AULA

Extensões de Corpos

7

META:

Determinar as noções e fatos básicos da teoria dos corpos.

OBJETIVOS:

Ao final da aula o aluno deverá ser capaz de:

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

Determinar a característica de um corpo.

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

Determinar uma base vetorial de uma extensão algébrica simples.

Determinar as operações adição e multiplicação para extensão algébricas simples.

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

PRÉ-REQUISITOS

Observação 6.1 e seção 6.4 da aula 6.

7.1 Introdução

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

7.2 Glossário

Ao longo desta seção, F denotará um corpo.

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

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

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

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

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

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

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

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

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

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

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

Elemento transcendente Elemento não algébrico.

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

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

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

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

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

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

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

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

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

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

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

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

7.3 Exemplos

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

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

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

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

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

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

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

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

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

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

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

   Multiplicação:

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

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

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

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

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

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

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

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

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

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

   (a) Elemento genérico:

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

(b) Operações:

Adição:

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

Multiplicação:

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

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

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

com

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

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

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

(d) Inverso multiplicativo:

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

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

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

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

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

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

   (a) Elemento genérico:

   $$a + b\alpha$$

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

   (b) Operações:

   Adição:

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

   Multiplicação:

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

   (c) Inverso multiplicativo:

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

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

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

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

(a) Elemento genérico:

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

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

(b) Operações:

Adição:

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

Multiplicação:

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

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

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

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

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

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

7.4 Fatos

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

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

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

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

   (b) Suponha K uma extensão de F contendo uma raiz α de $p(x)$. Seja $F(\alpha)$ o subcorpo de K gerado por F e α. Então,
   $$F(\alpha) \cong F[x]/(p(x)).$$
   Em particular, $F(\alpha) = F[\alpha]$.

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

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

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

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

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

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

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

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

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

7.5 Exercícios Resolvidos

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

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

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

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

   uma base de L sobre K e seja

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

   uma base de K sobre F. Considere o conjunto

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

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

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

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

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

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

Substituindo as igualdades acima na igualdade 7.7 obtemos

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

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

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

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

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

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

donde

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   Efetuando as operações na equação acima obtemos

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

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

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

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

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

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

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

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

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

Solução:

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

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

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

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

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

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

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

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

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

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

   Solução:

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

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

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

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

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

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

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

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

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

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

    Solução:

    i) Segue da implicação (iii) $\Rightarrow$ (i) no fato 4.

    ii) Foi provado na observação 6.1 da aula 6.

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

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

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

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

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

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

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

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

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

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

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

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

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

7.6 Conclusão

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

RESUMO

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

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

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

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

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

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

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

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

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

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

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

PRÓXIMA AULA

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

ATIVIDADES

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

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

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

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

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

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

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

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

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

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

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

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

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

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

LEITURA COMPLEMENTAR

GONÇALVES, Adilson, Introdução à álgebra, IMPA, Projeto Euclides, 5.ed., Rio de Janeiro, 2008.
HUNGERFORD, Thomas W., Abstract algebra: an introduction, Saunders College Publishing, 1990.