = [K : \Phi(H)]$ e $H = \Gamma(\Phi(H))$. □

Corolário 13.1. *A correspondência de Galois é sobrejetiva para extensões finitas.* □

13.4 Injetividade

Lema 13.4. *Seja $F \subset E \subset K$ extensões de corpos. Se K é Galois sobre F então K é Galois sobre E.* □

Teorema 13.2. *Se $F \subset K$ é uma extensão de Galois então $E = \Phi(\Gamma(E))$ para todo corpo intermediário E.*

Prova: Temos $E \subset \Phi(\Gamma(E))$. Resta mostrar que $\Phi(\Gamma(E)) \subset E$, ou seja, $\forall x \in \Phi(\Gamma(E)) \Rightarrow x \in E$. Por contrapositiva, esta implicação

é equivalente à mostrar que se $x \notin E$ então $x \notin \Phi(\Gamma(E))$. Mas, por definição de corpo fixado, $x \notin \Phi(\Gamma(E))$ significa dizer que existe $\sigma \in \Gamma(E)$ tal que $\sigma(x) \neq x$. Assim, o resultado fica provado se conseguirmos mostrar a seguinte implicação:

$$x \notin E \Rightarrow \sigma(x) \neq x \text{ para algum } \sigma \in \Gamma(E).$$

Pelo lema acima, K é Galois sobre E. Assim, K é extensão algébrica de E. Seja $\alpha \in K$. Se $\alpha \notin E$, então $m_{\alpha,E}(x)$ tem grau ≥ 2 (se deg $m_{\alpha,E}(x) = 1$, α estaria em E). As raízes de $m_{\alpha,E}(x)$ são todas distintas por separabilidade, e todas estão em K por normalidade. Seja $\beta \in K$ uma outra raiz de $m_{\alpha,E}(x)$ distinta de α. Pelo fato 2 da seção 12.3, existe $\sigma \in \Gamma(E) = Gal_E K$ tal que $\sigma(\alpha) = \beta \neq \alpha$. Assim, $\alpha \notin \Phi(\Gamma(E))$, como queríamos demonstrar. □.

Corolário 13.2. *A correspondência de Galois é injetiva para extensões de Galois.* □

Corolário 13.3. *Seja K uma extensão finita sobre F. Então*

$$K \text{ é Galois sobre } F \iff F = \Phi(Gal_F K). \quad \square$$

13.5 O Teorema Fundamental

Teorema 13.3. *Se K é uma extensão de Galois sobre F, então:*

1. *Existe uma bijeção entre o conjunto de todos os corpos intermediários da extensão e os subgrupos do grupo de Galois $Gal_F K$, dada por associar à cada corpo intermediário E o subgrupo $\Gamma(E) = Gal_E K$.*

2. *Esta correspondência é reversa com respeito à inclusão, isto é, $E_1 \subset E_2$ se e somente se $\Gamma(E_2) \subset \Gamma(E_2)$.*

3. $[K : E] = |\Gamma(E)|$ *e* $[E : F] = |\Gamma(F) : \Gamma(E)|$, *para todo* E, $F \subset E \subset K$.

4. Um corpo intermediário E *é normal sobre* F *se e somente se* $\Gamma(E)$ *é um subgrupo normal de* $\Gamma(F)$, *e neste caso* $\Gamma(F)/\Gamma(E) \cong Gal_F E$.

Prova:

1. A bijetividade de tal correspondência já foi provada nas seções 13.3, 13.4.

2. i) $E_1 \subset E_2 \Rightarrow$ todo E_2-automorfismo de K é E_1-automorfismo de K, por definição de F-automorfismos $\Rightarrow \Gamma(E_2) \subset \Gamma(E_1)$.

   ii) Suponha $H_1 \subset H_2$. Se $x \in K$ é fixado por todo automorfismo em H_2, é, em particular, fixado por todo automorfismo em H_1. Assim, $\Phi(H_2) \subset \Phi(H_1)$.

3. Pelo teorema 13.2, $E = \Phi(\Gamma(E))$. Por outro lado, o teorema 13.1 diz que $|H| = [K : \Phi(H)]$. Fazendo $H = \Gamma(E)$, temos

$$[K : E] = [K : \Phi(\Gamma(E))] = |\Gamma(E)|.$$

   Em particular, se $F = E$, $[K : F] = |\Gamma(F)| = |Gal_F K|$. Pelo teorema de Lagrange,

$$\begin{aligned} [K : E][E : F] &= [K : F] \\ &= |Gal_F K| = |Gal_E K||Gal_F K : Gal_E K| \end{aligned}$$

   onde $|Gal_F K : Gal_E K|$ denota o índice do subgrupo $Gal_E K$ em $Gal_F K$. Dividindo a equação acima por $[K : E] = |Gal_E K|$ segue que $[E : F] = |Gal_F K : Gal_E K|$.

4. Suponha $Gal_E K \trianglelefteq Gal_F K$ (subgrupo normal). Se $p(x)$ é um polinômio irredutível em $F[x]$ com uma raiz α em E, devemos mostrar que $p(x)$ fatora-se em $E[x]$, ou seja, cada raiz β de $p(x)$ está em E. Como K é normal sobre F, sabemos que $p(x)$ fatora-se em $K[x]$. Existe um automorfismo $\sigma \in Gal_F K$ tal que $\sigma(\alpha) = \sigma(\beta)$, pois α e β têm mesmo polinômio mínimo (fato 2). Por definição de subgrupo normal, $\sigma Gal_E K = Gal_E K \sigma$. Deste modo, qualquer que seja $\tau \in Gal_E K$, existe $\tau_1 \in Gal_E K$ para o qual vale a igualdade $\tau \circ \sigma = \sigma \circ \tau_1$. Como $\alpha \in E$, temos

$$\tau(\beta) = \tau(\sigma(\alpha)) = \sigma(\tau_1(\alpha)) = \sigma(\alpha) = \beta$$

Assim, β é fixado por cada elemento de $\tau \in Gal_E K$. Logo, por definição de corpo fixado, $\beta \in \Phi(Gal_E K) = \Phi(\Gamma(E)) = E$.

