EXTENSÕES DE CORPOS

Maria Lúcia Torres Villela
Instituto de Matemática
Universidade Federal Fluminense
setembro de 2008
Revisto em Março de 2009

Sumário

Introdução 3

Parte 1 - Extensões de Corpos 5

Seção 1 - Extensões algébricas ou transcendentes 7

Seção 2 - Construção de uma raiz 25

Seção 3 - Corpos de decomposição 39

Seção 4 - Extensões normais e separáveis 45

Parte 2 - Teoria de Galois 53

Seção 1 - A idéia da Teoria de Galois 55

Seção 2 - A conexão de Galois 63

Seção 3 - A equação geral do grau $\mathfrak{n}$ 79

Seção 4 - $\mathbb{C}$ é um corpo algebricamente fechado 93

Introdução

O objetivo deste texto é ser um apoio aos estudantes da disciplina Álgebra III, do Curso de Graduação em Matemática da Universidade Federal Fluminense, para o conteúdo correspondente ao estudo de extensões de corpos e à Teoria de Galois.

Estudaremos corpos sob o ponto de vista da resolução de equações.

Começaremos com os conceitos de característica de domínios e corpos e de corpo primo.

Introduziremos a adjunção de um conjunto a um corpo, utilizada para construir domínios ou extensões de corpos.

Veremos diversos tipos de extensões: algébricas, transcendentes, finitas e finitamente geradas.

Estudaremos corpos de decomposição ou corpos de raízes de polinômios com coeficientes em corpos, extensões normais, extensões separáveis e inseparáveis, automorfismos de corpos, corpos fixos e extensão de isomorfismo de corpos.

Finalizaremos com o estudo de extensões de corpos galoisianas e a Teoria de Galois, que estabelece uma bijeção entre os corpos intermediários da extensão galoisiana e os subgrupos do grupo dos automorfismos da extensão. Além disso, mostraremos que essa bijeção reverte a inclusão.

Veremos também a relação entre equações solúveis por radicais e grupos solúveis.

Finalizamos com uma aplicação da teoria estudada, uma bela demonstração de que o corpo dos números complexos é algebricamente fechado.

Recomendamos os seguintes textos:

- *Elements of Abstratc Algebra*, R. A. Dean, Wiley Internacional, 1974.

- *Topics in Algebra*, I. N. Herstein, John Wiley & Sons, 2^{nd} edition, 1975.

- *Galois Theory*, Ian Stewart, Chapman & Hall/CRC, 2^{nd} edition, 1989.

- *Algebra*, Thomas W. Hungerford, Springer-Verlag, 1974.

-*Galois Theory*, Joseph Rotman, Springer-Verlag, 1990.

Textos com um tratamento mais avançado:

- *Field and Galois Theory*, Patrick Morandi, Springer-Verlag, 1996.

- *Algebra*, Serge Lang, Addison-Wesley Publishing Company, 3^{nd} edition, 1993.

Parte 1

Extensões de Corpos

Consideraremos que o estudante tenha familiaridade com o domínio principal dos polinômios com coeficientes em corpos tais como: $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ e $\mathbb{Z}_p[x]$.

Relembramos o conceito de característica de domínios e corpos e definimos o corpo primo de um corpo.

Na primeira parte estudaremos extensões de corpos: algébricas e transcendentes, com ênfase nas algébricas.

Definiremos a adjunção de um conjunto a um corpo e usaremos esse conceito para construir domínios e extensões de corpos.

O conceito de grau da extensão de corpos $L|K$ permite relacionar a estrutura de corpo e de K-espaço vetorial de L.

Usaremos o anel quociente para construir uma raiz de um polinômio irredutível com coeficientes em um corpo K.

Para cada polinômio irredutível $p(x) \in K[x]$, construiremos uma extensão L de K, tal que L contenha uma raiz de $f(x)$.

Construiremos corpos de decomposição ou corpos de raízes de polinômios com coeficientes em corpos e estudaremos extensões normais, extensões separáveis e inseparáveis.

Extensões algébricas ou transcendentes

Lembramos que um domínio D é um anel comutativo com unidade tendo uma das seguintes condições equivalentes:

(i) Se $a, b \in D$ e $a \cdot b = 0_D$, então $a = 0_D$ ou $b = 0_D$.

(ii) Se $a, b, c \in D$, $c \neq 0_D$ e $a \cdot c = b \cdot c$, então $a = b$.

A unidade do anel D é o elemento neutro multiplicativo, denotado por 1_D.

Seja $\rho : \mathbb{Z} \longrightarrow D$ o único homomorfismo de anéis tal que $\rho(1) = 1_D$. Chamamos ρ de *homomorfismo característico* de D. Então,

$$\rho(n) = n1_D = \begin{cases} \underbrace{1_D + \cdots + 1_D}_{n \text{ parcelas}}, & n > 0 \\ 0, & n = 0 \\ \underbrace{(-1_D) + \cdots + (-1_D)}_{-n \text{ parcelas}}, & n < 0. \end{cases}$$

O núcleo de ρ é um ideal de $\mathbb{Z}$. Como $\mathbb{Z}$ é um domínio principal, existe $n_0 \in \mathbb{Z}$, com $n_0 \geq 0$, tal que Núcleo$(\rho) = (n_0) = n_0\mathbb{Z}$. Mais ainda, como D é um domínio, então o núcleo de ρ é um ideal primo de $\mathbb{Z}$. Assim, $n_0 = 0$ ou $n_0 = p$, com p primo.

Seja A um anel comutativo com unidade 1_A.
$I \subset A$ é um ideal de A se, e somente se,
$0_A \in I$,
$a, b \in I \Longrightarrow a + b \in I$,
$a \in A, b \in I \Longrightarrow a \cdot b \in I$.

I é um ideal primo se, e somente se, $I \subsetneq A$ é um ideal tal que $a, b \in A$ e $a \cdot b \in I$, então $a \in I$ ou $b \in I$.

No primeiro caso, ρ é injetor e D contém um subanel isomorfo a $\mathbb{Z}$, a saber, $D \supset \rho(\mathbb{Z}) = \{n1_D \,;\, n \in \mathbb{Z}\}$. Nesse caso, $n1_D \neq 0_D$, para todo $n \neq 0$.

No segundo caso, $p1_D = \underbrace{1_D + \cdots + 1_D}_{p \text{ parcelas}} = 0_D$ e, para cada $n \in \mathbb{Z}$, pela divisão euclidiana de n por p, existem q e r em $\mathbb{Z}$, com $0 \leq r \leq p - 1$ tais que $n = qp + r$ e $n1_D = (qp + r)1_D = q(p1_D) + r1_D = r1_D$. Assim,

$$\rho(\mathbb{Z}) = \{n1_D \,;\, n \in \mathbb{Z}\} = \{r1_D \,;\, 0 \leq r \leq p - 1\} = \{0_D, 1_D, \ldots, (p-1)1_D\},$$

é um subanel de D isomorfo a $\mathbb{Z}_p$.

Definição 1 (Característica de um domínio)
Seja D um domínio. Chamamos o gerador não-negativo do núcleo do homomorfismo característico $\rho : \mathbb{Z} \longrightarrow D$ de característica de D.
Dizemos que D é de característica 0, quando Núcleo$(\rho) = \{0\}$. Nesse caso, D contém um subanel isomorfo a $\mathbb{Z}$. Escrevemos car$(D) = 0$.
Dizemos que D é de característica p, onde p é um natural primo, quando Núcleo$(\rho) = p\mathbb{Z}$. Nesse caso, D contém um subanel isomorfo a $\mathbb{Z}_p$. Escrevemos car$(D) = p$.

Exemplo 1
$\mathbb{Z}$, $\mathbb{Z}[i] = \{a + bi \;\; a, b \in \mathbb{Z}\}$, $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \;\; a, b \in \mathbb{Z}\}$ são exemplos de domínios de característica 0.

Tomando p um natural primo, $\mathbb{Z}_p$ e $\mathbb{Z}_p[x]$, o domínio dos polinômios com coeficientes em $\mathbb{Z}_p$ são exemplos de domínios de característica prima p.

Exemplo 2

Todo corpo é um domínio. Portanto, a característica de um corpo é zero ou p, onde p é um natural primo.

$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \ ; \ a, b \in \mathbb{Q}\}$ e $\mathbb{Q}(i) = \{a + bi \ ; \ a, b \in \mathbb{Q}\}$ são exemplos de corpos de característica 0.

No momento, os únicos corpos de característica prima são $\mathbb{Z}_p$ e $\mathbb{Z}_p(x)$, o *corpo das funções racionais* com coeficientes em $\mathbb{Z}_p$, definido por

$$\mathbb{Z}_p(x) = \left\{ \tfrac{f(x)}{g(x)} \ ; \ f(x), g(x) \in \mathbb{Z}_p[x] \text{ e } g(x) \neq 0 \right\}.$$

Adiante veremos outros exemplos de corpos de característica prima.

Para todo domínio D, podemos construir o seu corpo de frações $Q(D)$, a saber, o conjunto

$$Q(D) = \left\{ \tfrac{a}{b} \ ; \ a, b \in D, b \neq 0 \right\},$$

onde $\frac{a}{b} = \frac{c}{d}$ se, e somente se, $a \cdot d = b \cdot c$.

$Q(D)$ é um corpo com as operações:

$$\tfrac{a}{b} + \tfrac{c}{d} = \tfrac{a \cdot d + b \cdot c}{b \cdot d} \text{ e } \tfrac{a}{b} \cdot \tfrac{c}{d} = \tfrac{a \cdot c}{b \cdot d}.$$

Estas operações independem dos representantes das frações. $Q(D)$ é um corpo que tem as seguintes propriedades:

(i) D é um subanel de $Q(D)$.

(ii) Se K é um corpo e D é um subanel de K, então $Q(D)$ é subcorpo de K.

De fato, seja $a \in D$. Então, para todo $b \in D$, tal que $b \neq 0_D$, temos que $\frac{a \cdot b}{b} = \frac{a}{1_D}$. Identificando $a = \frac{a}{1_D}$, vemos que a adição e a multiplicação de D correspondem à adição e à multiplicação de $Q(D)$ restritas às frações com denominador 1_D, mostrando que D é um subanel de $Q(D)$.

Seja agora K um corpo que contém D como um subanel. Sejam $a, b \in D$ com $b \neq 0_D$. Então, $a \cdot b^{-1} \in K$. Além disso, se $c, d \in D$ com $d \neq 0_D$ e $a \cdot b^{-1} = c \cdot d^{-1}$ em K, então multiplicando por $b \cdot d \in D \subset K$, temos que $a \cdot d = (a \cdot b^{-1}) \cdot (b \cdot d) = (c \cdot d^{-1}) \cdot (b \cdot d) = b \cdot c$. Assim, $\frac{a}{b} = \frac{c}{d}$ em $Q(D)$.

Identificamos $a \cdot b^{-1} = \frac{a}{b}$. Assim, $Q(D) \subset K$ é um anel com as operações de K, isto é, $Q(D)$ é um subanel de K.

Observamos também que $\mathrm{car}(Q(D)) = \mathrm{car}(D)$.

Exemplo 3

Se $D = \mathbb{Z}$, então $Q(\mathbb{Z}) = \mathbb{Q}$.

Se $D = \mathbb{Q}$, então $Q(\mathbb{Q}) = \mathbb{Q}$.

Em geral, se K é um corpo, então $Q(K) = K$.

Exemplo 4

Seja $\mathbb{Z}[i] = \{a + bi \ ; \ a, b \in \mathbb{Z}\}$ o domínio dos inteiros de Gauss. $\mathbb{Z}[i]$ é um anel com as operações de adição e multiplicação de números complexos, isto é, $\mathbb{Z}[i]$ é um subanel do corpo dos números complexos.

O corpo de frações de $\mathbb{Z}[i]$ é $\mathbb{Q}(i) = \{a + bi \ ; \ a, b \in \mathbb{Q}\}$.

Exemplo 5

Seja $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \ ; \ a, b \in \mathbb{Z}\}$. $\mathbb{Z}[\sqrt{2}]$ é um anel com as operações de adição e multiplicação de números reais, isto é, $\mathbb{Z}[\sqrt{2}]$ é um subanel do corpo dos números reais.

O corpo de frações de $\mathbb{Z}[\sqrt{2}]$ é $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ ; \ a, b \in \mathbb{Q}\}$.

Exemplo 6

Seja $\mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \ ; \ a, b \in \mathbb{Z}\}$. $\mathbb{Z}[\sqrt{3}]$ é um anel com as operações de adição e multiplicação de números reais, isto é, $\mathbb{Z}[\sqrt{3}]$ é um subanel do corpo dos números reais.

O corpo de frações de $\mathbb{Z}[\sqrt{3}]$ é $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \ ; \ a, b \in \mathbb{Q}\}$.

Exemplo 7

Seja K um corpo e seja $K[x]$ o domínio dos polinômios com coeficientes em K.

$K(x)$, o *corpo das funções racionais* com coeficientes em K, é definido por

$$K(x) = \left\{ \frac{f(x)}{g(x)} \ ; \ f(x), g(x) \in K[x] \text{ e } g(x) \neq 0 \right\}$$

e $K(x)$ é o corpo das frações de $K[x]$.

Agora estamos prontos para começar o nosso estudo de corpos.

Definição 2 (Extensão de corpos)

Sejam K e L corpos. Dizemos que L é uma *extensão de* K se, e somente se, K é um subcorpo de L. Escrevemos L|K. Nesse caso, $K \subset L$, K é um corpo com as operações de L e $1_K = 1_L$.

L|K lê-se extensão L sobre K. Observamos que $\mathrm{car}(L) = \mathrm{car}(K)$.

Exemplo 8
$\mathbb{C}|\mathbb{R}$, $\mathbb{R}|\mathbb{Q}$, $\mathbb{C}|\mathbb{Q}$, $\mathbb{Q}(i)|\mathbb{Q}$, $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$, $\mathbb{Q}(\sqrt{3})|\mathbb{Q}$ são exemplos de extensões de corpos. Assim como, $K(x)|K$, onde K é um corpo e x é uma indeterminada sobre K.

Seja K um corpo. Sabemos que $car(K) = 0$ ou $car(K) = p$, onde p é um natural primo.

No primeiro caso, K contém um domínio isomorfo a $\mathbb{Z}$, a saber, o domínio $D = \{n1_K \ ; \ n \in \mathbb{Z}\}$. Como K é um corpo, o corpo de frações de D é um subcorpo de K. Assim,

$$K \supset Q(D) = \left\{ \frac{n1_K}{m1_K} \ ; \ n, m \in \mathbb{Z} \text{ e } m \neq 0 \right\} \simeq \mathbb{Q}.$$

Observamos que o menor subcorpo de K é $Q(D) \simeq \mathbb{Q}$.

No segundo caso, K contém como subcorpo $\{0_K, 1_K, \ldots, (p-1)1_K\} \simeq \mathbb{Z}_p$.

Agora, $\{0_K, 1_K, \ldots, (p-1)1_K\}$ é o menor subcorpo de K.

Definição 3 (Corpo primo)
Seja K um corpo. O *corpo primo* de K é o menor subcorpo de K.

O corpo primo é obtido operando, sucessivamente, a unidade 1_K.

Quando $car(K) = 0$, $m1_K = 0_K$ se, e somente se, $m = 0$ e o corpo primo de K é $\left\{ \frac{n1_K}{m1_K} \ ; \ n, m \in \mathbb{Z} \text{ e } m \neq 0 \right\}$.

Quando $car(K) = p$, p primo, então $p1_K = 0_K$ e o corpo primo de K é $\{0_K, 1_K, \ldots, (p-1)1_K\}$.

Em característica prima p temos: $m1_K = 0 \iff p|m$.

Seja $L|K$ uma extensão de corpos. As operações de adição e multiplicação de L induzem em L uma estrutura de K-espaço vetorial.

$$\cdot : \begin{array}{ccc} K \times L & \longrightarrow & L \\ (a, \alpha) & \longmapsto & a \cdot \alpha \end{array} \quad \text{e} \quad + : \begin{array}{ccc} L \times L & \longrightarrow & L \\ (\alpha, \beta) & \longmapsto & \alpha + \beta \end{array}$$

Definição 4 (Grau de $L|K$)
A dimensão de L como K-espaço vetorial é chamada de *grau* de $L|K$. Denotamos $[L : K] = \dim_K(L)$.

Definição 5 (Extensões finitas)
Seja $L|K$ uma extensão de corpos. Dizemos que $L|K$ é *extensão finita* quando $[L : K] < \infty$. Caso contrário, dizemos que $L|K$ é *extensão infinita*.

Exemplo 9
Seja K um corpo.

Então, $K|K$ é uma extensão finita de grau 1, isto é, $[K : K] = 1$, pois K é um K-espaço vetorial de dimensão 1. Tomando $c \in K$, $c \neq 0$ temos que $\{c\}$ é uma base de K. Em particular, $\{1_K\}$ é uma base de K como K-espaço vetorial.

Exemplo 10

$\mathbb{C}|\mathbb{R}$ é uma extensão finita com $[\mathbb{C} : \mathbb{R}] = 2$.

