Capítulo 4

RAÍZES DE POLINÔMIOS

No capítulo anterior, discutimos elementos em uma dada extensão K de F que eram algébricos sobre F, isto é, elementos que satisfaziam polinômios em $F[x]$. Agora inverteremos o problema; dado um polinômio $p(x)$ em $F[x]$, queremos encontrar um corpo K, que seja uma extensão de F, no qual $p(x)$ tem uma raiz.

Definição 4.1: Se $p(x) \in F[x]$, então um elemento a, que esteja em alguma extensão do corpo F, é denominado uma *raiz* de $p(x)$ se $p(a) = 0$.

Exemplo 4.1: Dado $f(x) = x^2 - 2$, $f(x) \in \mathbb{Q}[x]$, $a = \sqrt{2} \in \mathbb{R}$ é uma raiz de $f(x)$, pois $f(\sqrt{2}) = 0$.

Teorema 4.1(Teorema do Resto): Se $p(x) \in F[x]$ e K é uma extensão de F, então $p(x) = (x - b)q(x) + p(b)$, para todo elemento $b \in K$, onde $q(x) \in K[x]$ e $gr[q(x)] = gr[p(x)] - 1$.

Demonstração: Como $F \subset K$, $F[x]$ está contido em $K[x]$, donde podemos considerar que $p(x)$ está em $K[x]$. Pelo algorítimo da divisão para polinômios em $K[x]$, $p(x) = (x - b)q(x) + r$, onde $q(x) \in K[x]$ e $r = 0$ ou $gr[r] < gr[(x - b)] = 1$.

Assim, $r = 0$ ou $gr[r] = 0$. Em qualquer caso, r é um elemento de K. Como $p(x) = (x - b)q(x) + r$, $p(b) = (b - b)q(b) + r = r$. Portanto, $p(x) = (x - b)q(x) + p(b)$.

Como $p(x) = (x - b)q(x) + r$ temos:

$gr[p(x)] = gr[(x - b)] + gr[q(x)] \Rightarrow gr[p(x)] = 1 + gr[q(x)] \Rightarrow gr[q(x)] = gr[p(x)] -$

Corolário 4.1.1: Se $a \in K$ é uma raiz de $p(x) \in F[x]$, onde $F \subset K$, então $(x - a) \mid p(x)$ em $K[x]$.

Demonstração: Do Teorema do resto, em $K[x]$, $p(x) = (x - a)q(x) + p(a) = (x - a)q(x)$ pois, $p(a) = 0$. Assim, $(x - a) \mid p(x)$ *em* $K[x]$. ■

Exemplo 4.2: Dado $f(x) = x^2 - 2$ em $\mathbb{Q}[x]$, vemos que $(x - \sqrt{2}) \mid f(x)$.

Definição 4.2.: O elemento $a \in K$ é uma *raiz* de $p(x) \in F[x]$ *de multiplicidade m* se $(x - a)^m | p(x)$, enquanto que $(x - a)^{m+1} \nmid p(x)$.

Neste momento é importante estabelecermos quantas raízes um polinômio possui num dado corpo. Sendo assim, se α é uma raiz de multiplicidade m de $p(x)$ então em $p(x)$ existem m raízes iguais a α.

Exemplo 4.3: Seja $p(x) = x^3 + 3x^2 - 4$.

$a = -2$ é uma raiz de multiplicidade 2, pois $p(a) = 0$ e $(x + 2)^2 \mid p(x)$, mas $(x + 2)^3 \nmid p(x)$.

Proposição 4.1.: Um polinômio de grau n sobre um corpo pode ter no máximo n raízes em qualquer extensão deste corpo.

Demonstração: Será feita por indução sobre n, o grau do polinômio $p(x)$. Se $p(x)$ é de

grau 1, então ele é da forma $\alpha x + \beta$, onde α, β estão num corpo F e $\alpha \neq 0$. Todo a tal que $p(a) = 0$ implica que $\alpha a + \beta = 0$, donde concluímos que $a = -\beta/\alpha$. Isto é, $p(x)$ possui uma única raiz $-\beta/\alpha$. Logo, a conclusão da Proposição certamente vale neste caso.