Reciprocamente, suponha E normal sobre F. E é finito sobre F, pois $F \subset E \subset K$ e K é finito sobre F. Defina a aplicação

$$\varphi : Gal_F K \to Gal_F E$$

onde $\varphi(\sigma) = \sigma_{|_E}$ é a restrição de um F-automorfismo de K ao corpo E. Temos

i) φ está bem definida. De fato, seja $\sigma \in Gal_F K$. Devemos mostrar que $\sigma_{|_E} \in Gal_F E$. Observe que

   a) Dado $\alpha \in E$, seja $p(x) = m_{\alpha,F}(x)$. E é normal sobre F, logo, $p(x)$ fatora-se em $E[x]$. Assim, todas as raízes de $p(x)$ estão em E. Como $\sigma(\alpha)$ é raiz de $p(x)$ então $\sigma(\alpha) \in E$. Portanto, $\sigma(E) \subset E$ e $\sigma_{|_E}$ define um endomorfismo em E.

   b) Para todo $\alpha \in E$, σ define uma permutação no conjunto $\{\alpha = \alpha_1, \alpha_2, \ldots, \alpha_t\}$ das raízes do polinômio

mínimo $m_{\alpha,F}(x)$. Então, $\alpha = \sigma(\alpha_i)$ para algum $i = 1, 2 \ldots, t$. Pela normalidade de E sobre F, $\alpha_i \in E$. Isto mostra a sobrejetividade de $\sigma_{|_E}$.

Então, $\sigma_{|_E} : E \to E$ é um automorfismo. Como $\sigma \in Gal_F K$, σ fixa cada elemento de F. Logo, $\sigma_{|_E} \in Gal_F E$.

ii) $\varphi : Gal_F K \to Gal_F E$ é um homomorfismo sobrejetivo de grupos. Fica como exercício provar que φ é homomorfismo. Provaremos a sobrejetividade. Como K é uma extensão normal e finita sobre F, $K = SF_F(f(x))$ para algum $f(x) \in F[x]$. Desde que $F \subset E$, $K = SF_E(f(x))$. Consequentemente, cada $\tau \in Gal_F E$ pode ser estendido à um F-automorfismo $\sigma \in Gal_F K$ tal que $\sigma_{|_E} = \tau$ (ver teorema 10.2).

iii)

$$\begin{aligned} Ker\ \varphi &= \{\sigma \in\ Gal_F K\ :\ \sigma_{|_E} = I_E \text{ identidade em } E\} \\ &= \{\sigma \in Gal_F K\ :\ \sigma(x) = x\ \forall\ x \in E\} \\ &= \{\sigma \in Gal_F K\ : \sigma \in Gal_E K\} \\ &= Gal_E K \end{aligned}$$

Assim, $Gal_E K \trianglelefteq Gal_F K$.

v) Pelo teorema fundamental do isomorfismo,

$$Gal_F K / Gal_E K \cong Gal_F E. \quad \square$$

13.6 Conclusão

Em geral, finitude é suficiente para caracterizar a sobrejetividade na correspondência de Galois. As condições que faltam à finitude para determinar a injetividade são normalidade e separabilidade.

Além da bijetividade na correspondência de Galois para extensões de Galois, o teorema fundamental caracteriza a normalidade de um dado corpo intermediário E via normalidade do subgrupo associado $\Gamma(E)$. Tal relação completamente fechada entre duas estruturas distintas confere à teoria de Galois uma beleza estética e profundidade teórica raramente vista na história do pensamento humano.

RESUMO

Finitude $\Rightarrow$ sobrejetividade da correspondência de Galois.

Finitude + Normalidade + Separabilidade $\Rightarrow$ injetividade da correspondência de Galois.

TEOREMA FUNDAMETAL DA TEORIA DE GALOIS

Se K é uma extensão de Galois sobre F, então:

1. Existe uma bijeção entre o conjunto de todos os corpos intermediários da extensão e os subgrupos do grupo de Galois $Gal_F K$, dada por associar à cada corpo intermediário E o subgrupo $\Gamma(E) = Gal_E K$.
2. Esta correspondência é reversa com respeito à inclusão, isto é, $E_1 \subset E_2$ se e somente se $\Gamma(E_2) \subset \Gamma(E_2)$.
3. $[K : E] = |\Gamma(E)|$ e $[E : F] = |\Gamma(F) : \Gamma(E)|$, para todo E, $F \subset E \subset K$.
4. Um corpo intermediário E é normal sobre F se e somente se $\Gamma(E)$ é um subgrupo normal de $\Gamma(F)$, e neste caso $\Gamma(F)/\Gamma(E) \cong Gal_F E$.

PRÓXIMA AULA

Estudaremos a solubilidade por radicais de uma equação algébrica definida sobre um corpo de característica zero. Veremos que uma equação algébrica é solúvel por radicais se e somente se o grupo de Galois do polinômio $f(x)$ é um grupo solúvel.

ATIVIDADES

ATIV. 13.1. Prove todos os itens do esboço da prova do lema principal.

ATIV. 13.2. Mostre a sobrejetividade da correspondência de Galois para extensõs finitas.

ATIV. 13.3. Mostre o lema 13.4: Seja $F \subset E \subset K$ extensões de corpos. Se K é Galois sobre F então K é Galois sobre E.

ATIV. 13.4. Prove o corolário 13.3: Seja K uma extensão finita sobre F. Então

$$K \text{ é Galois sobre } F \iff F = \Phi(Gal_F K).$$

ATIV. 13.5. Se K é Galois sobre F mostre que existe uma quantidade finita de subcorpos intermediários.

ATIV. 13.6. Se K é uma extensão normal de grau primo sobre $\mathbb{Q}$ então $Gal_{\mathbb{Q}} k \cong \mathbb{Z}_n$.

ATIV. 13.7. Mostre que a aplicação $\varphi : Gal_F K \to Gal_F E$, $\sigma \mapsto \sigma_{|_E}$ define um homomorfismo de grupos.

