6. Extensão Separável (Parte I)

Nosso interesse nesta seção será entender quando um polinômio irredutível possui raízes múltiplas em algum corpo algebricamente fechado. Veremos que tal situação é possível somente em característica positiva.

Definição 6.1. Sejam $\mathbb{F}$ um corpo, $f \in \mathbb{F}[X]$, Ω um corpo algebricamente fechado contendo $\mathbb{F}$, e $a \in \Omega$, com $f(a) = 0$. Dizemos que a *multiplicidade* da raiz a de f é m se $(X-a)^m$ divide f, mas $(X-a)^{m+1}$ não divide f. Se a multiplicidade de uma raiz a é 1, então dizemos que a é uma raiz *simples*. Caso contrário, dizemos que a é uma raiz *múltipla*.

Definição 6.2. Um polinômio f é dito ser *separável* se todas as suas raízes (em algum corpo algebricamente fechado) são simples.

Uma ferramenta prática para estudarmos a multiplicidade de uma raiz é dada pela derivada formal, definida a seguir. Sejam $\mathbb{F}$ um corpo e $f \in \mathbb{F}[X]$. Escreva $f = \alpha_0 + \alpha_1 X + \cdots + \alpha_m X^m$. A *derivada formal* de f, denotada por f', é, por definição

$$f'(X) = \alpha_1 + 2\alpha_2 X + \cdots + m\alpha_m X^{m-1} = \sum_{i=0}^{m-1} (i+1)\alpha_{i+1} X^i.$$

A propriedade de Leibniz vale para a derivada formal, isto é, se $f, g \in \mathbb{F}[X]$, então

$$(fg)' = f'g + fg'.$$

Outra propriedade interessante é a regra da cadeia:

$$(f(g(X)))' = f'(g(X))g'(X).$$

A verificação de ambas propriedades fica de exercício. Por fim, temos o seguinte, cuja demonstração fica de exercício:

Lema 6.3. *$f' = 0$ se, e somente se, vale um dos seguintes itens:*

(1) *ou* $\operatorname{car}\mathbb{F} = 0$ *e* $f \in \mathbb{F}$,
(2) *ou* $\operatorname{car}\mathbb{F} = p > 0$ *e* $f = g(X^p)$*, para algum* $g \in \mathbb{F}[X]$ *(ou seja,* $f \in \mathbb{F}[X^p]$*).*

Agora, assuma que $a \in \Omega$ é uma raiz de f. Então $f = (X-a)^m g$, para algum $g \in \Omega[X]$, em que $g(a) \neq 0$, e $m \geq 1$. Então

$$f' = m(X-a)^{m-1} g + (X-a)^m g'.$$

Assumindo, em princípio, que $m > 1$, temos então que $f'(a) = 0$. Por outro lado, se $m = 1$, então $f'(a) = (a-a)g' + g(a) = g(a) \neq 0$. Portanto, acabamos de provar o seguinte critério:

Proposição 6.4. *Seja $a \in \Omega$ uma raiz de $f \in \mathbb{F}[X]$. Então a é raiz múltipla de f se, e somente se, $f'(a) = 0$.* □

De um modo a não se prender a um único elemento $a \in \Omega$, temos o seguinte resultado:

Teorema 6.5. *Seja $f \in \mathbb{F}[X]$. Então f é separável se, e só se,* $\operatorname{mdc}(f, f') = 1$.

Demonstração. Se f não é separável, então $f = (X-a)^2 g$, para algum $g \in \mathbb{F}[X]$. Daí $f' = (X-a)((X-a)g' + 2g)$. Portanto, $\mathrm{mdc}(f, f') \neq 1$. Reciprocamente, assuma que $g(X) := \mathrm{mdc}(f, f') \neq 1$. Então, existe $a \in \Omega$ raiz de g. Daí, $f(a) = f'(a) = 0$. Da Proposição 6.4, segue que a é raiz múltipla da f. Conclui-se que f não é separável. □

Note que o critério $\mathrm{mdc}(f, f') = 1$ pode ser enunciado de forma independente da existência de um corpo maior Ω.