Admitindo que o resultado seja verdadeiro em qualquer corpo e para todos os polinômios de graus menores que n, suponhamos que $p(x)$ seja de grau n sobre F. Seja K uma extensão qualquer de F. Se $p(x)$ não possui raízes em K, então certamente a proposição está demonstrado, pois o número de raízes em K, a saber zero, é decididamente menor ou igual a n. Portanto, suponhamos que $p(x)$ possua pelo menos uma raiz $a \in K$ e que a seja uma raiz de multiplicidade m. Como $(x-a)^m | p(x)$, segue que $m \leq n$. Ora, $p(x) = (x-a)^m q(x)$, onde $q(x) \in K[x]$ é de grau $n-m$. Do fato que $(x-a)^{m+1} \nmid p(x)$ obtemos $(x-a) \nmid q(x)$, donde, pelo Corolário do Teorema do resto, a não é raiz de $q(x)$. Se $b \neq a$ é uma raiz em K de $p(x)$, então $0 = p(b) = (b-a)^m q(b)$; mas, como $b - a \neq 0$ e como estamos num corpo, concluimos que $q(b) = 0$. Isto é, qualquer raiz de $p(x)$, em K, diferente de a é necessariamente uma raiz de $q(x)$. Como $q(x)$ é de grau $n - m < n$, pela nossa hipótese de indução, $q(x)$ tem no máximo $n - m$ raízes em K, o que, junto com a outra raiz a contada m vezes, nos diz que $p(x)$ tem no máximo $m + (n - m) = n$ raízes em K. ■

Exemplo 4.4: Seja $p(x) = x^4 - 1 \in \mathbb{Q}[x]$. $\mathbb{R}$ é uma extensão de $\mathbb{Q}$ e, em $\mathbb{R}$ $p(x)$, tem duas raízes, a saber ± 1. Mas, em $\mathbb{C}$, outra extensão de $\mathbb{Q}$, $p(x)$ tem 4 raízes que são, $\pm 1, \pm i$.

Proposição 4.2.: Sejam $E = F[x]/V$, $V = (p(x))$, uma extensão de F de grau $n = gr[p(x)]$ e $p(x)$ um polinômio irredutível sobre F, então os elementos

$$1 + V,\ x + V,\ (x+V)^2 = x^2 + V\ ,\ldots,\ (x+V)^{n-1} = x^{n-1} + V$$

forma uma base de E sobre F.

Demonstração: Temos que $E = F[x] / (p(x)) = \{f(x) + V \mid f(x) \in F[x]\}$ $= \{q(x)p(x) + r(x) + V \mid q(x), r(x) \in F[x]\} = \{r(x) + V \mid r(x) \in F[x],\ gr[r(x)]$ $= \{a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + V \mid a_i \in F\}\}$.

Dessa forma, E é um corpo formado por todos os elementos da forma $a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + V$ Tal que $a_i \in F$.

Seja $e \in E$ qualquer,

então $e = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + V = (a_0 + V) + (a_1 x + V)$ $+ \ldots + (a_{n-1}x^{n-1} + V) = a_0(1+V) + a_1(x+V) + \ldots + a_{n-1}(x^{n-1} + V)$. Logo, $1 + V, x + V$, $x^{n-1} + V$ geram E.

Por outro lado, como $a + V = b + V \Leftrightarrow -b + a \in V$, então:

$a_0(1+V) + a_1(x+V) + \ldots + a_{n-1}(x^{n-1} + V) = V \quad \Leftrightarrow \quad a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + V = V = 0 +$

$\Leftrightarrow a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} \in V$, ou seja, $a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ é um múltiplo de $p(x)$. Como o grau de $p(x) = n$, teremos que $a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} = 0 \Leftrightarrow a_0 = a_1 = \ldots = a_{n-1} = 0$. Sendo assim, $1 + V, x + V, \ldots, x^{n-1} + V$ são LI. Logo, $1 + V, x + V, \ldots, x^{n-1} + V$ é uma base de E sobre F. ■

Teorema 4.2.: Se $p(x)$ é um polinômio em $F[x]$, de grau $n \geq 1$, e é irredutível sobre F, então existe uma extensão E de F, tal que $[E : F] = n$, na qual $p(x)$ tem uma raiz.

Demonstração: Seja $F[x]$ o anel dos polinômios em x sobre F e seja $V = (p(x))$ o ideal de $F[x]$ gerado por $p(x)$. V é um ideal maximal de $F[x]$, donde $E = F[x]/V$ é um corpo.

Primeiramente, queremos mostrar que E é uma extensão de F, na verdade, não é! Mas seja $\overline{F}$ a imagem de F em E, isto é, $\overline{F} = \{\alpha + V \mid \alpha \in F\}$. Afirmamos que $\overline{F}$ é um corpo isomorfo a F; de fato, se ψ é a aplicação de $F[x]$ em $F[x]/V = E$ definida por $\psi[f(x)] = f(x) + V$, então a restrição de ψ a F induz um isomorfismo de F em $\overline{F}$. Usando este isomorfismo identificamos F e $\overline{F}$; desta maneira podemos considerar E como uma extensão de F.