ATIV. 13.8. Seja K uma extensão de Galois de F e E um corpo intermediário. Mostre que todo F-automorfismo $\tau : E \to E$ estende-se à um F-automorfismo $\sigma : K \to K$.

ATIV. 13.9. Determine a correspondência de Galois das seguintes extensões:

a) $\mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$.

b) $SF_{\mathbb{Q}}(x^2 + x + 1)$ sobre $\mathbb{Q}$.

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

d) $\mathbb{Q}(i, \sqrt{2})$ sobre $\mathbb{Q}$.

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.

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

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

AULA

14

Exemplos

META:

Ilustrar o teorema fundamental da teoria de Galois com algumas correspondências não triviais.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:
Compreender e reproduzir os exemplos apresentados no texto e determinar outras correspondências não triviais.

PRÉ-REQUISITOS

Além da Aula 13, o aluno deverá saber a estrutura de grupos finitos até ordem oito e determinar raízes complexas da unidade.

14.1 Introdução

Na aula anterior, vimos a teoria da correspondência de Galois. Nesta, a ilustraremos por meio de alguns exemplos não triviais. Você deverá estudar cada exemplo com atenção e preencher todos os detalhes. Aproveite para aplicar seus conhecimento sobre grupos de ordem até oito e raízes complexas da unidade.

14.2 Exemplo 1: $Gal_{\mathbb{Q}}(x^3 - 2)$

1. **Corpo de raízes de $x^3 - 2$ sobre $\mathbb{Q}$:**

   Se $w \in \mathbb{C}$ é uma raiz cúbica complexa da unidade ($w = -\frac{1}{2} + \frac{\sqrt[3]{2}i}{2}$, por exemplo) então $\sqrt[3]{2}$, $\sqrt[3]{2}w$ e $\sqrt[3]{2}w^2$ são todas as raízes de $x^3 - 2$. Assim,

   $$\begin{aligned} SF_{\mathbb{Q}}(x^3 - 2) &= \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2) \\ &= \mathbb{Q}(\sqrt[3]{2}, i) \end{aligned}$$

   Como $SF_{\mathbb{Q}}(x^3 - 2)$ é um corpo de raízes de um polinômio sobre um corpo de característica zero, então $SF_{\mathbb{Q}}(x^3 - 2)$ é Galois sobre $\mathbb{Q}$.

2. **Ordem do grupo de Galois:**

   $$\begin{aligned} |Gal_{\mathbb{Q}} SF_{\mathbb{Q}}(x^3 - 2)| &= [SF_{\mathbb{Q}}(x^3 - 2) : \mathbb{Q}] \\ &= [\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \\ &= 2.3 = 6. \end{aligned}$$

3. **Elementos de $Gal_{\mathbb{Q}}(x^3 - 2)$:**

Tendo em mente o diagrama:

$$\begin{array}{c} \mathbb{Q}(\sqrt[3]{2}, w) \\ | \\ \mathbb{Q}(\sqrt[3]{2}) \\ | \\ \mathbb{Q} \end{array}$$

sabemos que um elemento $\sigma \in Gal_{\mathbb{Q}} SF_{\mathbb{Q}}(x^3 - 2)$ fica completamente determinado pelas imagens em $\sqrt[3]{2}$ e w. Sabemos também que $\sigma(\sqrt[3]{2})$ e $\sigma(w)$ são raízes, respectivamente, dos polinômios $m_{\sqrt[3]{2},\mathbb{Q}(x)} = x^3 - 2$ e $m_{w,\mathbb{Q}(x)} = x^2 + x + 1$. Então,

$$\begin{aligned} \sigma(\sqrt[3]{2}) &= \sqrt[3]{2},\ \sqrt[3]{2}w,\ \text{ou}\ \sqrt[3]{2}w^2 \\ \sigma(w) &= w,\ \text{ou}\ w^2 \end{aligned}$$

As combinações entre estas imagens nos dão seis possíveis elementos para $Gal_{\mathbb{Q}} SF_{\mathbb{Q}}(x^3 - 2)$. Como

$$|Gal_{\mathbb{Q}} SF_{\mathbb{Q}}(x^3 - 2) = 6,$$

necessariamente existem estes seis elementos. São eles:

$$\begin{array}{ccc|ccc|ccc} \sqrt[3]{2} & \overset{\iota}{\longmapsto} & \sqrt[3]{2} & \sqrt[3]{2} & \overset{\sigma_1}{\longmapsto} & \sqrt[3]{2}w & \sqrt[3]{2} & \overset{\sigma_2}{\longmapsto} & \sqrt[3]{2}w^2 \\ w & \longmapsto & w & w & \longmapsto & w & w & \longmapsto & w \end{array}$$

$$\begin{array}{ccc|ccc|ccc} \sqrt[3]{2} & \overset{\sigma_3}{\longmapsto} & \sqrt[3]{2} & \sqrt[3]{2} & \overset{\sigma_4}{\longmapsto} & \sqrt[3]{2}w & \sqrt[3]{2} & \overset{\sigma_5}{\longmapsto} & \sqrt[3]{2}w^2 \\ w & \longmapsto & w^2 & w & \longmapsto & w^2 & w & \longmapsto & w^2 \end{array}$$

Note que $\sigma_1^2 = \sigma_2$, $\sigma_1^3 = \sigma_3^2 = \iota$, $\sigma_1 \circ \sigma_3 = \sigma_4$, $\sigma_1^2 \circ \sigma_3 = \sigma_5$ e $\sigma_3 \circ \sigma_1 = \sigma_5 = \sigma_1^2 \circ \sigma_3$. Denotando $\sigma_1 = \theta$ e $\sigma_3 = r$ obtemos

$$\begin{aligned} Gal_{\mathbb{Q}}(x^3 - 2) &= \{\iota, r, \theta, \theta^2, r\theta, r\theta^2\} \\ &= < r, \theta\ :\ r^2 = \theta^3 = \iota,\ r\theta = \theta^2 r > \end{aligned}$$

Assim, $Gal_{\mathbb{Q}}(x^3-2) \cong D_3$, o grupo de simetrias de um triângulo.