De fato, $\{1, i\}$ gera $\mathbb{C}$ como $\mathbb{R}$-espaço vetorial, pois cada $\alpha \in \mathbb{C}$ é da forma $\alpha = a + bi$, onde $a, b \in \mathbb{R}$. Além disso, $a + bi = 0$ com $a, b \in \mathbb{R}$ se, e somente se, $a = b = 0$, mostrando que $\{1, i\}$ é linearmente independente sobre $\mathbb{R}$. Logo, $[\mathbb{C} : \mathbb{R}] = 2$.

Exemplo 11

Seja K um corpo e x uma indeterminada sobre K.

A extensão $K(x)|K$ é infinita, pois $\{1, x, x^2, \ldots, x^n, \ldots\}$ é linearmente independente sobre K. Nesse caso, $[K(x) : K] = \infty$.

Exemplo 12

$\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ é uma extensão finita de grau 2.

De fato, da definição de $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \ ; \ a, b \in \mathbb{Q}\}$ segue que $\{1, \sqrt{2}\}$ gera $\mathbb{Q}(\sqrt{2})$ como $\mathbb{Q}$-espaço vetorial.

Suponhamos que $a + b\sqrt{2} = 0$ com $a, b \in \mathbb{Q}$.

Se $b \neq 0$, então $\sqrt{2} = -a \cdot b^{-1} \in \mathbb{Q}$, que é uma contradição. Logo $b = 0$ e assim, $a = 0$. Portanto, $\{1, \sqrt{2}\}$ é linearmente independente sobre $\mathbb{Q}$. Então, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.

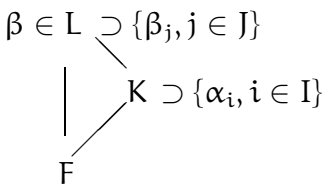
Proposição 1 (Multiplicatividade do grau)

Sejam $L|K$ e $K|F$ extensões finitas de corpos. Então, $L|F$ é extensão finita e $[L : F] = [L : K][K : F]$.

Demonstração: Seja $\{\alpha_i \ ; \ i = 1, \ldots, m\} \subset K$ uma base de $K|F$ e seja $\{\beta_j \ ; \ j = 1, \ldots, n\} \subset L$ uma base de $L|K$.

Vamos mostrar que $\{\alpha_i\beta_j \ ; \ i = 1, \ldots, m \text{ e } j = 1, \ldots, n\} \subset L$ é uma base de $L|F$. Acompanhe o raciocínio a seguir, tendo em vista o diagrama abaixo, onde $I = \{1, \ldots, m\}$ e $J = \{1, \ldots, n\}$.

Seja $\beta \in L$. Existem $b_j \in K$ tais que $\beta = \sum_{j=1}^{n} b_j\beta_j$, pois $\{\beta_j \ ; \ j = 1, \ldots, n\}$ gera $L|K$.



Para cada $b_j \in K$, existem $a_{ij} \in F$, tais que

A multiplicatividade dos graus vale quando I e J são conjuntos quaisquer. Temos $[L : K] = \sharp J$, $[K : F] = \sharp I$ e $[L : F] = \sharp(I \times J) = (\sharp I)(\sharp J)$, onde $\sharp$ é a cardinalidade. Nesse caso, tomando $\{\alpha_i, i \in I\}$ uma base de $K|F$ e $\{\beta_j, j \in J\}$ uma base de $L|K$ temos que $\{\alpha_i\,\beta_j, i \in I, j \in J\}$ é uma base de $L|F$.

$b_j = \sum_{i=1}^{m} a_{ij}\alpha_i$, pois $\{\alpha_i\ ;\ i = 1, \ldots, m\}$ gera $K|F$. Assim,

$$\begin{aligned}\beta = \sum_{j=1}^{n} b_j\beta_j &= \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_{ij}\alpha_i\right)\beta_j \\ &= \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_{ij}\alpha_i\beta_j\right) \\ &= \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}(\alpha_i\beta_j),\end{aligned}$$

mostrando que $\{\alpha_i\beta_j\ ;\ i = 1, \ldots, m \text{ e } j = 1, \ldots, n\}$ gera $L|F$.

Suponhamos agora que $0 = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}\alpha_i\beta_j$, com $a_{ij} \in F$.

Então, $0 = \sum_{j=1}^{n}\sum_{i=1}^{m} a_{ij}\alpha_i\beta_j = \sum_{j=1}^{n}\left(\sum_{i=1}^{m} a_{ij}\alpha_i\right)\beta_j$, com $\sum_{i=1}^{m} a_{ij}\alpha_i \in K$, para cada j.

Como $\{\beta_j\ ;\ j = 1, \ldots, n\}$ é linearmente independente sobre K, temos que $\sum_{i=1}^{m} a_{ij}\alpha_i = 0$, para cada $j = 1, \ldots, n$.

Como $\{\alpha_i\ ;\ i = 1, \ldots, m\}$ é linearmente independente sobre F, obtemos que $a_{ij} = 0$, para cada $i = 1, \ldots, m$. ■

Antes de vermos mais exemplos de extensões de corpos, precisamos de um conceito muito importante para construir corpos e também domínios: a adjunção.

Definição 6 (Adjunção)
Seja $L|K$ uma extensão de corpos e $S \subset L$. Definimos

$$K[S] = \bigcap_{\substack{A \text{ anel} \\ K \cup S \subset A \\ A \subset L,}} A \qquad \text{e} \qquad K(S) = \bigcap_{\substack{F \text{ corpo} \\ K \cup S \subset F \\ F \subset L}} F$$

$K[S]$ é o menor anel contido em L contendo $K \cup S$, forçosamente, é um domínio, enquanto $K(S)$ é o menor corpo contido em L contendo $K \cup S$.

Dizemos que $K[S]$ é o subanel de L obtido pela *adjunção de* S a K, enquanto $K(S)$ é o subcorpo de L obtido pela *adjunção de* S a K.

Exemplo 13

Seja $L|K$ uma extensão de corpos e $\alpha \in L$. Seja $S = \{\alpha\}$.

Seja $K[x]$ o domínio dos polinômios com coeficientes em K.

Primeiramente, observamos que para qualquer $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K[x]$ temos $f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + a_1\alpha + a_0 \in L$. É fácil verificar que $\{f(\alpha)\ ;\ f(x) \in K[x]\}$ é um subanel de L que contém $K \cup \{\alpha\}$. Além disso, qualquer subanel A de L que contenha $K \cup \{\alpha\}$ é tal que:

(i) Para todo $n \geq 1$, $\alpha^n \in A$;

(ii) $a\alpha^n \in A$, para todo $n \geq 1$ e para todo $a \in K$.

Assim, $A \supset K + K\alpha + \cdots + K\alpha^n$, para todo $n \geq 1$.

Portanto, $A \supset \{f(\alpha)\ ;\ f(x) \in K[x]\}$.

Concluímos, desse modo, que o menor subanel de L que contém $K \cup \{\alpha\}$ é $\{f(\alpha)\ ;\ f(x) \in K[x]\}$, isto é,

$$K[\alpha] = \{f(\alpha)\ ;\ f(x) \in K[x]\}.$$

$K(\alpha)$, o menor subcorpo de L que contém $K \cup \{\alpha\}$, tem que conter o domínio $K[\alpha]$. Portanto, $K(\alpha)$ contém o corpo de frações de $K[\alpha]$, isto é,

$$K(\alpha) \supset Q(K[\alpha]) = \underbrace{\left\{\frac{f(\alpha)}{g(\alpha)}\ ;\ f(x), g(x) \in K[x] \text{ e } g(\alpha) \neq 0\right\}}_{\text{é um corpo que contém } K\cup\{\alpha\}}.$$

$\alpha \in L$

$K(\alpha)$

$K[\alpha]$

K

Daí segue que

$$K(\alpha) = \left\{\tfrac{f(\alpha)}{g(\alpha)}\ ;\ f(x), g(x) \in K[x] \text{ e } g(\alpha) \neq 0\right\}.$$

Mais ainda, $K(\alpha)$ é o corpo de frações de $K[\alpha]$.

Exemplo 14

Consideremos a extensão $\mathbb{C}|\mathbb{Q}$ e $i \in \mathbb{C}$.

Quem é o domínio $\mathbb{Q}[i]$?

$\mathbb{Q}[i]$ é um subanel de $\mathbb{C}$ que contém $\mathbb{Q} \cup \{i\}$. Então, $\mathbb{Q}[i] \supset \mathbb{Q} + \mathbb{Q}i$. Como $\mathbb{Q} + \mathbb{Q}i$ é um anel que contém $\mathbb{Q} \cup \{i\}$, temos que $\mathbb{Q}[i] \subset \mathbb{Q} + \mathbb{Q}i$. Logo, $\mathbb{Q}[i] = \mathbb{Q} + \mathbb{Q}i = \{a + bi\ ;\ a, b \in \mathbb{Q}\}$. Do fato de $\mathbb{Q} + \mathbb{Q}i$ ser um corpo que contém $\mathbb{Q} \cup \{i\}$, concluímos que $\mathbb{Q}[i] = \mathbb{Q}(i)$.

Verifique que $\mathbb{Q} + \mathbb{Q}i$ é um subcorpo de $\mathbb{C}$.

Exemplo 15

Consideremos a extensão $\mathbb{R}|\mathbb{Q}$ e $\sqrt{2} \in \mathbb{R}$.

Quem é o domínio $\mathbb{Q}[\sqrt{2}]$?

EXTENSÃO DE CORPOS

$\mathbb{Q}[\sqrt{2}]$ é um subanel de $\mathbb{R}$ que contém $\mathbb{Q} \cup \{\sqrt{2}\}$. Então, $\mathbb{Q}[\sqrt{2}] \supset \mathbb{Q} + \mathbb{Q}\sqrt{2}$. Como $\mathbb{Q}+\mathbb{Q}\sqrt{2}$ é um anel que contém $\mathbb{Q}\cup\{\sqrt{2}\}$, temos que o menor com esta propriedade está contido em $\mathbb{Q}+\mathbb{Q}\sqrt{2}$, isto é, $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}+\mathbb{Q}\sqrt{2}$. Portanto, $\mathbb{Q}[\sqrt{2}] = \mathbb{Q} + \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2}\ ;\ a, b \in \mathbb{Q}\}$. Pelo fato de $\mathbb{Q} + \mathbb{Q}\sqrt{2}$ ser um corpo que contém $\mathbb{Q} \cup \{\sqrt{2}\}$, concluímos que $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$.

Verifique que $\mathbb{Q} + \mathbb{Q}\sqrt{2}$ é um subcorpo de $\mathbb{R}$.

Como no exemplo anterior, o menor subanel também é o menor subcorpo.

Vamos olhar com mais atenção.

Seja $L|K$ uma extensão de corpos e fixemos $\alpha \in L$.

Consideremos a função avaliação em α, $\varphi_\alpha : K[x] \longrightarrow L$ definida por $\varphi_\alpha(f(x)) = f(\alpha)$.

Então,

$P \subsetneq A$ é um ideal primo de um anel A, comutativo com unidade se, e somente se, $a.b \in P$ implica que $a \in P$ ou $b \in P$.

(i) φ_α é homomorfismo de anéis,

(ii) Imagem$(\varphi_\alpha) = K[\alpha]$ e

(iii) Núcleo$(\varphi_\alpha) = \{g(x) \in K[x]\ ;\ g(\alpha) = 0\}$ é um ideal primo de $K[x]$.

Como $K[x]$ é um domínio de ideais principais, só há duas possibilidades para Núcleo(φ_α):

Caso 1: Núcleo$(\varphi_\alpha) = \{0\}$

Nesse caso, o único polinômio com coeficientes em K que se anula em α é o polinômio identicamente nulo, φ_α é homomorfismo de anéis injetor e Imagem$(\varphi_\alpha) = K[\alpha]$ é isomorfo ao domínio dos polinômios com coeficientes em K, isto é, $K[x] \simeq K[\alpha]$. Não há relação algébrica entre α e os elementos de K, α é uma indeterminada sobre K.

Observamos que $K[\alpha] \subsetneq K(\alpha)$, $\{1, \alpha, \alpha^2, \ldots, \alpha^n, \ldots\}$ é linearmente independente sobre K e $[K(\alpha) : K] = \infty$.

Dizemos que α é *transcendente* sobre K.

Num domínio principal D um ideal $I \neq \{0\}$ é primo se, e somente se, $I = (p)$, onde p é elemento irredutível de D.

Caso 2: Núcleo$(\varphi_\alpha) = (p(x))$, onde $p(x) \in K[x]$ é polinômio mônico irredutível.

Sabemos que $p(x)$ é o polinômio mônico de menor grau que está no ideal, isto é, $p(\alpha) = 0$.

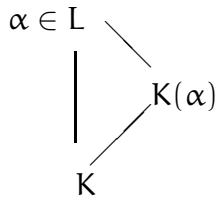
Nesse caso, dizemos que α é *algébrico* sobre K.

Mostraremos, a seguir, que $K[\alpha] = K(\alpha)$.

Seja $L|K$ uma extensão de corpos e seja $\alpha \in L$.

Observamos que $K(\alpha)$ é um subcorpo de L, é o menor subcorpo de L que contém $K \cup \{\alpha\}$. Assim,

$K \subset K(\alpha) \subset L$. O diagrama abaixo ilustra as extensões de corpos



Definição 7 (Elemento algébrico ou transcendente sobre K)
Seja L|K uma extensão de corpos e seja $\alpha \in L$. Dizemos que α é *algébrico* sobre K se, e somente se, existe $f(x) \in K[x]\backslash\{0\}$, tal que $f(\alpha) = 0$. Caso contrário, dizemos que α é *transcendente* sobre K.

Definição 8 (Polinômio mínimo de α sobre K)
Seja L|K uma extensão de corpos e seja $\alpha \in L$ algébrico sobre K. O polinômio $p(x) \in K[x]$ mônico irredutível, tal que $p(\alpha) = 0$, é chamado de *polinômio mínimo* de α sobre K.

Exemplo 16
Seja K um corpo.

Todo $\alpha \in K$ é algébrico sobre K com polinômio mínimo $x - \alpha \in K[x]$.

Exemplo 17

Verifique todas as afirmações desse Exemplo.

$i \in \mathbb{C}$ é algébrico sobre $\mathbb{R}$ e o seu polinômio mínimo sobre $\mathbb{R}$ é $x^2 + 1 \in \mathbb{R}[x]$.
$i \in \mathbb{C}$ é algébrico sobre $\mathbb{Q}$ e o seu polinômio mínimo sobre $\mathbb{Q}$ é $x^2 + 1 \in \mathbb{Q}[x]$.
$\sqrt{2} \in \mathbb{R}$ é algébrico sobre $\mathbb{Q}$ e o seu polinômio mínimo sobre $\mathbb{Q}$ é $x^2 - 2 \in \mathbb{Q}[x]$.
$\sqrt{2} \in \mathbb{R}$ é algébrico sobre $\mathbb{R}$ e o seu polinômio mínimo sobre $\mathbb{R}$ é $x - \sqrt{2} \in \mathbb{R}[x]$.
$\sqrt[3]{2} \in \mathbb{R}$ é algébrico sobre $\mathbb{Q}$ e o seu polinômio mínimo sobre $\mathbb{Q}$ é $x^3 - 2 \in \mathbb{Q}[x]$.

Exemplo 18

Uma demonstração pode ser encontrada em *Field and Galois Theory*, Patrick Morandi, página 133, como uma aplicação da Teoria de Galois.

π e e são exemplos de números reais transcendentes sobre $\mathbb{Q}$, pois o único polinômio com coeficientes racionais que se anula em π ou e é o polinômio identicamente nulo.

Teorema 1 (Caracterização de elementos algébricos)
Seja L|K uma extensão de corpos e seja $\alpha \in L$. Temos que α é algébrico sobre K se, e somente se, $[K(\alpha) : K] < \infty$. Nesse caso, $K(\alpha) = K[\alpha]$, $[K(\alpha) : K] = n$, onde $n = \text{grau}(p(x))$ e $p(x) \in K[x]$ é o polinômio mínimo de α sobre K.

Demonstração: Suponhamos que α seja algébrico sobre K.

Seja $n = \text{grau}(p(x)) \geq 1$, onde $(p(x)) = \text{Núcleo}(\varphi_\alpha)$ com $p(x)$ mônico e irredutível. Afirmamos que $K(\alpha) = K[\alpha]$ e $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de $K(\alpha)|K$.

De fato, seja $\beta \in K(\alpha)$. Então, $\beta = \frac{f(\alpha)}{g(\alpha)}$, onde $f(x), g(x) \in K[x]$ e $g(\alpha) \neq 0$. Então, $\text{mdc}(g(x), p(x)) = 1$. Logo, existem $a(x), b(x) \in K[x]$ tais que

$$1 = a(x)g(x) + b(x)p(x).$$

Avaliando em α, temos que:

$$1 = a(\alpha)g(\alpha) + b(\alpha)p(\alpha) = a(\alpha)g(\alpha).$$

Portanto, $\frac{1}{g(\alpha)} = a(\alpha)$. Logo, $\beta = \frac{f(\alpha)}{g(\alpha)} = f(\alpha)a(\alpha) \in K[\alpha]$, mostrando que $K(\alpha) \subset K[\alpha]$. Como $K[\alpha] \subset K(\alpha)$, concluímos que $K(\alpha) = K[\alpha]$.