No caso especial em que o polinômio é assumido ser irredutível, obtemos um critério mais simples:

Teorema 6.6. *Seja $f \in \mathbb{F}[X]$ irredutível. Então f é separável se, e somente se, $f' \neq 0$.*

Assim, se f é irredutível e vale um entre (i) ou $\mathrm{car}\,\mathbb{F} = 0$, (ii) ou $\mathrm{car}\,\mathbb{F} = p > 0$ e $f \notin \mathbb{F}[X^p]$, então f é separável.

Demonstração. Assuma que $f' = 0$. Então $\mathrm{mdc}(f, f') \neq 1$. Portanto, do Teorema 6.5, segue que f não é separável. Reciprocamente, assuma que f não é separável. Seja $a \in \Omega$ uma raiz múltipla de f. Então, da Proposição 6.4, segue que $f'(a) = 0$. Isso implica que $f' \in (f)$ (ideal gerado por f em $\mathbb{F}[X]$). Como $\mathrm{gr}(f') < \mathrm{gr}(f)$, segue que $f' = 0$.

A última afirmação do enunciado é válida devido a caracterização de quando $f' = 0$ (Lema 6.3). □

O próximo resultado nos mostra uma caracterização de polinômios irredutíveis que não são separáveis:

Teorema 6.7. *Sejam $\mathbb{F}$ um corpo de característica $p > 0$, e $f \in \mathbb{F}[X]$ irredutível. Então existem $m \geq 0$ e um polinômio irredutível e separável $g \in \mathbb{F}[X]$ tal que $f = g(X^{p^m})$.*

Demonstração. Se f é um polinômio separável, então a conclusão é válida se tomarmos $g = f$ e $m = 0$. Se f não é separável, então, do Teorema 6.6, $f' = 0$. Portanto, do Lema 6.3, $f = g(X^p)$, para algum $g \in \mathbb{F}[X]$. Se $g = g_1 g_2$, então $f = g_1(X^p)g_2(X^p)$. Portanto, como f é irredutível, segue que g é irredutível. Por indução no grau do polinômio, vale que g é separável, ou $g = h(X^{p^m})$, para algum $h \in \mathbb{F}[X]$ irredutível e separável. Portanto, $f = h(X^{p^{m+1}})$. □

Como consequência, obtemos a seguinte propriedade:

Corolário 6.8. *Seja $\mathbb{F}$ um corpo e $f \in \mathbb{F}[X]$ um polinômio irredutível. Então todas as suas raízes possuem a mesma multiplicidade.*

Demonstração. Exercício. □

Definição 6.9. Seja $\mathbb{E}/\mathbb{F}$ uma extensão algébrica de corpos. Dizemos que $a \in \mathbb{E}$ é *separável* sobre $\mathbb{F}$ se $\mathrm{Irr}(a, \mathbb{F})$ é um polinômio separável. Dizemos que a extensão $\mathbb{E}/\mathbb{F}$ é *separável* se todo $a \in \mathbb{E}$ é separável sobre $\mathbb{F}$.

Note que $a \in \mathbb{E}$ é separável sobre $\mathbb{F}$ se, e somente se, a é raiz de um polinômio separável em $\mathbb{F}[X]$.

Se $\mathrm{car}\,\mathbb{F} = p > 0$, então o mapa $F : \mathbb{F} \to \mathbb{F}$ definida por $F(a) = a^p$ é um endomorfismo de corpos (necessariamente injetora). A sua imagem é denotada por $\mathbb{F}^p$.

Definição 6.10. Seja $\mathbb{F}$ um corpo. Dizemos que $\mathbb{F}$ é *perfeito* se $\operatorname{car}\mathbb{F} = 0$, ou se $\operatorname{car}\mathbb{F} = p > 0$ e $\mathbb{F}^p = \mathbb{F}$.