4. **A correspondência de Galois:**

   (a) Subgrupos do grupo $Gal_{\mathbb{Q}}(x^3-2)$:

   $$\{\{\iota\}, \{\iota, \theta, \theta^2\}, \{\iota, r\}, \{\iota, r\theta\}, \{\iota, r\theta^2\}, Gal_{\mathbb{Q}}(x^3-2)\}$$

   ou em termos de geradores

   $$\{<\iota>, <\theta>, <r>, <r\theta>, <r\theta^2>, <r, \theta>\}$$

   (b) Subcorpos correspondentes: Seja

   $$\{1, \sqrt[3]{2}, \sqrt[3]{2}^2, w, w\sqrt[3]{2}, w\sqrt[3]{2}^2\}$$

   uma base de $SF_{\mathbb{Q}}(x^3-2)$ sobre $\mathbb{Q}$.

   i. $\Phi(<\theta>)$: Temos $w^2 = -1-w$, desde que w é raiz da equação $x^2+x+1=0$. Então, $\theta(x) = x$ se e somente se

   $$a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 + dw + ew\sqrt[3]{2} + fw\sqrt[3]{2}^2 =$$
   $$a - e\sqrt[3]{2} + (f-c)\sqrt[3]{4} + dw + (b-e)w\sqrt[3]{2} - cw\sqrt[3]{4}.$$

   Isto ocorre se e somente se $b = c = f = e = 0$. Assim, $\theta(x) = x$ se e somente se

   $$x = a + dw \in \mathbb{Q}(w)$$

   donde $\Phi(<\theta>) = \mathbb{Q}(w)$.

   Analogamente se determina os outros corpos fixados e obtém-se a seguinte correspondência:

Subgrupos		Corpos fixados
$\{\iota\}$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[3]{2}, w)$
$< r >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[3]{2})$
$< r\theta >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[3]{2}w)$
$< r\theta^2 >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[3]{2}w^2)$
$< \theta >$	$\longleftrightarrow$	$\mathbb{Q}(w)$
$< r, \theta >$	$\longleftrightarrow$	$\mathbb{Q}$

14.3 Exemplo 2: $Gal_{\mathbb{Q}}(x^4 - 2)$

1. **Corpo de raízes de $x^4 - 2$ sobre $\mathbb{Q}$:**

$$SF_{\mathbb{Q}}(x^4 - 2) = \mathbb{Q}(\sqrt[4]{2}, i)$$

2. **Ordem do grupo de Galois:**

$$\begin{aligned} |Gal_{\mathbb{Q}} SF_{\mathbb{Q}}(x^4 - 2)| &= [SF_{\mathbb{Q}}(x^4 - 2) : \mathbb{Q}] \\ &= [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] \\ &= 2.4 = 8. \end{aligned}$$

Exemplos

3. **Elementos de** $Gal_{\mathbb{Q}}(x^4-2)$**:**

$$\begin{array}{ccc} \sqrt[4]{2} & \overset{\iota}{\longmapsto} & \sqrt[4]{2} \\ i & \longmapsto & i \end{array} \qquad \begin{array}{ccc} \sqrt[4]{2} & \overset{\theta}{\longmapsto} & \sqrt[4]{2}i \\ i & \longmapsto & i \end{array}$$

$$\begin{array}{ccc} \sqrt[4]{2} & \overset{\theta^2}{\longmapsto} & -\sqrt[4]{2} \\ i & \longmapsto & i \end{array} \qquad \begin{array}{ccc} \sqrt[4]{2} & \overset{\theta^3}{\longmapsto} & -\sqrt[4]{2}i \\ i & \longmapsto & i \end{array}$$

$$\begin{array}{ccc} \sqrt[4]{2} & \overset{r}{\longmapsto} & \sqrt[4]{2} \\ i & \longmapsto & -i \end{array} \qquad \begin{array}{ccc} \sqrt[4]{2} & \overset{\theta r}{\longmapsto} & \sqrt[4]{2}i \\ i & \longmapsto & -i \end{array}$$

$$\begin{array}{ccc} \sqrt[4]{2} & \overset{\theta^2 r}{\longmapsto} & -\sqrt[4]{2} \\ i & \longmapsto & -i \end{array} \qquad \begin{array}{ccc} \sqrt[4]{2} & \overset{\theta^3 r}{\longmapsto} & -\sqrt[4]{2}i \\ i & \longmapsto & -i \end{array}$$

4. **Correspondência de Galois:**

	Subgrupos		Corpos fixados
ordem 1 :	$\{\iota\}$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[4]{2}, w)$
ordem 2 :	$< r >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[4]{2})$
	$< \theta^2 >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt{2}, i) = SF_{\mathbb{Q}}(t^4 - t^2 - 2)$
	$< \theta r >$	$\longleftrightarrow$	$\mathbb{Q}((1+i)\sqrt[4]{2})$
	$< \theta^2 r >$	$\longleftrightarrow$	$\mathbb{Q}(i\sqrt[4]{2})$
	$< \theta^3 r >$	$\longleftrightarrow$	$\mathbb{Q}((1-i)\sqrt[4]{2})$
Ordem 4 :	$< \theta >$	$\longleftrightarrow$	$\mathbb{Q}(i) = SF_{\mathbb{Q}}(t^2+1)$
	$< r, \theta^2 >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt{2}) = SF_{\mathbb{Q}}(t^2-2)$
	$< r, r\theta >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt{2}i) = SF_{\mathbb{Q}}(t^2+2)$
Ordem 8 :	$< r, \theta >$	$\longleftrightarrow$	$\mathbb{Q}$