Dado $\beta \in K(\alpha) = K[\alpha]$, existe $h(x) \in K[x]$ tal que $\beta = h(\alpha)$. Pela divisão euclidiana de $h(x)$ por $p(x)$, existem $q(x), r(x) \in K[x]$, unicamente determinados, tais que

$$h(x) = p(x)q(x) + r(x), \text{ com } r(x) = 0 \text{ ou } 0 \leq \text{grau}(r(x)) < \text{grau}(p(x)) = n.$$

Em qualquer dos casos, podemos escrever

$$r(x) = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} \text{ com } b_j \in K.$$

Assim,

$$\begin{aligned} \beta = h(\alpha) &= \underbrace{p(\alpha)}_{=0} q(\alpha) + r(\alpha) \\ &= r(\alpha) \\ &= b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}, \end{aligned}$$

mostrando que $\{1, \alpha, \ldots, \alpha^{n-1}\}$ gera $K(\alpha)$ sobre K.

Agora, $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1} = 0$, com nem todos os coeficientes nulos, contradiz a escolha de $p(x)$. Portanto, $b_0 = \cdots = b_{n-1} = 0$, isto é, $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é linearmente independente sobre K e $[K(\alpha) : K] = n$.

Reciprocamente, suponhamos que $[K(\alpha) : K]$ seja finito, digamos que $[K(\alpha) : K] = n \geq 1$. Consideremos $\{1, \alpha, \ldots, \alpha^n\}$. Esse conjunto é linearmente dependente sobre K, pois tem $n + 1$ elementos e $n + 1 > n = \dim_K K(\alpha)$. Logo, existem $c_0, c_1, \ldots, c_n \in K$, nem todos nulos, tais que $c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$.

Tomando $f(x) = c_0 + c_1x + \cdots + c_nx^n \in K[x]$, temos que $f(x) \neq 0$ e $f(\alpha) = c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$, mostrando que α é algébrico sobre K.

Corolário 1
Seja $L|K$ uma extensão de corpos e seja $\alpha \in L$. Temos que α é transcendente sobre K se, e somente se, $K(\alpha)|K$ é extensão infinita. Nesse caso, $K[\alpha] \subsetneq K(\alpha)$.

Definição 9 (Extensão simples)
Seja $L|K$ uma extensão de corpos. Dizemos que $L|K$ é uma extensão simples, se e somente se, existe $\alpha \in L$ tal que $L = K(\alpha)$.

Agora podemos dar mais exemplos de extensões de corpos.

Exemplo 19
Seja $\alpha = \sqrt[3]{2} \in \mathbb{R}$. Consideremos a extensão $\mathbb{Q}(\alpha)|\mathbb{Q}$. Temos que $\alpha^3 = 2$, assim α é raiz do polinômio $x^3 - 2 \in \mathbb{Q}[x]$, mostrando que α é algébrico sobre $\mathbb{Q}$. Pelo critério de Eisenstein, $x^3 - 2$ é irredutível em $\mathbb{Q}[x]$. Portanto, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$ e $\{1, \alpha, \alpha^2\}$ é uma base de $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$.

Consideremos $\beta = \frac{6}{\alpha^2+\alpha} \in \mathbb{Q}(\alpha)$. Existem $a, b, c \in \mathbb{Q}$, unicamente determinados tais que $\beta = a + b\alpha + c\alpha^2$.

Da igualdade $\frac{6}{\alpha^2+\alpha} = a + b\alpha + c\alpha^2$, obtemos:

$6 = (\alpha^2 + \alpha)(a + b\alpha + c\alpha^2) = a\alpha + (a + b)\alpha^2 + (b + c)\alpha^3 + c\alpha^4 \qquad (\star)$

Devemos escrever α^3 e α^4 como combinação linear da base. Temos $\alpha^3 = 2$ e $\alpha^4 = 2\alpha$. Substituindo em $(\star)$, obtemos:

$$\begin{aligned} 0 &= -6 + a\alpha + (a + b)\alpha^2 + (b + c)2 + 2c\alpha \\ &= (-6 + 2b + 2c)1 + (a + 2c)\alpha + (a + b)\alpha^2 \end{aligned}$$

Pelo fato de $\{1, \alpha, \alpha^2\}$ ser linearmente independente sobre $\mathbb{Q}$, obtemos:

$$\begin{aligned} a + b &= 0 \\ a + 2c &= 0 \\ 2b + 2c &= 6 \end{aligned}$$

Logo, $b = -a$, $2c = -a$ e $6 = -2a - a = -3a$. Então, $a = -2$, $b = 2$ e $c = 1$, isto é, $\beta = \frac{6}{\alpha^2+\alpha} = -2 + 2\alpha + \alpha^2$.

Outra solução: Os polinômios $x^3 - 2$ e $\frac{1}{6}x^2 + \frac{1}{6}x$ são primos entre si. Pelo algoritmo euclidiano, obtemos:

$$1 = (x^2 + 2x - 2)\left(\tfrac{1}{6}x^2 + \tfrac{1}{6}x\right) + \left(-\tfrac{1}{6}x - \tfrac{3}{6}\right)(x^3 - 2),$$

seguindo o resultado com a substituição de α na igualdade acima, como na demonstração do Teorema 1.

A partir das extensões simples podemos construir, indutivamente, outras extensões de corpos.

Exemplo 20

Seja $L|K$ uma extensão de corpos e sejam $\alpha, \beta \in L$. Seja $K(\alpha, \beta) = K(S)$, onde $S = \{\alpha, \beta\}$. Vale a seguinte propriedade:

$$K(\alpha, \beta) = K(\alpha)(\beta) = K(\beta)(\alpha).$$

Primeiramente, $\alpha \in K(\alpha, \beta)$ e $K \subset K(\alpha, \beta)$. Assim, o corpo $K(\alpha) \subset K(\alpha, \beta)$. Agora fazemos a adjunção de $\beta \in K(\alpha, \beta)$ ao subcorpo $K(\alpha)$. Dessa forma, obtemos a inclusão $K(\alpha)(\beta) \subset K(\alpha, \beta)$.

Os seguintes diagramas ilustram a inclusão $K(\alpha)(\beta) \subset K(\alpha, \beta)$.

Por outro lado, $K(\alpha)(\beta)$ é o menor subcorpo de L contendo $K(\alpha) \cup \{\beta\}$. Então, $K(\alpha)(\beta) \supset K(\alpha) \cup \{\beta\} \supset K \cup \{\alpha, \beta\}$. Logo, o corpo $K(\alpha)(\beta)$ tem que conter $K(\alpha, \beta)$, o menor subcorpo de L que contém $K \cup \{\alpha, \beta\}$.

Mostramos que $K(\alpha, \beta) = K(\alpha)(\beta)$.

Você deve mostrar a outra igualdade, procedendo de maneira análoga.

Exemplo 21

Vamos mostrar que $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Como $\sqrt{2}$ e $\sqrt{3}$ estão no corpo $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, então $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Logo, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbb{Q} \cup \{\sqrt{2} + \sqrt{3}\}$ e assim também contém $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, o menor subcorpo de $\mathbb{R}$ com essa propriedade.

Para mostrar que $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbb{Q}(\sqrt{2} + \sqrt{3})$, basta mostrar que $\sqrt{2}, \sqrt{3}$ estão em $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, visto que $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Seja $\alpha = \sqrt{2} + \sqrt{3}$. Então, $\sqrt{3} = \alpha - \sqrt{2}$ e $3 = \alpha^2 - 2\sqrt{2}\alpha + 2$, logo $\sqrt{2} = \frac{\alpha^2 - 1}{2\alpha} \in \mathbb{Q}(\alpha)$ e $\sqrt{3} = \alpha - \sqrt{2} = \alpha - \frac{\alpha^2 - 1}{2\alpha} \in \mathbb{Q}(\alpha)$.

Com isto, concluímos que $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Qual é o polinômio mínimo de α sobre $\mathbb{Q}$?

Elevando ao quadrado a igualdade $2\sqrt{2}\alpha = \alpha^2 - 1$, obtemos $\alpha^4 - 10\alpha^2 + 1 = 0$. Com isso, só concluímos que α é algébrico sobre $\mathbb{Q}$ e que $p(x)$, o polinômio mínimo de α sobre $\mathbb{Q}$, divide $x^4 - 10x^2 + 1$. Assim, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 4$.

Vamos determinar $[\mathbb{Q}(\alpha):\mathbb{Q}]$, usando que $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{2},\sqrt{3})$.
Sabemos que $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$. Como $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2})(\sqrt{3})$, basta determinar $[\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})]=n$ e usar a multiplicatividade do grau, isto é,

Volte ao Exemplo 17 e use o Teorema 1.

$$[\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=n[\mathbb{Q}(\sqrt{2}):\mathbb{Q}],$$

ilustrada no diagrama:

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2})(\sqrt{3}) & & \\ \Big| 2n & \searrow n & \\ & 2 \quad \mathbb{Q}(\sqrt{2}) & \\ & \searrow & \\ & \mathbb{Q} & \end{array}$$

$\sqrt{3}$ é raiz de $x^2-3\in\mathbb{Q}(\sqrt{2})[x]$. Logo, $n\leq 2$.
Vamos mostrar que $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$.
Suponhamos, por absurdo, que $\sqrt{3}\in\mathbb{Q}(\sqrt{2})$. Então $\sqrt{3}=a+b\sqrt{2}$, com $a,b\in\mathbb{Q}$, pois $\{1,\sqrt{2}\}$ é uma base de $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$. Se $a=0$, então $\sqrt{\frac{3}{2}}=b\in\mathbb{Q}$, é uma contradição. Se $b=0$, então $\sqrt{3}=a\in\mathbb{Q}$, também é uma contradição. Podemos supor que $a\neq 0$ e $b\neq 0$ e $3=a^2+2ab\sqrt{2}+2b^2$. Assim, $\sqrt{2}=\frac{3-a^2-2b^2}{2ab}\in\mathbb{Q}$, o que também é uma contradição.
Logo, $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$. Então, $n=[\mathbb{Q}(\sqrt{2})(\sqrt{3}):\mathbb{Q}(\sqrt{2})]>1$. Como $n\leq 2$ concluímos que $n=2$. Assim, $[\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}]=2n=4$. Logo, $\text{grau}(p(x))=4$ e $p(x)=x^4-10x^2+1$.

Mostramos assim que x^4-10x^2+1 é irredutível em $\mathbb{Q}[x]$.

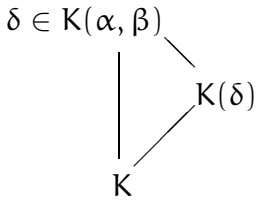
Proposição 2
Seja $L|K$ uma extensão de corpos. Se $\alpha,\beta\in L$ são algébricos sobre K, então $\alpha\pm\beta$, $\alpha\cdot\beta$ e $\frac{\alpha}{\beta}$, com $\beta\neq 0$, são algébricos sobre K. Desse modo,

$$\{\alpha\in L\,;\ \alpha \text{ é algébrico sobre } K\}$$

é um subcorpo de L que contém K.

Demonstração: Seja $\delta\in\{\alpha\pm\beta,\alpha\cdot\beta,\frac{\alpha}{\beta},\ \text{com } \beta\neq 0\}$. Então, $\delta\in K(\alpha,\beta)$ e $K\subset K(\delta)\subset K(\alpha,\beta)$. Vamos mostrar que $[K(\alpha,\beta):K]<\infty$. Pela multiplicatividade dos graus, obtemos que $[K(\delta):K]<\infty$ e, pelo Teorema 1, concluímos que δ é algébrico sobre K.

Veja no diagrama:

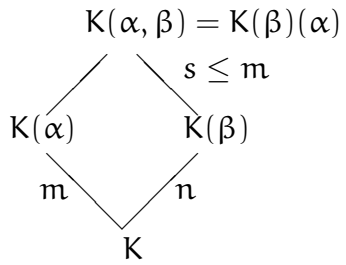


Sejam $f(x), g(x) \in K[x]$ os polinômios mínimos, respectivamente, de α e β sobre K, com $m = \text{grau}(f(x))$ e $n = \text{grau}(g(x))$. Pelo Teorema 1, temos que $[K(\alpha) : K] = m$ e $[K(\beta) : K] = n$. O polinômio $f(x) \in K[x] \subset K(\beta)[x]$ é tal que $f(\alpha) = 0$, mostrando que α é algébrico sobre $K(\beta)$ e $p(x)$, o polinômio mínimo de α sobre $K(\beta)$, divide $f(x)$ em $K(\beta)[x]$.

Assim, $s = \text{grau}(p(x)) \leq \text{grau}(f(x)) = m$.

Logo, $[K(\beta)(\alpha) : K(\beta)] = s \leq m$ é finito e $[K(\alpha, \beta) : K] = sn$ é finito.

O diagrama ilustra o raciocínio feito acima:



A última afirmação da Proposição é clara, lembrando que no Exemplo 16 observamos que todo elemento de K é algébrico sobre K. ■

Definição 10 (Fecho algébrico de $\mathbb{Q}$)
Consideremos a extensão de corpos $\mathbb{C}|\mathbb{Q}$. Chamamos de *fecho algébrico* de $\mathbb{Q}$ ao subcorpo $\overline{\mathbb{Q}}$ de $\mathbb{C}$ definido por

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \,;\, \alpha \text{ é algébrico sobre } \mathbb{Q}\}.$$

Pela Proposição anterior, $\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$.

Exemplo 22
A extensão $\overline{\mathbb{Q}}|\mathbb{Q}$ é infinita.

De fato, para todo $n \in \mathbb{N}$, com $n \geq 1$, temos que o polinômio $x^n - 2$ é irredutível em $\mathbb{Q}[x]$. Assim, $\sqrt[n]{2}$ é algébrico sobre $\mathbb{Q}$ e $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. Como $\mathbb{Q} \subset \mathbb{Q}(\sqrt[n]{2}) \subset \overline{\mathbb{Q}}$, então $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$, para todo $n \geq 1$.

Definição 11 (Extensão algébrica ou transcendente)
A extensão de corpos $L|K$ é dita *algébrica* se, e somente se, todo $\alpha \in L$ é algébrico sobre K. Caso contrário, $L|K$ é dita *transcendente*.

Exemplo 23
A extensão $\mathbb{C}|\mathbb{R}$ é algébrica.

De fato, se $\alpha \in \mathbb{C}$, então existem $a, b \in \mathbb{R}$, tais que $\alpha = a + bi$, logo $\alpha^2 - 2a\alpha + a^2 = (\alpha - a)^2 = (bi)^2 = -b^2$, portanto α é raiz do polinômio $f(x) = x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$. Logo, α é algébrico sobre $\mathbb{R}$.

Exemplo 24
A extensão $\overline{\mathbb{Q}} \mid \mathbb{Q}$, por construção, é algébrica.

Exemplo 25
A extensão $\mathbb{R}|\mathbb{Q}$ é transcendente.

Proposição 3
Se $L|K$ é extensão finita, então $L|K$ é algébrica.

Demonstração: Seja $\alpha \in L$. Então, $K \subset K(\alpha) \subset L$ e $[K(\alpha) : K]$ divide $[L : K]$. Logo, $[K(\alpha) : K]$ é finito e, pelo Teorema 1, α é algébrico sobre K. ■

Corolário 2
Se $L|K$ é uma extensão finita, então existem $\alpha_1, \ldots, \alpha_n \in L$, algébricos sobre K, tais que $L = K(\alpha_1, \ldots, \alpha_n)$.

Demonstração: Sejam $n = [L : K]$ e $\{\alpha_1, \ldots, \alpha_n\} \subset L$ uma base de L sobre K. Então,

$$L = K\alpha_1 + \cdots + K\alpha_n \subset K(\alpha_1, \ldots, \alpha_n) \subset L,$$

logo $L = K(\alpha_1, \ldots, \alpha_n)$. Pela Proposição anterior, α_j é algébrico sobre K, para todo $j = 1, \ldots, n$. ■

Cuidado: Nem toda extensão de corpos algébrica é finita. Por exemplo, $\overline{\mathbb{Q}} \mid \mathbb{Q}$ é algébrica e não é finita.

Exercícios

1. Seja D um domínio de característica prima p. Mostre que:
   (a) $(a + b)^p = a^p + b^p$, para quaisquer $a, b \in D$.
   (b) $(a+b)^{p^n} = a^{p^n} + b^{p^n}$, para todo $n \geq 1$ e para quaisquer $a, b \in D$.
   (c) $\varphi : D \longrightarrow D$ definida por $\varphi(x) = x^{p^n}$ é um homomorfismo de anéis injetor.
2. Para cada α e K determine o polinômio mínimo de α sobre K, $[K(\alpha) : K]$ e uma base de $K(\alpha)|K$:

(a) $\alpha = i$, $K = \mathbb{Q}$

(b) $\alpha = i$, $K = \mathbb{R}$

(c) $\alpha = 3 + \sqrt{3}$, $K = \mathbb{Q}$.

(d) $\alpha = 3 + \sqrt{3}$, $K = \mathbb{R}$.

(e) $\alpha = \sqrt[4]{2} + 1$, $K = \mathbb{Q}$

(f) $\alpha = \sqrt[4]{2} + 1$, $K = \mathbb{Q}(\sqrt{2})$.