Por conveniência de notação indiquemos o elemento $\psi(x) = x + V$, no corpo E, por a. Dado $f(x) \in F[x]$, afirmamos que $\psi(f(x)) = f(a)$, pois como ψ é um homomorfismo, se $f(x) = \beta_0 + \beta_1 x + \ldots + \beta_k x^k$, então
$\psi[f(x)] = \psi[\beta_0 + \beta_1 x + \ldots + \beta_k x^k] = \psi(\beta_0) + \psi(\beta_1)\psi(x)$
$+\ldots+\psi(\beta_k)\psi(x^k)$, e $\psi(x^i) = \psi(x)\ \psi(x)\ \ldots\ \psi(x)$, i vezes. Como $\beta_i \in F$ temos $\psi(\beta_i) = \beta_i$, pois ψ é um isomorfismo de F em $\overline{F}$. Vemos que $\psi(f(x)) = f(a)$. Em particular, como $p(x) \in V$, $\psi(p(x)) = 0$; contudo, $\psi(p(x)) = p(a)$. Assim, o elemento $a = \psi(x)$ em E é uma raiz de $p(x)$ e, pela Proposição 4.2, concluímos que $[E : F] = n$.■

Corolário 4.2.1: Se $f(x) \in F[x]$, então existe uma extensão finita E de F na qual $f(x)$ tem uma raiz. Além disso, $[E : F] \leq gr[f(x)]$.

Demonstração: Pela Proposição 4.2, temos que $[E : F] = gr[p(x)]$, onde $p(x)$ é irredutível sobre F. Basta considerar $p(x)$ sendo um fator irredutível de $f(x)$ e aplicar o Teorema anterior para obter que $[E : F] \leq gr[f(x)]$. A igualdade ocorre se $f(x)$ for irredutível.■

Definição 4.3: Se $f(x) \in F[x]$, uma extensão finita E de F é dita um *corpo de raízes sobre F para* $f(x)$ (ou corpo de decomposição de $f(x)$) se $f(x)$ pode ser fatorado como um produto de fatores lineares sobre E (isto é, em $E[x]$) mas não sobre subcorpos próprios de E.

Teorema 4.3: Seja $f(x) \in F[x]$ de grau $n \geq 1$. Então, existe uma extensão E de F, de grau no máximo $n!$, na qual $f(x)$ possui n raízes (e, portanto, um complemento completo de raízes).

Demonstração: Pelo Corolário 4.2.1, existe uma extensão E_0 de F com $[E_0 : F] \leq n$ na qual $f(x)$ possui uma raiz α. Assim, em $E_0[x]$, $f(x)$ pode ser fatorado como $f(x) = (x - \alpha)q(x)$, onde $q(x)$ é de grau $n - 1$. Continuando este processo, vemos que existe uma extensão E de E_0, de grau no máximo $(n - 1)!$, na qual $q(x)$ possui $n - 1$ raízes. Como toda raiz de $f(x)$ é α ou uma raiz de $q(x)$, obtemos em E todas as n raízes de $f(x)$; e ainda.
$[E : F] = [E : E_0] \cdot [E_0 : F] \leq (n - 1)!n = n!$.■

Exemplo 4.5: Seja F um corpo e seja $p(x) = x^2 + \alpha x + \beta$, $\alpha, \beta \in F$, *em* $F[x]$.

Vamos mostrar que se K é uma extensão qualquer de F, na qual $p(x)$ tem uma raiz a, então o elemento $b = -\alpha - a$ também em K é uma raiz de $p(x)$. De fato, se a é raiz de $p(x)$, então $p(a) = a^2 + \alpha a + \beta = 0$. Assim
$p(b) = (-\alpha - a)^2 + \alpha(-\alpha - a) + \beta = \alpha^2 + 2\alpha a + a^2 - \alpha^2$
$-\alpha a + \beta = a^2 + \alpha a + \beta = 0$, portanto, $(-\alpha - a)$ é raiz de $p(x)$.

Se $b = a$, $p(x)$ é necessariamente, igual a $(x - a)^2$. Isto é,
$b = -\alpha - a \Rightarrow -\alpha = a + a \Rightarrow \alpha = -2a.a^2 + \alpha a + \beta = 0 \Rightarrow \beta = -a^2 - \alpha a = a(-\alpha - a) = ab$
$\Rightarrow \beta = a^2$; e assim $p(x) = x^2 - 2ax + a^2 = (x - a)^2$. Dessa forma as *duas* raízes de $p(x)$ estão em K.