14.4 Exemplo 3: $Gal_{\mathbb{Q}}(x^8-2)$

Corpo de raízes de x^8-2 sobre $\mathbb{Q}$:

$$SF_{\mathbb{Q}}(x^8-2)=\mathbb{Q}(\sqrt[8]{2},i)$$

Ordem do grupo de Galois:

$$|Gal_{\mathbb{Q}}(x^8-2)|=[\mathbb{Q}(\sqrt[8]{2},i):\mathbb{Q}]=16.$$

Elementos do grupo de Galois: Um elemento do grupo de Galois $Gal_{\mathbb{Q}}SF_{\mathbb{Q}}(x^8-2)$ é determinado por sua ação sobre $\alpha=\sqrt[8]{2}$ e i. Sabemos ainda que tal ação leva α numa raiz de seu polinômio mínimo $m_{\alpha,\mathbb{Q}}(x)=x^8-2$ (irredutível por Eiseinstein, $p=2$) e leva i em $\pm i$. Sejam $\sqrt[8]{2}$, $\sqrt[8]{2}w,\ldots,\sqrt[8]{2}w^7$ onde $w=\dfrac{1}{2}+\dfrac{\sqrt{2}i}{2}$ é uma raíz oitava complexa da unidade. Deste modo existem exatamente 16 possibilidades.

$$\begin{cases} \alpha \overset{\iota}{\longmapsto} \alpha \\ i \longmapsto i \\ w \longmapsto w \end{cases} \qquad \begin{cases} \alpha \overset{r}{\longmapsto} \alpha \\ i \longmapsto -i \\ w \longmapsto w^7 \end{cases}$$

$$\begin{cases} \alpha \overset{\theta}{\longmapsto} \alpha w \\ i \longmapsto i \\ w \longmapsto w^5 \end{cases} \qquad \begin{cases} \alpha \overset{r\theta}{\longmapsto} \alpha w^7 \\ i \longmapsto -i \\ w \longmapsto w^3 \end{cases}$$

$$\begin{cases} \alpha & \overset{\theta^2}{\longmapsto} & \alpha w^6 \\ i & \longmapsto & i \\ w & \longmapsto & w \end{cases} \quad \begin{cases} \alpha & \overset{r\theta^2}{\longmapsto} & \alpha w^2 \\ i & \longmapsto & -i \\ w & \longmapsto & w^7 \end{cases}$$

$$\begin{cases} \alpha & \overset{\theta^3}{\longmapsto} & \alpha w^7 \\ i & \longmapsto & i \\ w & \longmapsto & w^5 \end{cases} \quad \begin{cases} \alpha & \overset{r\theta^3}{\longmapsto} & \alpha w \\ i & \longmapsto & -i \\ w & \longmapsto & w^3 \end{cases}$$

$$\begin{cases} \alpha & \overset{\theta^4}{\longmapsto} & -\alpha \\ i & \longmapsto & i \\ w & \longmapsto & w \end{cases} \quad \begin{cases} \alpha & \overset{r\theta^4}{\longmapsto} & -\alpha \\ i & \longmapsto & -i \\ w & \longmapsto & w^7 \end{cases}$$

$$\begin{cases} \alpha & \overset{\theta^5}{\longmapsto} & \alpha w^5 \\ i & \longmapsto & i \\ w & \longmapsto & w^5 \end{cases} \quad \begin{cases} \alpha & \overset{r\theta^5}{\longmapsto} & -\alpha \\ i & \longmapsto & -i \\ w & \longmapsto & w^3 \end{cases}$$

$$\begin{cases} \alpha & \overset{\theta^6}{\longmapsto} & \alpha w^2 \\ i & \longmapsto & i \\ w & \longmapsto & w \end{cases} \quad \begin{cases} \alpha & \overset{r\theta^6}{\longmapsto} & \alpha w^6 \\ i & \longmapsto & -i \\ w & \longmapsto & w^7 \end{cases}$$

$$\begin{cases} \alpha & \overset{\theta^7}{\longmapsto} & \alpha w^3 \\ i & \longmapsto & i \\ w & \longmapsto & w^5 \end{cases} \quad \begin{cases} \alpha & \overset{r\theta^7}{\longmapsto} & \alpha w^5 \\ i & \longmapsto & -i \\ w & \longmapsto & w^3 \end{cases}$$

Para computar a imagem de w perante os isomorfismos acima consideramos a relação $w = \frac{1}{2}(1+i)\alpha^4$. Como existem exatos 16 elementos no grupo de Galois e os que existem estão entre estes 16 acima, os 16 isomorfismos acima existem e compõem o grupo de galois do polinômio $x^8 - 2$. Temos ainda as re-

lações $\theta^8 = r^2 = \iota$ e $\alpha r = r\alpha^3$. Assim, temos mostrado que

$$Gal_{\mathbb{Q}}(x^8 - 2) = \left\langle r, \theta \ : \ \theta^8 = r^2 = \iota, \alpha r = r\alpha^3 \right\rangle$$

Correspondência de Galois:

Subgrupos		Corpos fixados
ordem 1 :		
$\{\iota\}$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[8]{2}, i)$
ordem 2 :		
$< r\theta^2 >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[8]{2}w)$
$< r\theta^6 >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[8]{2}w^3)$
$< r\theta^4 >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[8]{2}w^2)$
$< r >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[8]{2})$
$< \theta^4 >$	$\longleftrightarrow$	$\mathbb{Q}(i, \sqrt[4]{2})$
Ordem 4 :		
$< \theta^4, r\theta^6 >$	$\longleftrightarrow$	$\mathbb{Q}(i\sqrt[4]{2})$
$< \theta^4, r >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[4]{2})$
$< \theta^2 >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt{2}, i)$
$< r\theta^3 >$	$\longleftrightarrow$	$\mathbb{Q}((1+i)\sqrt[4]{2})$
$< r\theta >$	$\longleftrightarrow$	$\mathbb{Q}((1-i)\sqrt[4]{2})$
Ordem 8 :		
$< r, \theta^2 >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt{2})$
$< \theta >$	$\longleftrightarrow$	$\mathbb{Q}(i)$
$< r\theta^3, \theta^2 >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt{-2})$
Ordem 16 :		
$Gal_{\mathbb{Q}}(x^8 - 2)$	$\longleftrightarrow$	$\mathbb{Q}$

14.5 Conclusão

Determinar a correspondência de Galois é uma tarefa trabalhosa e requer um bom conhecimento da teoria dos grupos finitos. É, portanto, uma excelente oportunidade para colocarmos em prática nossos conhecimentos sobre teoria elementar de grupos.