(g) $\alpha = \cos\frac{2\pi}{5} + i\,\mathrm{sen}\,\frac{2\pi}{5}$, $K = \mathbb{Q}$.

(h) $\alpha = \sqrt{2+\sqrt{2}}$, $K = \mathbb{Q}$

(i) $\alpha = \sqrt{2+\sqrt{2+\sqrt{2}}}$, $K = \mathbb{Q}$

(j) $\alpha = \sqrt[3]{2+\sqrt{2}}$, $K = \mathbb{Q}$.

3. Determine o polinômio mínimo de $\alpha = \cos\frac{2\pi}{p} + i\,\mathrm{sen}\,\frac{2\pi}{p}$ sobre $\mathbb{Q}$, onde p é natural primo.

4. Seja x uma indeterminada sobre $\mathbb{Z}_p$, p primo. Seja $L = \mathbb{Z}_p(x)$.

   (a) Seja $K = \mathbb{Z}_p(x^p)$. Mostre que $L = K(x)$.

   (b) Mostre que $[L : K] = p$.

5. Mostre que $\sqrt[4]{2}$ é algébrico sobre $\mathbb{Q}$.

   (a) Mostre que $K = \mathbb{Q}(\sqrt{2})$ é um subcorpo de $L = \mathbb{Q}(\sqrt[4]{2})$.

   (b) Mostre que $L = K(\sqrt[4]{2})$.

   (c) Determine $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}(\sqrt{2})]$.

6. Seja $L = \mathbb{Q}(\omega)$, onde $\omega = \cos\frac{2\pi}{5} + i\,\mathrm{sen}\,\frac{2\pi}{5}$.

   (a) Construa uma base de $L|\mathbb{Q}$.

   (b) Escreva $\dfrac{\omega}{1+\omega+\omega^2}$ como combinação linear dessa base.

7. Seja $L = \mathbb{Q}(\alpha)$, onde $\alpha = \sqrt[4]{2}$.

   (a) Mostre que $\{1, \alpha, \alpha^2, \alpha^3\}$ é uma base de $L|\mathbb{Q}$.

   (b) Escreva $\dfrac{\alpha - 2}{1+\alpha+2\alpha^2-3\alpha^3}$ como combinação linear da base do item anterior.

8. Sejam $L = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ e $K = \mathbb{Q}(\sqrt{2})$.

   (a) Mostre que K é um subcorpo de L.

   (b) Calcule $[L : K]$.

   (c) Mostre que todo elemento de L se escreve de uma única maneira como $r + s\sqrt{2+\sqrt{2}}$, com $r, s \in \mathbb{Q}(\sqrt{2})$.

   (d) Represente $\dfrac{3+\sqrt{2+\sqrt{2}}}{5-2\sqrt{2+\sqrt{2}}}$ na forma do item anterior.

9. Seja $L = \mathbb{Q}(i, \sqrt{5})$. Para todo $\alpha \in \{\sqrt{5}, i + \sqrt{5}, 2 + \sqrt{5}, i\sqrt{5}\}$

   (a) Determine o polinômio mínimo de α sobre $\mathbb{Q}$.

   (b) Determine para que valores de α temos $L = \mathbb{Q}(\alpha)$.

10. Sejam L corpo, K um subcorpo de L e S um subconjunto de L.

    O subanel de L obtido pela adjunção de S a K, denotado por $K[S]$, é

$$K[S] := \bigcap_{R \cup S \subset A} A,$$

    onde A é subanel de L.

    O subcorpo de L obtido pela adjunção de S a K, denotado por $K(S)$, é

$$K(S) := \bigcap_{K \cup S \subset F} F,$$

    onde F é subcorpo de L.

    (a) Mostre que $K[S]$ é o menor subanel de L que contém $K \cup S$ e $K(S)$ é o menor subcorpo de L que contém $K \cup S$.

    (b) Mostre que $K(S)$ é o corpo de frações de $K[S]$.

    (c) Seja $S = \{\alpha, \beta\}$. Mostre que

$$K[S] = \{f(\alpha, \beta) \mid f \in K[x, y]\}.$$

    (d) Conclua que se $S = \{\alpha, \beta\}$, então

$$K(S) = \left\{ \frac{f(\alpha, \beta)}{g(\alpha, \beta)} \mid f, g \in K[x, y], g(\alpha, \beta) \neq 0 \right\}.$$

    (e) Escreva uma generalização dos dois itens anteriores.

    (f) Seja $S = S_1 \cup S_2$. Mostre que

$$K[S] = K[S_1][S_2] \quad \text{e} \quad K(S) = K(S_1)(S_2).$$

11. Seja $L = K(z)$, sendo z transcendente sobre K.

    Mostre que L é uma extensão finita do corpo $F = K\left(\frac{z^3}{z+1}\right)$ e determine o polinômio mínimo de z sobre F.

12. Seja L uma extensão de K. Prove que $L|K$ será algébrica se, e somente se, todo anel R entre K e L for um corpo.

13. Seja M uma extensão do corpo K. Mostre que se $[M : K]$ é um número primo, então todo corpo L com $K \subset L \subset M$ satisfaz $L = K$ ou $L = M$.

14. Seja $M|K$ uma extensão de corpos de grau primo.

    Mostre que se $\beta \in M \backslash K$, então $M = K(\beta)$.

15. Seja $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Prove que os elementos $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$, bem como os elementos 1, $\sqrt{2} + \sqrt{3}, (\sqrt{2} + \sqrt{3})^2, (\sqrt{2} + \sqrt{3})^3$ formam uma base de $L|\mathbb{Q}$.

16. Seja $\alpha \in \mathbb{C}$ uma raiz do polinômio $x^3 - 2x + 2$ e seja $\beta = \alpha^2 - \alpha$. Prove que $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ e determine o polinômio mínimo de β sobre $\mathbb{Q}$.

17. Seja $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$ a fatoração em $L[x]$ do polinômio $f(x) \in K[x]$ e seja $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Prove:

    (a) $[L : K] \leq n!$.

    (b) Seja $f(x)$ irredutível em $K[x]$. Então $[L : K] = n$ se, e somente se, $L = K(\alpha_j)$ para algum $j \in \{1, 2 \ldots, n\}$, e, nesse caso, $L = K(\alpha_j)$ para todo $j \in \{1, 2 \ldots, n\}$.

    (c) Seja p primo; então $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ é irredutível em $\mathbb{Q}[x]$ e tem as condições equivalentes indicadas em (b).

18. Sejam $f(x), g(x) \in K[x]$, sendo $g(x)$ irredutível. Prove que se $f(x)$ e $g(x)$ tiverem uma raiz comum em alguma extensão L de K, então existirá $h(x) \in K[x]$ tal que $f(x) = g(x)h(x)$.

19. Seja $L|K$ uma extensão de corpos. Dizemos que $L|K$ é finitamente gerada se existem $\alpha_1, \ldots, \alpha_n \in L$, tais que $L = K(\alpha_1, \ldots, \alpha_n)$.

    (a) Mostre que toda extensão finita $L|K$ é finitamente gerada.

    (b) Dê exemplo de uma extensão $L|K$ finitamente gerada tal que $[L : K]$ não é finito.

Construção de uma raiz

Nosso objetivo é resolver equações em uma indeterminada com coeficientes em um corpo K, isto é, encontrar raízes para polinômios com coeficientes em um corpo K.

Definição 12 (Raiz)
Seja $L|K$ uma extensão de corpos e seja $f(x) \in K[x]$. Um elemento $\alpha \in L$ é uma *raiz de* $f(x)$ se, e somente se, $f(\alpha) = 0$.

Exemplo 26
Seja $\omega = \cos\frac{2\pi}{5} + i\,\mathrm{sen}\,\frac{2\pi}{5} \in \mathbb{C}$.
Então, $\omega^5 = 1$ e ω é raiz de $f(x) = x^5 - 1 \in \mathbb{Q}[x]$.
Observamos que $f(x) = (x-1)(x-\omega)(x-\omega^2)(x-\omega^3)(x-\omega^4)$ em $\mathbb{C}[x]$.
Entretanto, $\{1, \omega, \omega^2, \omega^3, \omega^4\} \subset \mathbb{Q}(\omega)$.
O corpo $\mathbb{Q}(\omega)$ contém todas as raízes de $f(x) \in \mathbb{Q}[x]$ e $\mathbb{Q}(\omega) \subsetneq \mathbb{C}$.

Lembre que o conjunto das raízes complexas n-ésimas da unidade é um grupo cíclico de ordem n, com a multiplicação de números complexos, gerado por $\omega = \cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n}$. Além disso, ω^j também é gerador, para todo j tal que $1 \leq j < n$ e $\mathrm{mdc}(n, j) = 1$.

Proposição 4
Seja $L|K$ uma extensão de corpos e $\alpha \in L$ uma raiz de $f(x) \in K[x]$. Então, $x - \alpha$ divide $f(x)$ em $L[x]$.

Demonstração: Como $f(x) \in K[x] \subset L[x]$, pela divisão euclidiana de $f(x)$ por $x - \alpha$ em $L[x]$, existem $q(x), r(x) \in L[x]$ tais que

$$f(x) = (x-\alpha)q(x) + r(x), \text{ onde } r(x) = 0 \text{ ou } 0 \leq \mathrm{grau}(r(x)) < 1.$$

Logo, podemos escrever $r(x) = r \in L$ e $f(x) = (x-\alpha)q(x) + r$. Assim, $0 = f(\alpha) = 0 \cdot q(\alpha) + r$, logo $r = 0$ e $f(x) = (x-\alpha)q(x)$. ■

Definição 13 (Multiplicidade)
Seja $L|K$ uma extensão de corpos. Dizemos que $\alpha \in L$ é uma raiz de *multiplicidade* m de $f(x) \in K[x]$ se, e somente se, $(x-\alpha)^m$ divide $f(x)$ em $L[x]$, mas $(x-\alpha)^{m+1}$ não divide $f(x)$ em $L[x]$.

Nesse caso, em $L[x]$ temos que $f(x) = (x-\alpha)^m q(x)$, com $q(\alpha) \neq 0$.

Verifique!

Quando $m = 1$ dizemos que α é uma *raiz simples* de f; com $m = 2$, α é uma raiz dupla; com $m = 3$, α é uma raiz tripla e assim, sucessivamente.

Quando $m \geq 2$ dizemos que α é uma *raiz múltipla* de $f(x)$.

Exemplo 27
Todas as raízes de $f(x) = x^5 - 1$ em $\mathbb{C}$ são simples, conforme o Exemplo 26.

Exemplo 28
O polinômio $f(x) = (x^2-2)^2(x^2+1)$ tem duas raízes duplas e duas raízes simples em $\mathbb{C}$, pois $f(x) = (x^2-2)^2(x^2+1) = (x-\sqrt{2})^2(x+\sqrt{2})^2(x+i)(x-i)$ em $\mathbb{C}[x]$.

Quantas raízes um polinômio de grau $n \geq 1$ tem em um corpo?

Contamos uma raiz $\alpha \in L$ de multiplicidade m como sendo m raízes: $\alpha_1 = \alpha, \ldots, \alpha_m = \alpha$.

Proposição 5
Seja K um corpo. Se $f(x) \in K[x]$ é um polinômio de grau $n \geq 1$, então $f(x)$ tem no máximo n raízes em qualquer extensão L de K.

Demonstração: Procederemos por indução sobre $n = \text{grau}(f(x)) \geq 1$.

Se $f(x) = ax + b$ com $a, b \in K$, $a \neq 0$ e $\alpha \in L$ é uma raiz de f, então $a\alpha + b = 0$ e $\alpha = -\frac{b}{a} \in K$. Portanto, um polinômio de grau 1 com coeficientes em K tem exatamente 1 raiz em $K \subset L$. Logo, tem exatamente 1 raiz em qualquer extensão L de K.

Suponhamos o resultado válido para os polinômios com coeficientes em K de grau s, tais que $1 \leq s < n$. Seja L uma extensão de K e seja $f(x) \in K[x]$ com $\text{grau}(f(x)) = n$.

Se $f(x)$ não tem raiz em L, então o resultado é, trivialmente, verdadeiro para $f(x)$.

Suponhamos que $f(x)$ tenha pelo menos uma raiz $\alpha \in L$ de multiplicidade m. Como $(x-\alpha)^m$ divide $f(x)$ em $L[x]$, temos que $n = \text{grau}(f(x)) \geq \text{grau}((x-\alpha)^m) = m$. Em $L[x]$ temos: $f(x) = (x-\alpha)^m q(x)$ com $q(\alpha) \neq 0$ e $\text{grau}(q(x)) = n - m \geq 0$. Se $\beta \in L$ é uma raiz de $f(x)$ e $\beta \neq \alpha$, então $0 = f(\beta) = (\beta-\alpha)^m q(\beta) \in L$. Como L é um corpo, temos que $q(\beta) = 0$. Portanto, β é uma raiz de $q(x)$ e $1 \leq \text{grau}(q(x)) = n-m < n$. Pela hipótese de indução, $q(x)$ tem no máximo $n - m$ raízes em L e assim, $f(x)$ tem no máximo $m + (n-m) = n = \text{grau}(f(x))$ raízes em L. ■

Lembre que $m = 1, 2, \ldots, n$.

Observação: A proposição anterior vale se substituímos $L|K$ por $R|D$, onde R é um domínio, D é um subanel de R e $f(x) \in D[x]$.

No entanto, em anéis que não são domínios o resultado é falso. Por exemplo, $f(x) = 2x \in A[x]$, onde $A = \mathbb{Z}_4[t]$ é o anel de polinômios com coeficientes em $\mathbb{Z}_4$. O polinômio $f(x)$ tem grau 1 e tem uma infinidade de raízes: $\alpha_j = 2t^j$, com $j = 0, 1, \ldots$.

Nosso objetivo, primeiramente, dado $f(x) \in K[x]$, é construir uma ex-

tensão L de K, tal que $f(x)$ tenha uma raiz α. Para isto, precisamos de outros conceitos da teoria de anéis comutativos com unidade. Vamos introduzir o anel quociente, construído a partir de um anel A, comutativo com unidade 1_A, e um ideal I de A.

Seja A um anel comutativo com unidade 1_A e I um ideal de A. Sabemos que A é um grupo abeliano aditivo e I é um subgrupo normal de A então, usando a congruência módulo I, podemos considerar o grupo quociente

$$A/I = \{I + a \ ; \ a \in A\},$$

onde $a, b \in A$ e $I + a = I + b$ se, e somente se, $a \equiv b \mod I$ se, e somente se, $a - b \in I$.

Lembre que ...
$I \subset A$ é um ideal de A se, e somente se,
$0_A \in I$;
$x, y \in I \Longrightarrow x + y \in I$;
$a \in A, x \in I \Longrightarrow a \cdot x \in I$.

Lembramos que a classe de equivalência de $a \in A$, denotada por $\overline{a}$, é chamada de *classe de congruência módulo* I ou *classe residual módulo* I. Temos

$$\begin{aligned} \overline{a} &= \{x \in A \ ; \ x \equiv a \mod I\} \\ &= \{x \in A \ ; \ x - a \in I\} \\ &= \{x \in A \ ; \ x \in I + a\} \\ &= I + a \end{aligned}$$

Sejam $a, b \in A$. A operação de adição em A/I é dada por

$$\overline{a} + \overline{b} = \overline{a + b}.$$

A seguinte propriedade adicional da congruência módulo I permitirá dar a A/I uma estrutura de anel comutativo.

Proposição 6 (Propriedade da congruência módulo I)
Sejam A um anel comutativo com unidade 1_A e I um ideal de A. Sejam $a, b, a', b' \in A$.

Se $a \equiv a' \mod I$ e $b \equiv b' \mod I$, então $a \cdot b \equiv a' \cdot b' \mod I$.

Demonstração: Sejam $a \equiv a' \mod I$ e $b \equiv b' \mod I$. Então, existem λ, λ' em I, tais que $a - a' = \lambda$ e $b - b' = \lambda'$. Logo,

$$\begin{aligned} a \cdot b - a' \cdot b' &= a \cdot b + (-a \cdot b' + a \cdot b') - a' \cdot b' = a \cdot (b - b') + (a - a') \cdot b' \\ &= a \cdot \lambda' + \lambda \cdot b' \in I, \end{aligned}$$

mostrando que $a \cdot b \equiv a' \cdot b' \mod I$. ■

Agora podemos definir a multiplicação em A/I e dar a A/I uma estrutura de anel comutativo.

Definição 14 (Multiplicação em A/I)
Sejam A um anel comutativo com unidade 1_A e I um ideal de A. Sejam $a, b \in A$. Definimos

$$\overline{a} \cdot \overline{b} \;=\; \overline{a \cdot b}$$

Observamos que essa definição não depende dos representantes das classes residuais. De fato, pela Proposição 6, temos que

$$\begin{array}{l} a \equiv a' \mod I \text{ e} \\ b \equiv b' \mod I \end{array} \quad \Longrightarrow \quad a \cdot b \equiv a' \cdot b' \mod I$$

$$\overset{(1)}{\Longleftrightarrow} \quad \overline{a \cdot b} = \overline{a' \cdot b'}$$

$$\overset{(2)}{\Longleftrightarrow} \quad \overline{a} \cdot \overline{b} = \overline{a \cdot b} = \overline{a' \cdot b'} = \overline{a'} \cdot \overline{b'}$$

Em (1) usamos que $c \sim d \Longleftrightarrow \overline{c} = \overline{d}$, em qualquer relação de equivalência. Em (2) reescrevemos a definição da multiplicação, usando a igualdade obtida em (1).