Se $b \neq a$, então as *duas* raízes de $p(x)$ também estão em K, pois $a, b \in K$. Portanto, K é uma extensão de F onde $p(x)$ se decompõe em fatores lineares e $[K : F] \leq 2 = 2!$

O Teorema anterior afirma a existência de uma extensão finita E na qual o polinômio dado $f(x)$, de grau n sobre F, tem n raízes. Se
$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $a_n \neq 0$, então $f(x) = a_n(x^n + \frac{a_{n-1}x^{n-1}}{a_n} + \ldots + \frac{a_0}{a_n})$; e se as n raízes em E são $\alpha_1, \ldots, \alpha_n$, usando o Corolário 4.1.1, $f(x)$ pode ser fatorado sobre E como $f(x) = a_n(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$. Assim $f(x)$ decompõe-se completamente sobre E como

um produto de fatores *lineares*.

Exemplo 4.6: Seja $F = \mathbb{Q}$. $F(\omega)$ é o corpo de raízes de $f(x) = x^4 + x^2 + 1$, formado pela adjunção da raís ω, onde $\omega = \frac{(-1+\sqrt{3}\,i)}{2}$.

Para mostrar isto devemos fatorar $f(x)$ como um produto de fatores lineares. Para isso, faça em $f(x)$, $x^2 = t$, $x = a + bi$, isto implica que $f(t) = t^2 + t + 1$; logo:

$t_1 = \frac{(-1+\sqrt{3}\,i)}{2}$ *e* $t_2 = \frac{(-1-\sqrt{3}\,i)}{2}$ são raízes de $f(t)$. De fato:

$$f(t_1) = \left(\frac{(-1+\sqrt{3}\,i)}{2}\right)^2 + \frac{(-1+\sqrt{3}\,i)}{2} + 1 = \frac{-1-\sqrt{3}\,i}{2} + \frac{-1+\sqrt{3}\,i}{2} + 1 = 0.$$

$$f(t_2) = \left(\frac{(-1-\sqrt{3}\,i)}{2}\right)^2 + \frac{(-1-\sqrt{3}\,i)}{2} + 1 = \frac{-1+\sqrt{3}\,i}{2} + \frac{-1-\sqrt{3}\,i}{2} + 1 = 0.$$

Assim, como $(a+bi)^2 = \frac{(-1-\sqrt{3}\,i)}{2}$, temos que:

$$\begin{cases} (a^2 - b^2) + 2abi = \frac{-1+\sqrt{3}\,i}{2} \\ a^2 - b^2 = -\frac{1}{2} \end{cases} \Rightarrow \begin{cases} a = \frac{1}{2} \\ b = -\frac{\sqrt{3}}{2} \end{cases} ; \quad \begin{cases} a = -\frac{1}{2} \\ b = \frac{\sqrt{3}}{2} \end{cases}$$

Dessa forma, vemos que $\frac{1-\sqrt{3}\,i}{2}$, $\frac{1+\sqrt{3}\,i}{2}$, $\frac{-1+\sqrt{3}\,i}{2}$, $\frac{-1-\sqrt{3}\,i}{2}$ são as quatro raízes de $f(x)$.

Portanto,

$$f(x) = x^4 + x^2 + 1 = \left(x - \frac{1-\sqrt{3}\,i}{2}\right)\left(x - \frac{1+\sqrt{3}\,i}{2}\right)\left(x - \frac{-1+\sqrt{3}\,i}{2}\right)\left(x - \frac{-1-\sqrt{3}\,i}{2}\right).$$

Exemplo 4.7: Seja F o corpo dos números racionais e seja $f(x) = x^3 - 2$. No corpo dos números complexos as três raízes de $f(x)$ são $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ e $\omega^2\sqrt[3]{2}$, onde $\omega = \frac{-1+\sqrt{3}\,i}{2}$ e $\sqrt[3]{2}$ é raiz cúbica real de 2. Não podemos decompor $x^3 - 2$ em $F(\sqrt[3]{2})$, pois como um subcorpo do corpo dos reais, ele não pode conter o número complexo, $\omega\sqrt[3]{2}$. Pelo Teorema 4.3.$[E : F] \leq 3! = 6$, onde E é o corpo de raízes de $x^3 - 2$ sobre F; pela observação acima, como $x^3 - 2$ é irredutível sobre F e como $[F(\sqrt[3]{2}) : F] = 3$, pelo Corolário 4.1.1, $3 = [F(\sqrt[3]{2}) : F] \mid [E : F]$. Finalmente, $[E : F] > [F(\sqrt[3]{2}) : F] = 3$. Logo a única possibilidade é $[E : F] = 6$.

Os três exemplos ilustram o que afirma o Teorema 4.3, pois nem todos polinômios precisam de uma extensão máxima, ou seja, que tenha grau n!.