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

Anéis quocientes $k[x]/I$

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.