Logo, a multiplicação das classes residuais independe do elemento de A que é representante da classe.

Proposição 7 (Propriedades da adição e multiplicação de A/I)
Sejam A um anel comutativo com unidade 1_A e I um ideal de A.

A adição e a multiplicação de A/I têm as seguintes propriedades, para quaisquer $\overline{a}, \overline{b}, \overline{c} \in A/I$:

A1 (Associativa) $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$;
A2 (Comutativa) $\overline{a} + \overline{b} = \overline{b} + \overline{a}$;
A3 (Existência de elemento neutro) $\overline{0}_A = I$ é o elemento neutro aditivo

$$\overline{0}_A + \overline{a} = \overline{a};$$

A4 (Existência de simétrico) o simétrico de $\overline{a}$ é $\overline{-a}$

$$\overline{a} + \overline{-a} = \overline{0}_A;$$

M1 (Associativa) $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$;
M2 (Comutativa) $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$;
AM (Distributiva) $(\overline{a} + \overline{b}) \cdot \overline{c} = \overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c}$.

Além disso, quando $I \neq A$ temos a propriedade adicional:
M3 (Existência de unidade) $\overline{1}_A = I + 1_A$ é a unidade de A/I

Nesse caso, $\overline{0_A} \neq \overline{1_A}$, pois $A/I \neq \{\overline{0_A}\}$.

$$\overline{1}_A \cdot \overline{a} = \overline{a}.$$

Demonstração: As propriedades A1, A2, A3, A4 são as propriedades do grupo abeliano aditivo A/I. M2 e M3 são facilmente verificadas.

Faremos a demonstração apenas de M1 e AM.

$$\begin{aligned}(\overline{a} \cdot \overline{b}) \cdot \overline{c} &\overset{(1)}{=} \overline{a \cdot b} \cdot \overline{c} \\ &\overset{(2)}{=} \overline{(a \cdot b) \cdot c} \\ &\overset{(3)}{=} \overline{a \cdot (b \cdot c)} \\ &\overset{(4)}{=} \overline{a} \cdot \overline{b \cdot c} \\ &\overset{(5)}{=} \overline{a} \cdot (\overline{b} \cdot \overline{c}),\end{aligned}$$

Em (1) e (2) usamos a definição da multiplicação das classes residuais. Em (3) usamos que a multiplicação em A é associativa. Em (4) e (5), novamente, usamos a definição da multiplicação das classes residuais.

mostrando M1.

$$\begin{aligned}(\overline{a} + \overline{b}) \cdot \overline{c} &\overset{(1)}{=} \overline{a + b} \cdot \overline{c} \\ &\overset{(2)}{=} \overline{(a + b) \cdot c} \\ &\overset{(3)}{=} \overline{a \cdot c + b \cdot c} \\ &\overset{(4)}{=} \overline{a \cdot c} + \overline{b \cdot c} \\ &\overset{(5)}{=} \overline{a} \cdot \overline{c} + \overline{b} \cdot \overline{c},\end{aligned}$$

Em (1) usamos a definição da adição das classes residuais e em (2), a definição da multiplicação. Em (3) usamos a distributividade em A. Em (4) usamos a definição da adição das classes residuais e em (5), a definição da multiplicação.

mostrando AM. ■

Observação: Quando $I = A$ para quaisquer $a, b \in A$ temos que $a \equiv b \mod I$. Nesse caso, $A/I = \{\overline{0_A}\}$ é o anel identicamente nulo.

Corolário 3

Sejam A um anel comutativo com unidade 1_A e I um ideal de A. Então, A/I é um anel comutativo. Mais ainda, se $I \neq A$, então A/I é um anel comutativo com unidade $I + 1_A$.

Há dois tipos de ideais que desempenham um papel importante no contexto dos anéis quociente.

Definição 15 (Ideal primo ou ideal maximal)

Seja A um anel comutativo com unidade.

Um ideal P de A, $P \neq A$, é um *ideal primo* se, e somente se,

se $a, b \in A$ e $a \cdot b \in P$, então $a \in P$ ou $b \in P$.

Um ideal M de A, $M \neq A$, é um *ideal maximal* se, e somente se,

para qualquer ideal I de A, tal que $M \subsetneq I \subset A$, temos $I = A$.

Exemplo 29

Seja A um domínio. O ideal $I = \{0\}$ é um ideal primo, pois se $a, b \in A$ e $a \cdot b = 0$, então $a = 0$ ou $b = 0$.

Exemplo 30

Em $\mathbb{R}[x]$, o ideal $I = I(x^2 - 3x + 2)$ não é um ideal primo, pois $x^2 - 3x + 2 = (x-1)(x-2) \in I$, com $x - 1 \notin I$ e $x - 2 \notin I$.

Definição 16 (Elemento primo)

Seja A um domínio. Um elemento $p \in A$ não-invertível é dito *primo* se, e somente se, $a, b \in A$ e p divide $a \cdot b$, então p divide a ou p divide b. Assim, p é primo se, e somente se, o ideal $I(p)$ é primo.

Exemplo 31

Num domínio A, se p é primo, então p é irredutível.

De fato, suponhamos que $p = a \cdot b$. Então, p divide $a \cdot b$. Como p é primo, temos que p divide a ou p divide b. Digamos que p divide b. Logo, existe $\lambda \in A$, tal que $b = \lambda \cdot p$ e $p = a \cdot b = a \cdot \lambda \cdot p$. Cancelando p, obtemos $1_A = a \cdot \lambda$, mostrando que a é invertível.

Exemplo 32

Num domínio principal todo elemento irredutível é primo.

De fato, seja p irredutível e suponhamos que p divida $a \cdot b$, com p não dividindo a. Então, $\text{mdc}(p, a) = 1_A$. Como A é um domínio principal, então existem $x, y \in A$ tais que $1 = x \cdot p + y \cdot a$. Logo,

$$b = 1_A \cdot b = (x \cdot p + y \cdot a) \cdot b = x \cdot p \cdot b + y \cdot a \cdot b \in pA,$$

mostrando que p divide b.

Exemplo 33

Nos domínios principais todo ideal gerado por um elemento irredutível é um ideal maximal.

De fato, seja $M = pA$, onde p é irredutível. Consideremos um ideal I de A tal que $M = pA \subsetneq I$. Vamos mostrar que $I = A$.

Como $M = pA \subsetneq I$, existe $a \in I$ tal que $a \notin M = pA$. Logo, a não é múltiplo de p. Como p é primo, temos que $\text{mdc}(p, a) = 1$. Portanto, existem $x, y \in A$ tais que $1 = x \cdot p + y \cdot a$. Observando que $x \cdot p \in M \subset I$, $y \cdot a \in I$ e I é um ideal, concluímos que $1 = x \cdot p + y \cdot a \in I$. Logo, $I = A$.

Exemplo 34

No domínio principal dos inteiros o ideal $\{0\}$ é primo e não é maximal, pois

$$\{0\} \subsetneq n\mathbb{Z} \subsetneq \mathbb{Z}, \text{ para todo } n \in \{2, 3, 4, \ldots\}.$$

Os ideais maximais de $\mathbb{Z}$ são $I(p)$, onde p é um natural primo.

Exemplo 35

No domínio principal $\mathbb{R}[x]$ os ideais maximais são $I(x-a)$, onde $a \in \mathbb{R}$ ou $I(x^2+bx+c)$, tais que $b, c \in \mathbb{R}$ e $b^2 - 4c < 0$.

No domínio principal $\mathbb{C}[x]$ os ideais maximais são $I(x-a)$, onde $a \in \mathbb{C}$.

Em $K[x]$, K corpo, os ideais $I(x-a)$, onde $a \in K$ são sempre maximais.

Proposição 8

Seja A um anel comutativo com unidade 1_A. Se M é um ideal maximal, então M é um ideal primo.

Demonstração: Seja M um ideal maximal de A. Sejam $a, b \in A$, tais que $a \cdot b \in M$ e $a \notin M$. Vamos mostrar que $b \in M$.

Consideremos o ideal $I = M + I(a)$. Observamos que $M \subsetneq M + I(a)$, pois $a \in M + I(a)$ e $a \notin M$. Como M é ideal maximal, então $A = M + I(a)$. Logo, existem $m \in M$ e $x \in A$, tais que $1_A = m + x \cdot a$. Multiplicando a igualdade anterior por b, obtemos

$$b = 1_A \cdot b = (m + x \cdot a) \cdot b = m \cdot b + x \cdot a \cdot b \in M. \qquad \blacksquare$$

A soma de ideais é um ideal. Se I e J são ideais de A, então a soma $I + J$ é um ideal, onde $I + J = \{x + y \,;\, x \in I \text{ e } y \in J\}$.

Proposição 9

Seja A um anel comutativo com unidade 1_A. Valem as seguintes propriedades:

(i) P é um ideal primo de A se, e somente se, A/P é um domínio.

(ii) M é um ideal maximal de A se, e somente se, A/M é um corpo.

Num domínio principal temos que p é primo se, e somente se, p é irredutível, isto é, p não é invertível e se $p = a \cdot b$, então a ou b é invertível.

Demonstração:

(i) ($\Longrightarrow$:) Suponhamos que P seja um ideal primo de A. Como $P \neq A$, pelo Corolário 3 sabemos que A/P é um anel comutativo com unidade. Sejam $a, b \in A$ tais que $\overline{a} \cdot \overline{b} = \overline{0_A}$. Então,

$$\begin{aligned} \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \overline{0_A} \quad &\text{se, e somente se,} \quad a \cdot b \equiv 0_A \mod P \\ &\text{se, e somente se,} \quad a \cdot b \in P. \end{aligned}$$

Como P é um ideal primo, temos $a \in P$ ou $b \in P$. Portanto, $\overline{a} = \overline{0_A}$ ou $\overline{b} = \overline{0_A}$.

(i)($\Longleftarrow$:) Suponhamos que A/P seja um domínio. Então, A/P é um anel com unidade e assim, $P \subsetneq A$. Sejam $a, b \in A$, tais que $a \cdot b \in P$. Então,

$\overline{0_A} = \overline{a \cdot b} = \overline{a} \cdot \overline{b}$. Como A/P é um domínio, temos $\overline{a} = \overline{0_A}$ ou $\overline{b} = \overline{0_A}$. Portanto, $a \in P$ ou $b \in P$.

(ii)($\Longrightarrow$:) Suponhamos que M seja um ideal maximal de A. Pela Proposição 8, M é um ideal primo e, pelo item (i), A/M é um domínio. Precisamos mostrar apenas que todo elemento $\overline{a} \neq \overline{0_A}$ em A/M é invertível. Como $\overline{a} \neq \overline{0_A}$, então $a \notin M$ e $M \subsetneq M + I(a) \subset A$. Logo, $A = M + I(a)$. Assim, existem $m \in M$ e $x \in A$ tais que $1_A = m + x \cdot a$. Tomando as classes módulo M, obtemos

Lembre que ...
$M + I(a)$ é um ideal, pois a soma de ideais é um ideal.

$$\overline{1_A} = \overline{m + x \cdot a} = \overline{m} + \overline{x \cdot a} = \overline{x} \cdot \overline{a}.$$

Logo, $\overline{x}$ é o inverso de $\overline{a}$ em A/M.

(ii)($\Longleftarrow$:) Suponhamos que A/M seja um corpo. Então, A/M é um domínio e, pelo item (i), M é um ideal primo. Logo, $M \neq A$. Seja I um ideal de A tal que $M \subsetneq I \subset A$. Tome $x \in I$ tal que $x \notin M$. Então, $\overline{x} \neq \overline{0_A}$ e existe $\overline{y} \in A/M$ tal que $\overline{1_A} = \overline{x} \cdot \overline{y} = \overline{x \cdot y}$. Logo, existe $m \in M$, tal que $1_A - x \cdot y = m \in M$, isto é, $1_A = m + x \cdot y \in I$. Portanto, $I = A$, mostrando que M é maximal. ■

Note que ...
$m \in M \subsetneq I \Longrightarrow m \in I$,
$x \in I, y \in A \Longrightarrow x \cdot y \in I$.
Assim, $m + x \cdot y \in I$.

Como aplicação, temos uma nova demonstração do seguinte resultado.

Corolário 4
Sejam K um corpo, $p(x) \in K[x]$ polinômio mônico.

$K[x]/(p(x))$ é um corpo se, e somente se, $p(x)$ é irredutível.

Seja K um corpo e seja $p(x) \in K[x]$ polinômio mônico irredutível com $n = \text{grau}(p(x))$. Consideremos $M = (p(x))$. Então,

Forçosamente, $n \geq 1$.

$$L = K[x]/M = \{M + f(x)\ ;\ f(x) \in K[x]\} \text{ é um corpo.}$$

Seja $f(x) \in K[x]$. Pela divisão euclidiana de $f(x)$ por $p(x)$, existem $q(x)$ e $r(x)$ em $K[x]$, unicamente determinados, tais que

$$f(x) = p(x)q(x) + r(x), \text{ onde } r(x) = 0 \text{ ou } 0 \leq \text{grau}(r(x)) < n.$$

Podemos escrever $r(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, com $a_0, \ldots, a_{n-1}$ em K.

Assim,

$$\begin{aligned} M + f(x) &= M + \underbrace{p(x)q(x)}_{\in M} + r(x) \\ &= M + r(x) \\ &= M + (a_0 + a_1x + \cdots + a_{n-1}x^{n-1}) \\ &= (M + a_0) + (M + a_1)(M + x) + \cdots + (M + a_{n-1})(M + x)^{n-1}. \end{aligned}$$

Na última igualdade usamos as definições da adição e da multiplicação de classes: a classe da soma de polinômios é a soma das classes dos polinômios; a classe de um produto de polinômios é o produto das classes dos polinômios.

Escrevendo $\alpha = M + x$, temos:

$$M + f(x) = (M + a_0) + (M + a_1)\alpha + \cdots + (M + a_{n-1})\alpha^{n-1}.$$

Suponhamos que $a, b \in K$ e $M + a = M + b$. Então, $a - b \in M \cap K$ logo, $a - b$ é múltiplo de $p(x)$ e $a - b \in K$, portanto $a - b = 0$, isto é, $a = b$.

Assim, o homomorfismo de anéis

$$\begin{array}{ccc} K & \longrightarrow & L = K[x]/M \\ a & \longmapsto & M + a \end{array}$$

é injetor e $\{M + a\ ;\ a \in K\}$ é um subcorpo de $L = K[x]/M$ isomorfo a K.

Identificamos $\{M + a\ ;\ a \in K\} \subset L = K[x]/M$ com $\{a\ ;\ a \in K\}$ e assim,

$$L = K[x]/M \simeq \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\ ;\ a_j \in K\} = K[\alpha], \text{ com } p(\alpha) = 0.$$

A última afirmação decorre do fato de M ser o elemento neutro aditivo do anel quociente e escrevendo $p(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$ temos

$$M = M + p(x) \simeq \alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = p(\alpha).$$

A passagem ao quociente do domínio $K[x]$ pelo ideal maximal gerado pelo polinômio mônico irredutível fabrica uma raiz para esse polinômio, a saber, $\alpha = M + x \in L$, a classe de x. $L \simeq K[\alpha]$ é K-espaço vetorial de dimensão $n = \text{grau}(p(x))$ e é uma extensão de K na qual $p(x)$ tem uma raiz.

Provamos o seguinte teorema.

Teorema 2
Sejam K um corpo e $p(x) \in K[x]$ polinômio mônico irredutível. Então, existe uma extensão $L|K$ com $[L : K] = n$, tal que $p(x)$ tem uma raiz $\alpha \in L$.

Sabemos que polinômios de graus 2 ou 3 com coeficientes em um corpo K são irredutíveis em $K[x]$ se, e somente se, não têm raízes em K.

Vamos dar um exemplo, interessantíssimo.

Cuidado! $x^4 + x^2 + 1$ não tem raízes em $\mathbb{Z}_2$, mas não é irredutível em $\mathbb{Z}_2[x]$, pois $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.

Exemplo 36

Consideremos o polinômio $p(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$.

Avaliando $p(x)$ em $0, 1 \in \mathbb{Z}_2$, temos $p(0) = 1$ e $p(1) = 1$. Portanto, $p(x)$ não tem raízes em $\mathbb{Z}_2$. Logo, $p(x)$ é irredutível em $\mathbb{Z}_2[x]$.

Seja $L = \mathbb{Z}_2[x]/(x^2+x+1) \simeq \mathbb{Z}_2[\alpha] = \{a + b\alpha\,;\ a, b \in \mathbb{Z}_2\}$ e $\alpha^2 + \alpha + 1 = 0$.

Assim, $\mathbb{Z}_2 \subset \mathbb{Z}_2[\alpha]$, $\mathrm{car}(\mathbb{Z}_2[\alpha]) = 2$, $[\mathbb{Z}_2[\alpha] : \mathbb{Z}_2] = 2$ e $\mathbb{Z}_2[\alpha]$ é um corpo com 2^2 elementos, pois $x^2 + x + 1$ é o polinômio mínimo de α sobre $\mathbb{Z}_2$ e $\{1, \alpha\}$ é uma base de $\mathbb{Z}_2[\alpha]|\mathbb{Z}_2$.