RESUMO

$Gal_{\mathbb{Q}}(x^3 - 2) \cong D_3$

Correspondência de Galois

Subgrupos		Corposfixados
$\{\iota\}$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[3]{2}, w)$
$< r >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[3]{2})$
$< r\theta >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[3]{2}w)$
$< r\theta^2 >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[3]{2}w^2)$
$< \theta >$	$\longleftrightarrow$	$\mathbb{Q}(w)$
$< r, \theta >$	$\longleftrightarrow$	$\mathbb{Q}$

$Gal_{\mathbb{Q}}(x^4 - 2) \cong D_4$

Correspondência de Galois

	Subgrupos		Corposfixados
ordem 1 :	$\{\iota\}$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[4]{2}, w)$

$$
\begin{array}{lccc}
\text{ordem } 2: & < r > & \longleftrightarrow & \mathbb{Q}(\sqrt[4]{2}) \\
& < \theta^2 > & \longleftrightarrow & \mathbb{Q}(\sqrt{2}, i) = SF_{\mathbb{Q}}(t^4 - t^2 - 2) \\
& < \theta r > & \longleftrightarrow & \mathbb{Q}((1+i)\sqrt[4]{2}) \\
& < \theta^2 r > & \longleftrightarrow & \mathbb{Q}(i\sqrt[4]{2}) \\
& < \theta^3 r > & \longleftrightarrow & \mathbb{Q}((1-i)\sqrt[4]{2}) \\
\text{Ordem } 4: & < \theta > & \longleftrightarrow & \mathbb{Q}(i) = SF_{\mathbb{Q}}(t^2 + 1) \\
& < r, \theta^2 > & \longleftrightarrow & \mathbb{Q}(\sqrt{2}) = SF_{\mathbb{Q}}(t^2 - 2) \\
& < r, r\theta > & \longleftrightarrow & \mathbb{Q}(\sqrt{2}i) = SF_{\mathbb{Q}}(t^2 + 2) \\
\text{Ordem } 8: & < r, \theta > & \longleftrightarrow & \mathbb{Q}
\end{array}
$$

$Gal_{\mathbb{Q}}\mathbb{Q}(\sqrt[8]{2}, i)$:

Correspondência de Galois:

	Subgrupos		Corposfixados
ordem 1 :			
	$\{\iota\}$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[8]{2}, i)$
ordem 2 :			
	$< r\theta^2 >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[8]{2}w)$
	$< r\theta^6 >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[8]{2}w^3)$
	$< r\theta^4 >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[8]{2}w^2)$
	$< r >$	$\longleftrightarrow$	$\mathbb{Q}(\sqrt[8]{2})$
	$< \theta^4 >$	$\longleftrightarrow$	$\mathbb{Q}(i, \sqrt[4]{2})$

Exemplos

Ordem 4 :

$$\begin{array}{ccc} <\theta^4, r\theta^6> & \longleftrightarrow & \mathbb{Q}(i\sqrt[4]{2}) \\ <\theta^4, r> & \longleftrightarrow & \mathbb{Q}(\sqrt[4]{2}) \\ <\theta^2> & \longleftrightarrow & \mathbb{Q}(\sqrt{2}, i) \\ <r\theta^3> & \longleftrightarrow & \mathbb{Q}((1+i)\sqrt[4]{2}) \\ <r\theta> & \longleftrightarrow & \mathbb{Q}((1-i)\sqrt[4]{2}) \end{array}$$

Ordem 8 :

$$\begin{array}{ccc} <r, \theta^2> & \longleftrightarrow & \mathbb{Q}(\sqrt{2}) \\ <\theta> & \longleftrightarrow & \mathbb{Q}(i) \\ <r\theta^3, \theta^2> & \longleftrightarrow & \mathbb{Q}(\sqrt{-2}) \end{array}$$

Ordem 16 :

$$Gal_{\mathbb{Q}}(x^8 - 2) \longleftrightarrow \mathbb{Q}$$

PRÓXIMA AULA

Apresentaremos o critério de solubilidade por radicais de Galois para equações algébricas.

ATIVIDADES

ATIV. 14.1. Para cada exemplo desta aula, mostre que cada corpo intermediário é de fato o corpo fixado do subgrupo correspondente. Determine ainda os corpos intermediários que são normais sobre o corpo base.

ATIV. 14.2. Mostre que $Gal_{\mathbb{Q}}SF_{\mathbb{Q}}(x^4-2) \cong D_4$ e determine a correspondência de Galois de $SF_{\mathbb{Q}}(x^4-2)$ sobre $\mathbb{Q}$. Mostre também que $Gal_{\mathbb{Q}(i)}SF_{\mathbb{Q}}(x^4-2) \cong \mathbb{Z}_4$.

ATIV. 14.3. Determine a correspondência de Galois de $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ sobre $\mathbb{Q}$.

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.

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

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

AULA

Solubilidade por Radicais 15

META:

Apresentar o critério de solubilidade por radicais de Galois para equações algébricas.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

Enunciar o critério de Galois.

Exibir uma quíntica não solúvel por radicais.

PRÉ-REQUISITOS

Aula 14, teorema de Cauchy sobre p-grupos, grupos de permutações e o uso de derivadas para construção de Gráficos de funções.