Exemplo 6.1. Seja $\mathbb{F}$ um corpo de característica $p > 0$. Então $\mathbb{K} := \mathbb{F}(X)$ não é perfeito. Seja $\mathbb{E} = \mathbb{F}(X^p) \subseteq \mathbb{K}$. Então, veremos a seguir que a extensão $\mathbb{K}/\mathbb{E}$ não é separável.

Proposição 6.11. *Todo corpo finito e todo corpo algebricamente fechado são perfeitos.*

Demonstração. Seja $\mathbb{F}$ um corpo finito de característica $p > 0$. Então, sendo o mapa $F(a) = a^p$ injetivo e $\mathbb{F}$ finito, vale que F é sobrejetivo. Portanto, $\mathbb{F}^p = \mathbb{F}$.

Agora, seja $\mathbb{F}$ um corpo algebricamente fechado. Dado $a \in \mathbb{F}$, o polinômio $X^p - a$ admite alguma raiz em $\mathbb{F}$, digamos $b \in \mathbb{F}$. Portanto, $b^p = a$. Isso mostra que $\mathbb{F}^p = \mathbb{F}$. □

A seguir, mostraremos a relação entre corpos perfeitos e polinômios e extensões separáveis.

Teorema 6.12. *Seja $\mathbb{F}$ um corpo. As seguintes afirmações são equivalentes:*

(i) *O corpo $\mathbb{F}$ é perfeito.*
(ii) *Todo polinômio irredutível em $\mathbb{F}[X]$ é separável.*
(iii) *Toda extensão algébrica $\mathbb{E}/\mathbb{F}$ é separável.*

Demonstração. Se $\operatorname{car}\mathbb{F} = 0$, então todas as afirmações são válidas. Portanto, assuma que $\operatorname{car}\mathbb{F} = p > 0$.

$(i) \Rightarrow (ii)$: Seja $f \in \mathbb{F}[X]$ um polinômio irredutível. Se f não é separável, então do Teorema 6.6, $f \in \mathbb{F}[X^p]$. Portanto,

$$f(X) = \alpha_0 + \alpha_1 X^p + \alpha_2 X^{2p} + \cdots + \alpha_m X^{mp}.$$

Como $\mathbb{F}$ é perfeito (por (i)), segue que existem $\beta_0, \ldots, \beta_m \in \mathbb{F}$, de modo que $\beta_i^p = \alpha_i$, $i = 0, 1, \ldots, m$. Portanto,

$$f = \beta_0^p + \beta_1^p X^p + \cdots + \beta_m^p X^p = (\beta_0 + \beta_1 X + \cdots + \beta_m X^m)^p .$$

Isso contradiz a irredutibilidade de f. Portanto, f é separável.

$(ii) \Rightarrow (iii)$: Sejam $\mathbb{E}/\mathbb{F}$ uma extensão algébrica, e $a \in \mathbb{E}$. Então, $\operatorname{Irr}(a, \mathbb{F})$ é irredutível. De (ii) segue que o mesmo é separável. Portanto, a extensão $\mathbb{E}/\mathbb{F}$ é separável.

$(iii) \Rightarrow (i)$: Dado $a \in \mathbb{F}$, seja $f = X^p - a$. Se b é uma raiz de f, então $b^p = a$, e portanto, $f = X^p - b^p = (X - b)^p$. Daí, o polinômio minimal p_b de b sobre $\mathbb{F}$ divide $(X - b)^p$. Então, todas as suas raízes são iguais a b. Como a extensão $\mathbb{F}[b]/\mathbb{F}$ é algébrica, de (iii), vale que a mesma é separável. Portanto, p_b é separável. Assim, $p_b = X - b$. Segue que $b \in \mathbb{F}$. Então $\mathbb{F}^p = \mathbb{F}$, ou seja, $\mathbb{F}$ é perfeito.

□