Observamos que $\mathbb{Z}_2[\alpha] = \{0, 1, \alpha, 1 + \alpha\}$.

O polinômio mínimo de α sobre $\mathbb{Z}_2$ nos dá a relação algébrica relevante para fazer as multiplicações em $\mathbb{Z}_2[\alpha]$. As potências de α podem ser obtidas da seguinte maneira:

$$\begin{aligned} \alpha^2 + \alpha + 1 = 0 &\iff \alpha^2 = -\alpha - 1 = \alpha + 1 \\ &\implies \alpha^3 = \alpha^2 \cdot \alpha = (\alpha + 1)\alpha = \alpha^2 + \alpha = 1 \\ &\implies \alpha^3 = 1. \end{aligned}$$

O polinômio $x^3 - 1$ tem todas as suas raízes em $\mathbb{Z}_2[\alpha]$.

Veja o Exercício 1 da Seção 1, que ensina a calcular potências p-ésimas em um corpo de característica p.

De fato, $x^3 - 1 = (x - 1)(x^2 + x + 1)$.

Como $p(\alpha + 1) = (\alpha + 1)^2 + (\alpha + 1) + 1 = (\alpha^2 + 1) + \alpha = \alpha^2 + \alpha + 1 = 0$, então $\alpha + 1$ é a outra raiz de $x^2 + x + 1$. Logo, as raízes de $x^3 - 1$ são $1, \alpha$ e $\alpha + 1$.

Para todo p primo e todo $n \geq 1$ existe um corpo de característica p com p^n elementos, conforme veremos no próximo Exemplo.

Em *Códigos Corretores de Erros* de A. Hefez e M.L.T. Villela, Série Computação e Matemática, IMPA, 2002, veja no Teorema 2, página 70, a existência de polinômios mônicos irredutíveis em $\mathbb{Z}_p[x]$ de grau n, para todo $n \geq 1$.

Exemplo 37

Seja p um natural primo. Para cada $n \geq 1$ existe $p(x) \in \mathbb{Z}_p[x]$ mônico irredutível de grau n. Então, $L = \mathbb{Z}_p[x]/(p(x))$ é um corpo com p^n elementos de característica prima p, em virtude de $L \simeq \mathbb{Z}_p[\alpha]$, onde $\alpha = (p(x)) + x$ e $[\mathbb{Z}_p[\alpha] : \mathbb{Z}_p] = n$.

Corolário 5

Seja $f(x) \in K[x]$ com $\mathrm{grau}(f(x)) \geq 1$. Então, existe uma extensão finita $L|K$ na qual $f(x)$ tem uma raiz α e $[L : K] \leq \mathrm{grau}(f(x))$.

Demonstração: Seja $p(x) \in K[x]$ um fator mônico e irredutível de $f(x)$. Como $p(x)$ divide $f(x)$, toda raiz de $p(x)$ é uma raiz de $f(x)$.

Pelo Teorema anterior, existe extensão $L|K$ na qual $p(x)$ tem uma raiz α e $[L : K] = \mathrm{grau}(p(x)) \leq \mathrm{grau}(f(x))$. ■

Teorema 3

Seja $f(x) \in K[x]$ com $n = \text{grau}(f(x)) \geq 1$. Então, existe uma extensão L de K tal que $[L : K] \leq n!$ na qual $f(x)$ tem n raízes (L tem todas as raízes de $f(x)$).

Demonstração: Indução sobre $n = \text{grau}(f(x))$.

Se $f(x) \in K[x]$ tem grau 1, então $f(x)$ tem todas as suas raízes em $L = K$ e $[L : K] = 1 \leq 1!$.

Suponhamos o resultado válido para polinômios de grau s com coeficientes em corpos, onde $1 \leq s < n$. Seja $f(x) \in K[x]$ com $\text{grau}(f(x)) = n$. Vamos mostrar que vale para $f(x)$.

Pelo Corolário anterior, existe uma extensão $F|K$ na qual $f(x)$ tem uma raiz α_1 e $[F : K] \leq \text{grau}(f(x)) = n$. Em $F[x]$ temos $f(x) = (x - \alpha_1)q(x)$, com $\text{grau}(q(x)) = n - 1$ e $q(x) \in F[x]$. Por hipótese de indução, existe uma extensão L de F, na qual $q(x)$ tem $n - 1$ raízes com $[L : F] \leq (n-1)!$. As raízes de $f(x)$ são α_1 e as raízes de $q(x)$. Portanto, em L o polinômio $f(x)$ tem n raízes, o máximo possível, e $[L : K] = [F : K][L : F] \leq n(n-1)! = n!$.

■

L
| $\leq (n-1)!$
F
| $\leq n$
K

Exemplo 38

O polinômio $f(x) = x^2 + 1 \in \mathbb{Q}[x]$ tem todas as suas raízes em $\mathbb{Q}(i)$ e $[\mathbb{Q}(i) : \mathbb{Q}] = 2 = 2!$.

Exemplo 39

O polinômio $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ tem todas as suas raízes em $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ e $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4 < 4!$.

Exemplo 40

O polinômio $f(x) = x^3 - 1 \in \mathbb{Q}[x]$ tem todas as suas raízes em $\mathbb{Q}(\omega)$, onde $\omega = \cos\frac{2\pi}{3} + i\,\text{sen}\,\frac{2\pi}{3}$ e $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2 < 3!$.

Lembre que $x^3 - 1 = (x-1)(x^2 + x + 1) = (x-1)(x-\omega)(x-\omega^2)$.

Exemplo 41

O polinômio $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ se decompõe em $\mathbb{C}[x]$ como

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2}).$$

$\mathbb{C} \supset \mathbb{Q}$, mas $\mathbb{C}$ é um corpo muito grande. Todas as raízes de $f(x)$ estão em $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\omega, \sqrt[3]{2})$ e $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = 6 = 3!$.

Exercícios

1. Seja $\mathbb{R}[x]$ o domínio dos polinômios com coeficientes reais.

   Seja $I = I(x)$ o ideal gerado por x.

   (a) Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{R}[x]$.
   Mostre que $\overline{f(x)} = \overline{a_0}$, isto é, $f(x) \equiv a_0 \mod I$.

   (b) Sejam $a, b \in \mathbb{R}$.
   Mostre que $a \equiv b \mod I$ se, e somente se, $a = b$.

   (c) Mostre que $\mathbb{R}[x]/I$ é um corpo e conclua que $I = I(x)$ é um ideal maximal de $\mathbb{R}[x]$.

   (d) Identifique o anel $\mathbb{R}[x]/I$.

2. Seja $\mathbb{Z}[x]$ o domínio dos polinômios com coeficientes inteiros.

   Seja $I = I(x)$ o ideal gerado por x.

   (a) Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$.
   Mostre que $\overline{f(x)} = \overline{a_0}$, isto é, $f(x) \equiv a_0 \mod I$.

   (b) Sejam $a, b \in \mathbb{Z}$.
   Mostre que $a \equiv b \mod I$ se, e somente se, $a = b$.

   (c) Mostre que $\mathbb{Z}[x]/I$ é um domínio e conclua que $I = I(x)$ é um ideal primo de $\mathbb{Z}[x]$.

   $\mathbb{Z}[x]$ não é um domínio principal. O ideal $I(2, x)$ não é principal.

   (d) Identifique o anel $\mathbb{Z}[x]/I$.

   (e) Conclua que I não é um ideal maximal.

3. Seja $p(x) = x^2 + 1 \in \mathbb{R}[x]$.

   (a) Mostre que $p(x)$ é irredutível em $\mathbb{R}[x]$.

   (b) Seja $L = \mathbb{R}[x]/(p(x))$. Mostre que L é um corpo isomorfo a $\mathbb{C}$.

4. Seja $p(x) = x^3 + x + 1$.

   (a) Mostre que $p(x)$ é irredutível em $\mathbb{Z}_2[x]$.

   (b) Seja $L = \mathbb{Z}_2[x]/(p(x))$. Mostre que L é um corpo com 8 elementos.

   (c) Construa a tabela de multiplicação dos elementos de L.

5. Seja $p(x) = x^2 + 1$.

   (a) Mostre que $p(x)$ é irredutível em $\mathbb{Z}_3[x]$.

(b) Seja $L = \mathbb{Z}_3[x]/(p(x))$. Mostre que L é um corpo com 9 elementos.

(c) Construa a tabela de multiplicação dos elementos de L.

6. Seja $p(x) = x^4 + x + 1$.

(a) Mostre que $p(x)$ é irredutível em $\mathbb{Z}_2[x]$.

(b) Seja $L = \mathbb{Z}_2[x]/(p(x))$. Mostre que L é um corpo com 16 elementos.

(c) Seja $\alpha = (p(x)) + x$. Mostre que $\alpha^{15} = 1$ e os elementos não-nulos de L podem ser escritos como α^j, onde $j = 1, \ldots, 14$.

7. Seja $L|K$ uma extensão de grau n.

(a) Mostre que para todo $\alpha \in L$, o grau do polinômio mínimo de α sobre K divide n.

(b) Mostre que se $p(x) \in K[x]$ é irredutível em $K[x]$ e grau$(p(x))$ não divide n, então $p(x)$ não tem raízes em L.

(c) Mostre que $x^3 - 2$ não tem raízes em $\mathbb{Q}(\sqrt[n]{2})$, para todo $n = 2^m$, onde $m \geq 1$, $m \in \mathbb{N}$.

Para os alunos que querem saber mais sobre ideais maximais.

8. Seja p um natural primo. Consideremos

$$A = \left\{ \frac{m}{n} \; ; \; m, n \in \mathbb{Z} \text{ e } p \text{ não divide } n \right\}.$$

(a) Mostre que A é um anel comutativo com unidade.

(b) Seja $P = \left\{ \frac{m}{n} \in A \; ; \; p \text{ divide } m \right\}$.
Mostre que P é um ideal maximal de A.

Corpos de decomposição

Vamos introduzir o conceito de corpo de decomposição ou corpo de raízes sobre K de um polinômio $f(x) \in K[x] \backslash K$. A idéia é construir uma extensão L de K tal que $f(x)$ se decomponha num produto de potências de fatores lineares em $L[x]$, de modo que L seja o menor corpo com essa propriedade.

Definição 17 (Corpo de decomposição ou corpo de raízes)
Seja $f(x) \in K[x]$ com grau$(f(x)) \geq 1$. Uma extensão $L|K$ é dita um *corpo de decomposição ou corpo de raízes* de $f(x)$ sobre K se, e somente se, $f(x)$ se decompõe em produto de fatores lineares em $L[x]$ e não se decompõe em produto de fatores lineares em $F[x]$, onde F é qualquer subcorpo próprio de L contendo K.

Observação 1: Pela definição acima, L é o menor corpo contendo K com a propriedade de $f(x)$ ter grau$(f(x))$ raízes em L.

Observação 2: Veremos que, essencialmente, $L = K(\alpha_1, \ldots, \alpha_n)$, onde $n =$ grau$(f(x))$ e $\alpha_1, \ldots, \alpha_n$ são as raízes de f, contadas com as suas multiplicidades.

Exemplo 42
Os 4 Exemplos anteriores são exemplos de corpos de decomposição sobre $\mathbb{Q}$, a saber,

$\mathbb{Q}(i, -i) = \mathbb{Q}(i)$ é corpo de decomposição sobre $\mathbb{Q}$ de $x^2 + 1 \in \mathbb{Q}[x]$.

$\mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ é corpo de decomposição sobre $\mathbb{Q}$ de $(x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$.

$\mathbb{Q}(1, \omega, \omega^2) = \mathbb{Q}(\omega)$, com $\omega = \cos\frac{2\pi}{3} + i\,\mathrm{sen}\,\frac{2\pi}{3}$, é corpo de decomposição sobre $\mathbb{Q}$ de $x^3 - 1 \in \mathbb{Q}[x]$.

$\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\omega, \sqrt[3]{2})$, com $\omega = \cos\frac{2\pi}{3} + i\,\mathrm{sen}\,\frac{2\pi}{3}$, é corpo de decomposição sobre $\mathbb{Q}$ de $x^3 - 2 \in \mathbb{Q}[x]$.

Digamos que $L|K$ e $L'|K$ são corpos de decomposição sobre K de $f(x)$ em $K[x]$. Qual a relação entre L e L'?

Definição 18 (Extensões isomorfas)
Dizemos que $L|K$ e $L'|K'$ são *extensões isomorfas* se, e somente se, existe $\varphi : L \longrightarrow L'$ isomorfismo de corpos tal que $\varphi(K) = K'$.

Definição 19 (Extensão de isomorfismo)
Seja $\varphi : K \longrightarrow K'$ um isomorfismo de corpos e sejam $L|K$ e $L'|K'$ extensões

de corpos. Dizemos que $\psi : L \longrightarrow L'$ *estende* φ se, e somente se, ψ é um isomorfismo, tal que $\psi|_K = \varphi$. Equivalentemente, o seguinte diagrama é comutativo:

$$\begin{array}{ccc} L & \overset{\psi}{\dashrightarrow} & L' \\ i\uparrow & & i'\uparrow \\ K & \xrightarrow{\varphi} & K', \end{array}$$

onde $i : K \longrightarrow L$ e $i' : K' \longrightarrow L'$ são as inclusões naturais.

Nesse caso, $L|K$ e $L'|K'$ são extensões isomorfas.

Proposição 10 (Extensão de isomorfismo)
Seja $\varphi : K \longrightarrow K'$ um isomorfismo de corpos, então

(i) $K[x]$ e $K'[x]$ são domínios isomorfos.

(ii) Se $L|K$ e $L'|K'$ são extensões de corpos, $p(x) \in K[x]$ é mônico irredutível, $\alpha \in L$ é raiz de $p(x)$ e $\beta \in L'$ é raiz de $\varphi(p)(x)$, então o isomorfismo $\varphi : K \longrightarrow K'$ admite extensão, também denotada por φ, $\varphi : K(\alpha) \longrightarrow K'(\beta)$ definida por $\varphi(\alpha) = \beta$. Equivalentemente, o seguinte diagrama é comutativo:

$$\begin{array}{ccc} K(\alpha) & \overset{\varphi}{\dashrightarrow} & K'(\beta) \\ i\uparrow & & i'\uparrow \\ K & \xrightarrow{\varphi} & K', \end{array}$$

onde $\varphi(\alpha) = \beta$ e $i : K \longrightarrow K(\alpha)$ e $i' : K' \longrightarrow K'(\beta)$ são as inclusões naturais.

Demonstração:

(i) De fato, se $f(x) = a_0 + a_1x + \cdots + a_mx^m \in K[x]$ e definimos $\varphi(f)(x) = \varphi(a_0) + \varphi(a_1)x + \cdots + \varphi(a_m)x^m$, então $\varphi : K[x] \longrightarrow K'[x]$ é um isomorfismo de anéis.

(ii) É claro que $p(x)$ é irredutível em $K[x]$ se, e somente se, $\varphi(p)(x)$ é irredutível em $K'[x]$.

Como $\alpha \in L$ é raiz de $p(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$, então $0 = p(\alpha) = \alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0$.

Se existe isomorfismo φ do corpo $K(\alpha)$ em outro corpo, então

$\varphi(1_K) = 1_{K'}$.

$$\begin{aligned} 0 = \varphi(0) &= \varphi(\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0) \\ &= \varphi(\alpha)^n + \varphi(b_{n-1})\varphi(\alpha)^{n-1} + \cdots + \varphi(b_1)\varphi(\alpha) + \varphi(b_0) \\ &= \varphi(p)(\varphi(\alpha)), \end{aligned}$$

isto é, $\varphi(\alpha)$ é raiz de $\varphi(p)(x)$, com $\varphi(p)(x)$ mônico e irredutível no domínio $\varphi(K)[x] = K'[x]$.

A extensão φ está perfeitamente definida se conhecemos $\varphi(\alpha)$, pois $\varphi(\alpha^2) = \varphi(\alpha \cdot \alpha) = \varphi(\alpha)^2, \ldots, \varphi(\alpha^{n-1}) = \varphi(\alpha)^{n-1}$ e $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de $K(\alpha)$ sobre K, onde $n = \text{grau}(p(x))$.

$p(x)$ é o polinômio mínimo de α sobre K.

Portanto, dado isomorfismo $\varphi : K \longrightarrow K'$ existe um único isomorfismo $\varphi : K(\alpha) \longrightarrow K'(\beta)$ com $\varphi(\alpha) = \beta$. ■

Corolário 6 (Extensão da identidade)
Se $p(x) \in K(x)$ é polinômio mônico irredutível e α e β são duas raízes de $p(x)$, então $K(\alpha)$ e $K(\beta)$ são corpos isomorfos com $\varphi : K(\alpha) \longrightarrow K(\beta)$ definida por $\varphi(a) = a$, para $a \in K$ e $\varphi(\alpha) = \beta$. Nesse caso, $\varphi|_K = I$, isto é, φ estende a função identidade em K e dizemos que φ é um K-isomorfismo.

Isso motiva a seguinte definição.