15.1 Introdução

A expressão

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

é bastante conhecida por você. É a fórmula para a solução da equação quadrática $ax^2+bx+c = 0$ sobre os reais (poderia ser sobre corpos de característica $\neq 2$). Embora muito menos conhecidas, existem fórmulas análogas para a solução de equações algébricas de grau 3 e 4. A analogia consiste em que tais fórmulas envolvem somente as operações definidas sobre um corpo (adição, subtração, multiplicação e divisão) e extração de raízes. Equações assim resolvidas (por meio de fórmulas envolvendo radicais e operações elementares no corpo) ficaram conhecidas por *equações solúveis por radicais* e o processo, bem como o problema de determinar tais soluções, foi chamado *solubilidade por radicais.*

A disparidade entre a simplicidade para obtenção da fórmula para equações quadráticas e a engenhosidade e complexidade para solubilidade das equações cúbicas e quárticas instigou matemáticos de várias gerações. De 1600 A.C. à 1771. O problema tornou-se ainda mais instigante quando Ruffini e Abel exibiram independentemente quínticas (equações algébricas de grau 5) não solúveis por radicais. Isto foi em torno de 1820. Extinguia-se o sonho de se obter fórmulas radicais para resolver uma equação algébrica geral de grau n.

O balde de água fria jogado por Abel e Ruffini no problema da solubilidade de equações algébricas não foi suficiente para fazer os matemáticos desistirem completamente do problema. Muito pelo contrário, apenas tornou o problema ainda mais desafiador: saber se uma dada equação algébrica de grau $n \geq 5$ seria ou não solúvel por radicais. Por volta de 1830, Évarist Galois(1811-1832) resolveu

por completo o problema exibindo seu critério de solubilidade.

15.2 Grupos Solúveis

15.2.1 Definição

Um grupo G é dito solúvel se existe uma cadeia de subgrupos

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n = \{e\}$$

na qual cada G_i é um subgrupo normal do grupo precedente G_{i-1} e o grupo quociente G_{i-1}/G_i é abeliano.

15.2.2 Exemplos

1. Todo grupo abeliano G é solúvel, pois $G \supseteq \{e\}$ satisfaz as condições requeridas.

2. S_3 é solúvel. De fato, $< (123) >$ é um subgrupo normal de G de ordem 3 (verifique!) e a cadeia

   $$S_3 \supseteq < (123) > \supseteq \{e\}$$

   é tal que $S_3/ < (123) >$ é abeliano (ordem 2) e $< (123) > /\{e\} =< (123) >$ é abeliano (grupo cíclico).

3. Seja F um corpo de característica zero e ω uma raiz primitiva da unidade. A extensão $K = F(\zeta)$ é o corpo de raízes do polinômio $x^n - 1$, logo normal. Desde que F tem característica zero, K é separável sobre F. Então, K é de Galois sobre F. O grupo de Galois $Gal_F K$ é solúvel. De fato, quaisquer que sejam $\sigma, \tau \in Gal_F K$, $\sigma(\zeta)$ e $\tau(\zeta)$ são raízes de $x^n - 1$, logo são potências de ζ (ζ é raiz primitiva!). Assim,

   $$\sigma \circ \tau(\zeta) = \sigma(\tau(\zeta)) = \sigma(\zeta^r) = \sigma(\zeta)^r = (\zeta^s)^r = \zeta^{rs}$$

$$\tau \circ \sigma(\zeta) = \tau(\sigma(\zeta)) = \tau(\zeta^s) = \tau(\zeta)^s = (\zeta^r)^s = \zeta^{rs}$$

donde $\sigma \circ \tau = \tau \circ \sigma$. Então, $Gal_F K$ é abeliano, logo solúvel.

15.2.3 Fatos

1. S_n não é solúvel para $n \geq 5$.

2. Imagem homomórfica de um grupo solúvel é solúvel.

15.3 Extensões Radicais

15.3.1 Definição

Um corpo K é dito ser uma extensão radical de um corpo F se existe uma cadeia de corpos

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r = K$$

na qual para cada $i = 1, 2, \ldots, r$, tem-se $F_i = F_{i-1}(\alpha_i)$ com $\alpha_i^m \in F_{i-1}$ para algum inteiro m.

15.3.2 Exemplos

1. Toda extensão quadrática (grau dois) é radical. (Atividade)

2. $\mathbb{Q}(\sqrt{5}, \sqrt[7]{1-\sqrt{2}}, \sqrt[7]{1+\sqrt{2}})$ é extensão normal de $\mathbb{Q}$.

15.3.3 Fatos

1. Seja F, E, L corpos de característica zero com $F \subseteq E \subseteq L = E(\alpha)$ e $\alpha^k \in E$. Se L é finita sobre F e E é normal sobre F, então existe uma extensão M de L que é radical sobre E e normal sobre F.

2. Seja F um corpo de característica zero e $f(x) \in F[x]$. Se $f(x) = 0$ é solúvel por radicais, então existe uma extensão radical normal de F contendo um corpo de raízes de $f(x)$.

15.4 O Critério de Solubilidade de Galois

Seja F um corpo de característica zero e $f(x) \in F[x]$. Então, $f(x)$ é solúvel por radicais $\Longleftrightarrow$ o grupo de Galois de $f(x)$ é solúvel.

A prova deste resultado é parte de um curso de pós-graduação. Para o que precisaremos na próxima seção segue um esboço para a prova da condição necessária.

1. Existe uma extensão normal radical K de F contendo $SF_F(f(x))$ (Fato 2).

2. $SF_F(f(x))$ é normal sobre F. (Caracterização de extensões normais via corpos de raízes)

3. $Gal_F SF_E(f(x))$ é solúvel.

OBS 15.1. O último item no esboço da prova acima admite a seguinte generalização:

> Seja K uma extensão radical normal de F, ambos de característica zero. Então, $Gal_F E$ é solúvel para todo corpo intermediário E normal sobre F.

15.5 Uma quíntica não solúvel por radicais

O grupo de galois do polinômio $f(x) = 2x^5 - 10x + 5 \in \mathbb{Q}[x]$ é isomorfo à S_5, não solúvel. Consequentemente, a equação

$$f(x) = 2x^5 - 10x + 5 = 0$$

não é solúvel por radicais. Deste modo,

> Não existe uma fórmula envolvendo somente as operações definidas no corpo e extração de raízes para a solução de uma equação algébrica geral de grau 5.