Definição 20 (K-isomorfismo)
Dizemos que $L|K$ e $L'|K$ são extensões K-isomorfas se, e somente se, existe $\varphi : L \longrightarrow L'$ um isomorfismo, tal que $\varphi|_K = I$, equivalentemente, existe um isomorfismo de L em L' que estende $I : K \longrightarrow K$. Nesse caso, o seguinte diagrama é comutativo

$$\begin{array}{ccc} L & \overset{\varphi}{\dashrightarrow} & L' \\ i \uparrow & & i' \uparrow \\ K & \overset{I}{\longrightarrow} & K \end{array}$$

onde $i : K \longrightarrow L$ e $i' : K \longrightarrow L'$ são as inclusões naturais.

Teorema 4 (Extensão de isomorfismo a corpos de raízes)
Sejam $f(x) \in K[x] \backslash K$, $\varphi : K \longrightarrow K'$ um isomorfismo de corpos, L um corpo de raízes de $f(x)$ sobre K e L' um corpo de raízes de $\varphi(f)(x)$ sobre K'. Então, $L|K$ e $L'|K'$ são extensões isomorfas, com um isomorfismo ψ que estende φ.

$$\begin{array}{ccc} L & \overset{\psi}{\dashrightarrow} & L' \\ i \uparrow & & i' \uparrow \\ K & \overset{\varphi}{\longrightarrow} & K' \end{array}$$

Antes de demonstrarmos esse Teorema, como conseqüência, obtemos o seguinte resultado muito importante:

Corolário 7 (Unicidade do corpo de decomposição)
Se $L|K$ e $L'|K$ são corpos de decomposição sobre K de $f(x) \in K[x] \backslash K$, então $L|K$ e $L'|K$ são extensões K-isomorfas.

Demonstração: Tomamos no Teorema anterior $K' = K$ e $\varphi = I$, $I : K \longrightarrow K$. Então, existe isomorfismo $\psi : L \longrightarrow L'$ tal que o seguinte diagrama é comutativo

$$\begin{array}{ccc} L & \overset{\psi}{\dashrightarrow} & L' \\ i\uparrow & & i'\uparrow \\ K & \overset{I}{\longrightarrow} & K \end{array}$$

isto é, $\psi(a) = a$, para todo $a \in K$. ■

Demonstração do Teorema 4: A prova será feita por indução sobre $n = [L : K]$.

Suponhamos que $[L : K] = 1$. Então, $f(x) \in K[x]$ se decompõe em $L = K$ em produto de fatores lineares, isto é, $f(x)$ tem todas as suas raízes em K e $f(x) = a(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_m)$ com $a, \alpha_1, \ldots, \alpha_m \in K$. Como $\varphi : K[x] \longrightarrow K'[x]$ é isomorfismo de anéis, então $\varphi(f)(x) = \varphi(a)(x - \varphi(\alpha_1)) \cdot \ldots \cdot (x - \varphi(\alpha_m))$ com $\varphi(a), \varphi(\alpha_1), \ldots, \varphi(\alpha_n) \in \varphi(K) = K'$ e $\varphi(f)(x)$ se decompõe em $K'[x]$. Logo, $L' = K'$ e $\varphi : K \longrightarrow K'$ é o isomorfismo procurado.

Suponhamos o Teorema válido para os polinômios com coeficientes em K_0, cujo corpo de decomposição L_0 sobre K_0 tenha $[L_0 : K_0] < n$. Seja $f(x)$ em $K[x]$ com corpo de decomposição L sobre K, tal que $[L : K] = n > 1$. Então, $f(x)$ tem um fator mônico irredutível $p(x) \in K[x]$ com grau$(p(x)) = r > 1$. Seja $\varphi(p)(x)$ o fator mônico irredutível de $\varphi(f)(x)$ em $K'[x]$. Como $f(x)$ se decompõe em L e $p(x)$ divide $f(x)$ em $K[x]$, então todas as raízes de $p(x)$ estão em L. Logo, existe $\alpha \in L$ tal que $p(\alpha) = 0$. Portanto,

$$[L : K(\alpha)] = \frac{[L : K]}{[K(\alpha) : K]} = \frac{n}{r} < n.$$

$$\begin{array}{c} L \\ | \\ K(\alpha) \\ | \\ K \end{array}$$

Tomando L' um corpo de raízes de $\varphi(f)(x)$ sobre K' e $\beta \in L'$ uma raiz de $\varphi(p)(x)$, então o isomorfismo $\varphi : K \longrightarrow K'$ se estende a um isomorfismo de $K(\alpha)$ em $K'(\beta)$, também denotado por φ, com $\varphi(\alpha) = \beta$.

O diagrama ao lado ilustra o raciocínio acima.

$$\begin{array}{ccc} L & & L' \\ i\uparrow & & i'\uparrow \\ K(\alpha) & \overset{\varphi}{\dashrightarrow} & K'(\beta) \\ i\uparrow & & i'\uparrow \\ K & \overset{\varphi}{\longrightarrow} & K' \end{array}$$

Afirmamos que L é um corpo de raízes de $f(x)$ sobre $K_0 = K(\alpha)$, assim como L' é um corpo de raízes de $\varphi(f)(x)$ sobre $K'(\beta)$.

De fato, $f(x) \in K[x] \subset K(\alpha)[x]$ e $f(x)$ se decompõe em L num produto de fatores lineares e não pode se decompor em um subcorpo F com $K_0 \subset F \subsetneq L$ pois, senão, L não seria corpo de raízes sobre K de $f(x)$.

Observe que $K \subset K(\alpha) = K_0 \subset F$.

Como $[L : K_0] < n$, pela hipótese de indução, $\varphi : K_0 = K(\alpha) \longrightarrow K'(\beta)$ se estende a um isomorfismo $\psi : L \longrightarrow L'$. Esse é o isomorfismo procurado.

$$\begin{array}{ccc} L & \overset{\psi}{\dashrightarrow} & L' \\ i\uparrow & & i'\uparrow \\ K(\alpha) & \xrightarrow{\varphi} & K'(\beta) \\ i\uparrow & & i'\uparrow \\ K & \xrightarrow{\varphi} & K'. \end{array}$$

O diagrama acima ilustra a hipótese de indução. ■

Exemplo 43

Todo polinômio de grau 2 com coeficientes em K se decompõe em fatores lineares em uma extensão simples de K, de grau no máximo 2 sobre K, obtida pela adjunção a K de uma de suas raízes.

De fato, digamos que $f(x) = a(x^2 + bx + c) \in K[x]$, com $a \neq 0$. Seja L uma extensão de K na qual $f(x)$ tem uma raiz α. Então, α é raiz de $x^2 + bx + c \in K[x]$ e $x^2 + bx + c = (x - \alpha)(x + b + \alpha)$ em $L[x]$.

Faça a divisão de $x^2 + bx + c$ por $x - \alpha$ e use que $\alpha^2 + b\alpha + c = 0$.

As raízes de $f(x)$ são α e $-b - \alpha$, ambas estão em $K(\alpha)$. Assim, $K(\alpha)$ é o corpo de raízes sobre K de $f(x)$. Mais ainda,

$$\alpha \in K \iff -b - \alpha \in K \iff K = K(\alpha) \iff [K(\alpha) : K] = 1$$
$$\alpha \notin K \iff -b - \alpha \notin K \iff K \subsetneq K(\alpha) \iff [K(\alpha) : K] = 2.$$

Observação: Finalizamos lembrando que um corpo K é algebricamente fechado se, e somente se, todo polinômio não-constante em $K[x]$ tem uma raiz em K. Nesse caso, mostra-se que se $f(x) \in K[x]\backslash K$, então existem $a, \alpha_1, \ldots, \alpha_n \in K$, com $a \neq 0$, tais que $f(x) = a(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$.

Para todo corpo K, existe corpo algebricamente fechado $\overline{K}$, tal que $K \subset \overline{K}$.

A demonstração da afirmação acima usa o Lema de Zorn e não será feita aqui, podendo ser vista em *Algebra*, Serge Lang, 3^{nd} edition, 1993, Addison Wesley Publishing Company. O fato é que corpos de raízes sobre K de polinômios em $K[x]\backslash K$ são construídos como subcorpos de $\overline{K}$, assim como corpos de raízes de polinômios não-constantes em $\mathbb{Q}[x]$ são construídos como subcorpos de $\mathbb{C}$.

Na Seção 4 da Parte 2, como uma aplicação da teoria apresentada, daremos uma demonstração de que $\mathbb{C}$ é corpo algebricamente fechado.

Exercícios

1. Para cada $f(x) \in K[x]$ determine L, o corpo de decomposição de $f(x)$ sobre K:

   (a) $f(x) = x^3 - 1 \in \mathbb{Q}[x]$;
   (b) $f(x) = x^4 - 1 \in \mathbb{Q}[x]$;
   (c) $f(x) = x^6 - 1 \in \mathbb{Q}[x]$;
   (d) $f(x) = x^8 - 1 \in \mathbb{Q}[x]$;
   (e) $f(x) = x^{12} - 1 \in \mathbb{Q}[x]$;
   (f) $f(x) = x^4 - 2 \in \mathbb{Q}[x]$;
   (g) $f(x) = x^4 - 2 \in \mathbb{Q}(\sqrt{2})[x]$;
   (h) $f(x) = x^4 - 4 \in \mathbb{Q}[x]$;
   (i) $f(x) = x^n - 1 \in \mathbb{Q}[x]$;
   (j) $f(x) = x^n - a \in \mathbb{Q}[x]$, $a > 0$.

2. No Exercício anterior, determine $[L : K]$:

   (a) nos oito primeiros itens;
   (b) no item (i), no caso n primo;
   (c) no item (j), no caso n e a naturais primos.

3. Sejam $f(x) \in \mathbb{Q}[x]$ e L o corpo de decomposição de $f(x)$ sobre $\mathbb{Q}$. Determine L e $[L : \mathbb{Q}]$.

   (a) $f(x) = x^7 - 1$ (b) $f(x) = x^3 - 3$
   (c) $f(x) = x^4 + 1$ (d) $f(x) = x^6 + 1$
   (e) $f(x) = x^4 - 3$ (f) $f(x) = (x^2 + 1)(x^2 - 5)$

4. Sejam $\alpha = \sqrt{2 + \sqrt{2}}$ e $L = \mathbb{Q}(\alpha)$.

   (a) Determine $p(x)$, o polinômio mínimo de α sobre $\mathbb{Q}$.
   (b) Determine todas as raízes de $p(x)$.
   (c) Determine α^{-1} e mostre que L é o corpo de decomposição de $p(x)$ sobre $\mathbb{Q}$.

5. Sejam K, L corpos e $\sigma : K \longrightarrow L$ um homomorfismo injetor. Mostre que $\sigma(1_K) = 1_L$ e $\mathrm{car}(K) = \mathrm{car}(L)$.

Observe que σ é um $\mathbb{Q}$-homomorfismo e $\sigma : L \longrightarrow \sigma(L)$ é um isomorfismo que estende $I : \mathbb{Q} \longrightarrow \mathbb{Q}$.

6. Para cada subcorpo L de $\mathbb{C}$, determine todos os homomorfismos injetores $\sigma : L \longrightarrow \mathbb{C}$ e o corpo $\sigma(L)$:

   (a) $L = \mathbb{Q}(\sqrt{2})$ (b) $L = \mathbb{Q}(\sqrt[4]{2})$ (c) $L = \mathbb{Q}(\sqrt[3]{2})$
   (d) $L = \mathbb{Q}(i, \sqrt[4]{2})$ (e) $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$, onde $\omega = \cos\frac{2\pi}{3} + i\,\mathrm{sen}\,\frac{2\pi}{3}$

7. Sejam $L|K$ e $L'|K'$ extensões isomorfas. Mostre que $[L : K] = [L' : K']$.

Extensões normais e separáveis

Veremos que o conceito de normalidade está relacionado com corpos de decomposição e a separabilidade com raízes simples de polinômios irredutíveis.

Definição 21 (Extensão normal)
Uma extensão $L|K$ é *normal* se, e somente se, cada polinômio mônico irredutível $f(x) \in K[x]$ que tem uma raiz em L tem todas as suas raízes em L.

Exemplo 44
$\mathbb{C}|\mathbb{R}$ é uma extensão normal, pois todo polinômio com coeficientes reais tem todas as suas raízes em $\mathbb{C}$.

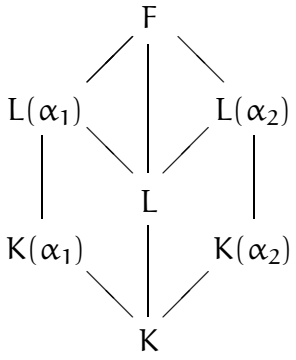
$\mathbb{C}$ é um corpo algebricamente fechado, os polinômios mônicos irredutíveis em $\mathbb{R}[x]$ são $x - a$ ou $x^2 + bx + c$, com $a, b, c \in \mathbb{R}$ e $b^2 - 4c < 0$.

Exemplo 45
$\mathbb{Q}(\sqrt[4]{2})|\mathbb{Q}$ não é normal, pois $f(x) = x^4 - 2 \in \mathbb{Q}[x]$, irredutível em $\mathbb{Q}[x]$, não tem todas as suas raízes em $\mathbb{Q}(\sqrt[4]{2})$.

Teorema 5 (Caracterização das extensões normais finitas)
Uma extensão $L|K$ é normal finita se, e somente se, L é corpo de decomposição sobre K de algum polinômio $f(x) \in K[x]\backslash K$.

Demonstração: Suponhamos que $L|K$ seja normal finita. Pelo Corolário 2 da Seção 1, existem $\alpha_1, \ldots, \alpha_n \in L$ algébricos sobre K tais que $L = K(\alpha_1, \ldots, \alpha_n)$. Sejam $p_1(x), \ldots, p_n(x) \in K[x]$ os polinômios mínimos, respectivamente, de $\alpha_1, \ldots, \alpha_n$ sobre K. Seja $f(x) = p_1(x) \cdot \ldots \cdot p_n(x) \in K[x]$. Pela normalidade de $L|K$, todas as raízes de $p_j(x)$, $j = 1, \ldots, n$, estão em L, logo $f(x)$ se decompõe em produto de fatores lineares em L. Qualquer corpo $F \supset K$ com a propriedade de $f(x)$ se decompor em produto de fatores lineares, contém $K \cup \{\alpha_1, \ldots, \alpha_n\}$. Portanto, $F \supset K(\alpha_1, \ldots, \alpha_n) = L$. Então, L é o corpo de decomposição sobre K de $f(x)$.

Reciprocamente, suponhamos que L seja corpo de decomposição sobre K de algum polinômio $f(x) \in K[x]\backslash K$. Então, $L|K$ é, claramente, uma extensão finita. Para provar a normalidade seja $p(x) \in K[x]$ um polinômio mônico irredutível que tenha uma raiz em L. Vamos mostrar que todas as raízes de $p(x)$ estão em L. Consideremos $F \supset L$ um corpo de decomposição de $f(x)p(x)$ sobre K. Sejam α_1 e α_2 raízes de $p(x)$ em F. Afirmamos que $[L(\alpha_1) : L] = [L(\alpha_2) : L]$. De fato, consideremos o seguinte diagrama de subcorpos de F



Para $j = 1, 2$ temos:

$$[L(\alpha_j) : L][L : K] = [L(\alpha_j) : K] = [L(\alpha_j) : K(\alpha_j)][K(\alpha_j) : K]. \qquad (\star)$$

$[K(\alpha_1) : K] = [K(\alpha_2) : K]$, pois $p(x)$ é o polinômio mínimo de α_1 e α_2 sobre K. É claro que $L(\alpha_j)$ é um corpo de decomposição sobre $K(\alpha_j)$ de $f(x)$. Pelo Corolário 6 da Seção 3, $K(\alpha_1)$ e $K(\alpha_2)$ são corpos isomorfos e, pelo Teorema 4 da Seção 3, $L(\alpha_1)|K(\alpha_1)$ e $L(\alpha_2)|K(\alpha_2)$ são extensões isomorfas. Portanto, $[L(\alpha_1) : K(\alpha_1)] = [L(\alpha_2) : K(\alpha_2)]$. Substituindo em $(\star)$, obtemos $[L(\alpha_1) : L] = [L(\alpha_2) : L]$, mostrando a afirmação.

Fez o Exercício 7 da Seção 3?

Agora, se $\alpha_1 \in L$, então $L(\alpha_1) = L$, que é equivalente a $[L(\alpha_1) : L] = 1$, portanto $[L(\alpha_2) : L] = 1$. Assim, $\alpha_2 \in L$. ■

Agora apresentamos a relação entre o conceito de derivada de polinômios com coeficientes em corpos e a multiplicidade das raízes.

Definição 22 (Derivada)
Seja $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$, onde K é um corpo. A *derivada* de $f(x)$ é o polinômio $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1} \in K[x]$.

Assim, a derivada é a função D definida por

$$\begin{array}{rccc} D: & K[x] & \longrightarrow & K[x] \\ & f(x) = \displaystyle\sum_{j=0}^{n} a_jx^j & \longmapsto & f'(x) = \displaystyle\sum_{j=1}^{n} ja_jx^{j-1} \end{array}$$

Proposição 11 (Propriedades da derivada)
Sejam K um corpo, $a \in K$ e $f(x), g(x) \in K[x]$. Valem as seguintes propriedades:

(i) $(f(x) + g(x))' = f'(x) + g'(x)$.

(ii) $(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x)$.

(iii) $(af(x))' = af'(x)$.

(iv) $((x-a)^m)' = m(x-a)^{m-1}$, para todo $m \geq 1$.

Demonstração: Você deve fazer a demonstração, que é uma verificação sistemática, usando as definições da derivada e das operações de adição e multiplicação de polinômios. O item (iv) deve ser feito por indução sobre $m \geq 1$, usando o item (ii). ■

Lema 1

O polinômio $f(x) \in K[x] \backslash K$ tem uma raiz múltipla (em alguma extensão L de K) se, e somente se, $f(x)$ e $f'(x)$ têm um fator comum de grau maior ou igual a 1 em $K[x]$.

Demonstração: Suponhamos que $\alpha \in L$ seja uma raiz de $f(x) \in K[x]$ com multiplicidade $m > 1$. Então, $f(x) = (x-\alpha)^m q(x)$ em $L[x]$, com $q(\alpha) \neq 0$. Assim, $f'(x) = m(x-\alpha)^{m-1}q(x) + (x-\alpha)^m q'(x)$. Avaliando em α, obtemos $f'(\alpha) = m \cdot 0 \cdot q(\alpha) + 0 \cdot q'(\alpha) = 0$. Logo, α também é raiz de $f'(x)$. Tomando $p(x) \in K[x]$, o polinômio mínimo de α sobre K, temos que $p(x)$ divide $f(x)$ e $p(x)$ divide $f'(x)$ em $K[x]$.

Na primeira parcela à direita da igualdade, usamos que $m - 1 > 0$.

Reciprocamente, suponhamos que $g(x) \in K[x]$, grau$(g(x)) \geq 1$, seja um fator comum de $f(x)$ e $f'(x)$. Seja $\alpha \in L \supset K$ uma raiz de $g(x)$. Afirmamos que $f(x) = (x-\alpha)^m q(x)$, $q(\alpha) \neq 0$ com $m > 1$.

De fato, caso contrário, $f(x) = (x-\alpha)q(x)$, com $q(\alpha) \neq 0$ e $f'(x) = q(x) + (x-\alpha)q'(x)$, então $f'(\alpha) = q(\alpha) \neq 0$, uma contradição. ■

Corolário 8

Seja $p(x) \in K[x]$ um polinômio irredutível.

(i) Se car$(K) = 0$, então todas as raízes de $p(x)$ são simples.

(ii) Se car$(K) = p$, então $p(x)$ tem raiz múltipla se, e somente se, $p(x) \in K[x^p]$.

Demonstração: Primeiramente, pelo Lema anterior, $p(x) \in K[x]$ tem raiz múltipla se, e somente se, $p(x)$ e $p'(x)$ têm um divisor comum de grau maior ou igual a 1. Como $p(x)$ é irredutível, isto é equivalente a $p(x)$ dividir $p'(x)$. Então, $p'(x) = 0$. De fato, se $p'(x) \neq 0$, então grau$(p'(x)) <$ grau$(p(x))$ e $p(x)$ não divide $p'(x)$.

Quais as condições para $p'(x) = 0$?

Seja $p(x) = \sum_{j=0}^{n} a_j x^j$. Então, $p'(x) = \sum_{j=1}^{n} j a_j x^{j-1} = 0$ se, e somente se, $j a_j = 0$, para $j = 1, \ldots, n$.

Seja car$(K) = 0$, então

$$\begin{aligned} p'(x) = 0 &\iff ja_j = 0, \text{ para todo } j = 1, \ldots, n \\ &\iff a_j = 0, \text{ para todo } j = 1, \ldots, n \\ &\iff p(x) = a_0. \end{aligned}$$

Esse caso não pode ocorrer com $p(x)$ irredutível. Portanto, se há raízes múltiplas, estamos em característica prima.

Seja $\text{car}(K) = p$, então

$$\begin{aligned} p'(x) = 0 &\iff ja_j = 0, \text{ para todo } j = 1, \ldots, n \\ &\iff a_j = 0 \text{ sempre que } p \nmid j, \text{ com } j = 1, \ldots, n \\ &\iff p(x) = \sum a_{lp} x^{lp} = \sum a_{lp} (x^p)^l \in K[x^p], \end{aligned}$$

concluindo a demonstração. ■

Definição 23 (Polinômio irredutível separável ou inseparável)
O polinômio irredutível $p(x) \in K[x]$ é dito *separável* sobre K se, e somente se, todas as suas raízes são simples. Caso contrário, o polinômio irredutível é dito *inseparável* sobre K.

O polinômio $f(x) \in K[x]$ é dito *separável* sobre K se, e somente se, os seus fatores irredutíveis em $K[x]$ são separáveis sobre K.

Exemplo 46
Os polinômios $p(x) = x^2 - 2$ e $q(x) = x^3 - 2$ são irredutíveis em $\mathbb{Q}[x]$ e separáveis sobre $\mathbb{Q}$.
O polinômio $f(x) = (x^2 + 1)(x^2 - 2)^3 \in \mathbb{Q}[x]$ é separável sobre $\mathbb{Q}$, pois seus fatores irredutíveis são separáveis.

Definição 24 (Elemento separável)
Seja $L|K$ uma extensão de corpos. Um elemento $\alpha \in L$ algébrico sobre K é dito *separável* sobre K se, e somente se, o polinômio mínimo de α sobre K é separável sobre K.

Definição 25 (Extensão separável)
Seja $L|K$ uma extensão de corpos. $L|K$ é uma *extensão separável* se, e somente se, todo elemento de L algébrico sobre K é separável sobre K. Caso contrário, $L|K$ é dita *extensão inseparável*.

Exemplo 47
$\overline{\mathbb{Q}}|\mathbb{Q}$ é uma extensão separável, assim como, toda extensão finita de $\mathbb{Q}$ é uma extensão separável, pois polinômios irredutíveis em $\mathbb{Q}[x]$ têm todas as raízes simples.

Exemplo 48
$\mathbb{R}|\mathbb{Q}$ é extensão separável.

Exemplo 49

Sejam x, y transcendentes sobre $\mathbb{Z}_p$, $K = \mathbb{Z}_p(x^p)$ e $L = \mathbb{Z}_p(x) = K(x)$ e $f(y) = y^p - x^p \in K[y]$.

Então, x é raiz de $f(y)$ de multiplicidade p, pois $f(y) = y^p - x^p = (y - x)^p$.

Reveja o Exercício 1 da Seção 1.

Observamos que $x \notin K$ e $f(y)$ é irredutível em $K[y]$ (verifique!), isto é, $f(y)$ é o polinômio mínimo de x sobre K.

A extensão $L|K$ é uma extensão inseparável, pois $x \in L$ é inseparável sobre K.

Exemplo 50

$\mathbb{Z}_p$ é um corpo de característica prima p, tal que os polinômios irredutíveis em $\mathbb{Z}_p[x]$ têm raízes simples, isto é, são separáveis.

De fato, seja $f(x) \in \mathbb{Z}_p[x]$ irredutível e suponhamos, por absurdo, que $f(x)$ tenha uma raiz múltipla. Então, pelo Corolário anterior, existe $g(x) \in \mathbb{Z}_p[x]$ tal que $f(x) = g(x^p)$.

Escrevendo $g(x) = \sum_{j=0}^{n} a_j x^j$, temos $f(x) = g(x^p) = \sum_{j=0}^{n} a_j (x^p)^j$, com $a_j \in \mathbb{Z}_p$.

Pelo Teorema de Fermat, $a_j^p = a_j$, para todo j, logo

$$\begin{aligned} f(x) = g(x^p) &= \sum_{j=0}^{n} a_j (x^p)^j \\ &= \sum_{j=0}^{n} a_j{}^p (x^j)^p \\ &= \sum_{j=0}^{n} (a_j x^j)^p \\ &= \left(\sum_{j=0}^{n} a_j x^j \right)^p \\ &= (g(x))^p, \end{aligned}$$

Reveja o Exercício 1 da Seção 1.

então, $f(x)$ é redutível em $\mathbb{Z}_p[x]$, uma contradição.

Assim, se $L|\mathbb{Z}_p$ é extensão finita, então $L|\mathbb{Z}_p$ é uma extensão separável.

A teoria das extensões de corpos de característica prima, onde polinômios irredutíveis podem ter raízes múltiplas, é mais sofisticada e não será feita aqui.

Daqui por diante, consideraremos nos Exemplos apenas corpos de característica zero ou extensões finitas de $\mathbb{Z}_p$.

Nos corpos de característica zero toda extensão finita é simples, conforme conseqüência do próximo Teorema.

Teorema 6
Seja $car(K) = 0$. Se α e β são algébricos sobre K, então existe $\gamma \in K(\alpha, \beta)$, tal que $K(\alpha, \beta) = K(\gamma)$.

Demonstração: Sejam $f(x)$ e $g(x)$ em $K[x]$, respectivamente, os polinômios mínimos de α e β sobre K, com $grau(f(x)) = n$ e $grau(g(x)) = m$. Seja $L \supset K(\alpha, \beta)$ um corpo de decomposição sobre K de $f(x) \cdot g(x)$. Então, $f(x)$ e $g(x)$ se decompõem em produto de fatores lineares em $L[x]$, sendo as raízes de $f(x)$ distintas, assim como as raízes de $g(x)$. Digamos que $\alpha = \alpha_1, \ldots, \alpha_n$ e $\beta = \beta_1, \ldots, \beta_m$ são as raízes em L de $f(x)$ e $g(x)$, respectivamente. Consideremos a equação

Aqui usamos que $car(K) = 0$.

$$\alpha_i + x\beta_j = \alpha + x\beta,$$

com $j \neq 1$ e $x \in L$.

Essa equação tem uma única solução em L, a saber,

$$x = \frac{\alpha_i - \alpha}{\beta - \beta_j},$$

para cada $i = 1, \ldots, n$ e $j = 2, \ldots, m$.

Como $car(K) = 0$, temos que K é infinito, logo existe $c \in K$ tal que $c \neq \dfrac{\alpha_i - \alpha}{\beta - \beta_j}$, para todo $i = 1, \ldots, n$ e $j = 2, \ldots, m$. Tomamos $\gamma = \alpha + c\beta$.

Lembre que ...
O corpo primo de K é isomorfo a $\mathbb{Q}$.

Afirmamos que $K(\alpha, \beta) = K(\gamma)$.

De fato, como $\gamma = \alpha + c\beta \in K(\alpha, \beta)$, então $K(\gamma) \subset K(\alpha, \beta)$.

Mostraremos agora que α e β estão em $K(\gamma)$. Temos $\alpha = \gamma - c\beta$. Consideremos $h(x) = f(\gamma - cx) \in K(\gamma)[x] \subset L[x]$. Então,

$$h(\beta) = f(\gamma - c\beta) = f(\alpha) = 0.$$

Como $g(\beta) = 0$ e $g(x) \in K[x] \subset K(\gamma)[x]$, então $g(x)$ e $h(x)$ têm fator comum $x - \beta$, em alguma extensão de $K(\gamma)$. Afirmamos que $x - \beta$ é o máximo divisor comum de $h(x)$ e $g(x)$ em $K(\gamma)[x]$. De fato, se $\beta_j \neq \beta$ é outra raiz de $g(x)$, então $\gamma - c\beta_j \neq \alpha_i$,

$$h(\beta_j) = f(\gamma - c\beta_j) \neq 0.$$

Além disso, $(x-\beta)^2 \nmid g(x)$. Logo, $\mathrm{mdc}_{F[x]}(g(x), h(x)) = x-\beta$, onde F é alguma extensão de $K(\gamma)$. Isto significa que $\mathrm{mdc}_{K(\gamma)[x]}(g(x), h(x)) \neq 1$ e tem que ser um divisor de $x-\beta$. Logo, esse mdc é $x-\beta$, isto é, $x-\beta \in K(\gamma)[x]$, logo $\beta \in K(\gamma)$. Portanto, $\alpha = \gamma - c\beta \in K(\gamma)$, daí segue que $K(\alpha,\beta) \subset K(\gamma)$, concluindo a demonstração da afirmação. ■

Corolário 9 (Teorema do elemento primitivo)
Seja $L|K$ uma extensão finita, com $\mathrm{car}(K) = 0$. Então, $L = K(\alpha)$, para algum $\alpha \in L$.

Demonstração: Seja $L|K$ uma extensão finita. Pelo Corolário 2 da Seção 1, existem $\alpha_1, \ldots, \alpha_n$ em L, algébricos sobre K, tais que $L = K(\alpha_1, \ldots, \alpha_n)$.

A demonstração é por indução sobre n, o número de geradores algébricos de L sobre K.

Se $n = 1$, nada há a demonstrar. Suponhamos o resultado válido para os corpos gerados sobre K por n elementos algébricos, onde $n \geq 1$. Seja $L = K(\alpha_1, \ldots, \alpha_n, \alpha_{n+1})$, com α_j algébrico sobre K. Escrevemos $L = F(\alpha_{n+1})$, onde $F = K(\alpha_1, \ldots, \alpha_n)$. Então, por hipótese de indução, existe $\gamma \in F$ tal que $F = K(\gamma)$. Então,

$$L = K(\alpha_1, \ldots, \alpha_{n+1}) = F(\alpha_{n+1}) = K(\gamma)(\alpha_{n+1}) = K(\gamma, \alpha_{n+1}).$$

$$\begin{array}{c} L = F(\alpha_{n+1}) = K(\gamma)(\alpha_{n+1}) \\ | \\ F = K(\alpha_1, \ldots, \alpha_n) = K(\gamma) \\ | \\ K \end{array}$$

Pelo Teorema anterior, existe $\alpha \in L$ tal que $L = K(\gamma, \alpha_{n+1}) = K(\alpha)$. ■

Exercícios

1. Determine quais das seguintes extensões de corpos são normais:
   (a) $\mathbb{Q}(i, \sqrt{5}) \mid \mathbb{Q}$
   (b) $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$
   (c) $\mathbb{Q}(\sqrt{2}, \sqrt{5}) \mid \mathbb{Q}$
   (d) $\mathbb{Q}(\sqrt[4]{2}) \mid \mathbb{Q}(\sqrt{2})$
   (e) $\mathbb{Q}(\sqrt[4]{2}, i) \mid \mathbb{Q}$.
2. Seja $L|K$ uma extensão de grau 2, com $\mathrm{car}(K) \neq 2$.
   (a) Mostre que existe $\alpha \in L$ tal que $L = K(\alpha)$ e $\alpha^2 \in K$.
   (b) Mostre que $L|K$ é uma extensão normal e separável.

3. Seja $L|K$ uma extensão de corpos e seja F um corpo intermediário, isto é, $K \subset F \subset L$. Mostre que:

   (a) $L|K$ é extensão algébrica se, e somente se, $F|K$ e $L|F$ são extensões algébricas.

   Vale a recíproca no item (b).

   (b) Se $L|K$ é extensão separável, então $F|K$ e $L|F$ são extensões separáveis.

   (c) Se $L|K$ é extensão normal, então $L|F$ é extensão normal.

4. Dê exemplo de corpos $K \subset F \subset L$, tais que $L|K$ é extensão finita normal e a extensão $F|K$ não é normal.

5. Determine $\alpha \in L$ tal que $L = K(\alpha)$:

   (a) $L = \mathbb{Q}(i, \sqrt{5})$ e $K = \mathbb{Q}$.

   (b) $L = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ e $K = \mathbb{Q}$.

   (c) $L = \mathbb{Q}(\sqrt[4]{2})$ e $K = \mathbb{Q}(\sqrt{2})$.

   (d) L é o corpo de raízes sobre $\mathbb{Q}$ de $x^6 - 1$ e $K = \mathbb{Q}$.

6. Sejam p um natural primo e $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$.

   (a) Mostre que $f(x)$ tem todas as raízes simples.

   (b) Seja L um corpo de raízes de $f(x)$ sobre $\mathbb{Z}_p$.
   Seja $F = \{\alpha \in L \,;\, f(\alpha) = 0\}$.
   Mostre que se $\alpha, \beta \in F$, então $\alpha - \beta$, $\alpha \cdot \beta$ e β^{-1}, com $\beta \neq 0$, estão em F. Conclua que F é um corpo e $F = L$.

   (c) Mostre que $[F : \mathbb{Z}_p] = n$.

   (d) Conclua que L é um corpo com p^n elementos.

7. Seja $\mathbb{F}$ um corpo finito.

   (a) Mostre que $\mathrm{car}(\mathbb{F}) = p$, para algum primo p.

   (b) Seja $\mathbb{F}_p = \{0_{\mathbb{F}}, 1_{\mathbb{F}}, \ldots, (p-1)1_{\mathbb{F}}\}$ o corpo primo de $\mathbb{F}$. Mostre que $[\mathbb{F} : \mathbb{F}_p] = n$, para algum natural $n \geq 1$, e $| \mathbb{F} | = p^n$.

   (c) Mostre que para todo $\alpha \in \mathbb{F}$, tal que $\alpha \neq 0$, temos $\alpha^{p^n - 1} = 1_{\mathbb{F}}$.

   (d) Mostre que $\mathbb{F}$ é um corpo de raízes de $x^{p^n} - x$ sobre $\mathbb{F}_p$.