Para ver que $Gal_F(f(x))$ é isomorfo à S_5 siga os seguintes passos:

1. Usando a técnica de derivadas aprendida no cálculo I, mostre que ± 1 são os pontos críticos (reais) de $f(x) = 0$.

2. Pelo uso da segunda derivada, mostre que $f(x) = 0$ admite um único máximo relativo em $x = -1$, um único mínimo relativo em $x = 1$ e um ponto de inflexão em $x = 0$. (Esboce o gráfico)

3. Conclua que a equação $f(x) = 0$ admite exatamente três raízes reais distintas. Use o teorema do valor médio para funções contínuas.

4. Mostre que $f(x)$ é irredutível em $\mathbb{Q}[x]$.

5. Sabemos que $Gal_{\mathbb{Q}} SF_{\mathbb{Q}}(f(x)) = [SF_{\mathbb{Q}}(f(x)) : \mathbb{Q}]$ (Teorema fundamental da teoria de Galois).

6. Se α é qualquer raiz de $f(x)$ então $m_{\alpha,\mathbb{Q}}(x) = f(x)$. Logo,

$[\mathbb{Q}(\alpha):\mathbb{Q}]=5$. Assim,

$$\begin{aligned} Gal_{\mathbb{Q}}SF_{\mathbb{Q}}(f(x)) &= [SF_{\mathbb{Q}}(f(x)):\mathbb{Q}] \\ &= [SF_{\mathbb{Q}}(f(x)):\mathbb{Q}(\alpha)][\mathbb{Q}(\alpha):\mathbb{Q}] \\ &= 5[SF_{\mathbb{Q}}(f(x)):\mathbb{Q}(\alpha)] \end{aligned}$$

Então, 5 é primo e divide a ordem do grupo $Gal_{\mathbb{Q}}SF_{\mathbb{Q}}(f(x))$. Pelo teorema de Cauchy, $Gal_{\mathbb{Q}}SF_{\mathbb{Q}}(f(x))$ admite um subgrupo cíclico de ordem 5 (ou elemento de ordem 5).

7. O grupo de Galois, considerado como um grupo de permutações das raízes de $f(x)$, é um subgrupo de S_5. Os único elementos de S_5 de ordem 5 são os 5-ciclos. Então, $Gal_{\mathbb{Q}}SF_{\mathbb{Q}}(f(x))$ é um subgrupo de S_5 contendo um 5-ciclo.

8. O isomorfismo conjugação em $\mathbb{C}$ induz um automorfismo em $SF_{\mathbb{Q}}(f(x))$ intercalando as duas únicas raízes complexas de $f(x)$ e fixando as outras três raízes reais. Este automorfismo como um elemento de $Gal_{\mathbb{Q}}SF_{\mathbb{Q}}(f(x))$ é uma transposição.

9. Deste modo, $Gal_{\mathbb{Q}}SF_{\mathbb{Q}}(f(x))$ é um subgrupo de S_5 contendo uma transposição e um 5-ciclo. Logo, $Gal_{\mathbb{Q}}SF_{\mathbb{Q}}(f(x)) = S_5$ (Atividade).

Prezado aluno, chegamos ao final do curso. É compreensível o cansaço ocasionado pelo enorme esforço dispendido para chegarmos até aqui. Mas, o deleite da aprendizagem na matemática é proporcional ao quanto não trivial for o que estivermos aprendendo. Fatos não triviais não são por acaso e sua compreensão requer dedicação e perseverança. Eis o que torna a matemática um conhecimento de poucos.

15.6 Conclusão

O critério de solubilidade de Galois resolveu um problema milenar. Somente isto já seria suficiente para tornar seu critério uma das soluções mais importantes da história da matemática. Mas, a maior importância deste critério consiste no uso de uma estrutura abstrata (grupos) para resolver um problema sem nenhuma conexão aparente. Isto não somente evidenciou o potencial da álgebra para solução de problemas mas iniciou uma nova era na matemática chamada moderna.

RESUMO

Grupos Solúveis Um grupo G é dito solúvel se existe uma cadeia de subgrupos

$$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \cdots \supseteq G_{n-1} \supseteq G_n = \{e\}$$

na qual cada G_i é um subgrupo normal do grupo precedente G_{i-1} e o grupo quociente G_{i-1}/G_i é abeliano.

Não existe uma fórmula envolvendo somente as operações definidas no corpo e extração de raízes para a solução de uma equação algébrica geral de grau 5

Extensões Radicais

Um corpo K é dito ser uma extensão radical de um corpo F se existe uma cadeia de corpos

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_r = K$$

na qual para cada $i = 1, 2, \ldots, r$, tem-se $F_i = F_{i-1}(\alpha_i)$ com $\alpha_i^m \in F_{i-1}$ para algum inteiro m.

Critério de Solubilidade de Galois

Seja F um corpo de característica zero e $f(x) \in F[x]$. Então, $f(x)$ é solúvel por radicais $\Longleftrightarrow$ o grupo de Galois de $f(x)$ é solúvel.

A quíntica $2x^5 - 10x + 5 \in \mathbb{Q}[x]$ não é solúvel por radicais.

ATIVIDADES

ATIV. 15.1. Faça uma pesquisa sobre as fórmulas envolvendo radicais para uma equação cúbica. Use seus resultados para determinar as raízes da equação $x^3 + 3x + 2 = 0$.

ATIV. 15.2. Mostre que toda extensão radical é finita.

ATIV. 15.3. Mostre que toda extensão quadrática é radical.

ATIV. 15.4. Mostre que o corpo $\mathbb{Q}(\sqrt{5}, \sqrt[7]{1-\sqrt{2}}, \sqrt[7]{1+\sqrt{2}})$ é uma extensão radical de $\mathbb{Q}$.

ATIV. 15.5. Seja H um subgrupo de S_5. Se H contém um 5-ciclo e uma transposição então $H = S_5$.

ATIV. 15.6. Use os passos para mostrar a não solubilidade por radicais da quíntica exibida no texto e construa uma outra quíntica não solúvel por radicais.

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.