Capítulo 3

EXTENSÕES DE CORPOS E GRAU DE UMA EXTENSÃO

Trataremos aqui do estudo de corpos, corpos finitos, extensões de corpos e discorreremos sobre o grau de uma extensão.

Definição 3.1: Um *corpo* é um anel comutativo com elemento unidade no qual todo elemento não nulo possui inverso multiplicativo.

Como exemplo de corpos podemos citar:

- O conjunto dos números racionais sob adição e multiplicação usuais;
- O conjunto dos números reais sob adição e multiplicação usuais;
- O conjunto $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$, (*primo*), sob adição e multiplicação módulo p.

Note, entretanto que os conjuntos $\mathbb{Z}$ e $\mathbb{Z}_n$, n composto, não são corpos pois:

- $a \in \mathbb{Z},\ a \neq \pm 1, \nexists\ \ b \in \mathbb{Z}$ tal que $ab = 1$.
- $\exists\ a, b \in \mathbb{Z}_n,\ a \neq 0$ e $b \neq 0$, tal que $ab \equiv 0 \mod n$.

Exemplo 3.1: Seja $\alpha = \sqrt{2} \in \mathbb{R}$ e $K = \mathbb{Q}$. Vamos mostrar que:
$K[\alpha] = \mathbb{Q}[\sqrt{2}\,] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

Por definição temos $\mathbb{Q}[\sqrt{2}\,] = \{f(\sqrt{2}\,) \mid f(x) \in \mathbb{Q}[x]\}$. Agora se $f(x) \in \mathbb{Q}[x]$, segue pelo algorítimo da divisão que existe $q(x),\ r(x) \in \mathbb{Q}[x]$ tais que
$f(x) = q(x)(x^2 - 2) + r(x)$, onde $r(x) = a + bx,\ a, b \in \mathbb{Q}$, e daí vem que $f(\sqrt{2}\,) = r(\sqrt{2}\,) = a + b\sqrt{2},\ a, b \in \mathbb{Q}$.

Dessa forma $J = \mathbb{Q}[\sqrt{2}\,] = \{f(\sqrt{2}\,) : f(x) \in \mathbb{Q}[x]\} = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ é um corpo.

De fato:

i) $[(a_1 + b_1\sqrt{2}\,) + (a_2 + b_2\sqrt{2}\,)] + (a_3 + b_3\sqrt{2}\,) = [(a_1 + a_2) + (b_1 + b_2)\sqrt{2}\,] + a_3 + b$
$= (a_1 + a_2) + a_3 + [(b_1 + b_2) + b_3]\sqrt{2} = (a_1 + a_2 + a_3) + (b_1 + b_2 + b_3)\sqrt{2} = [a_1 + (a_2 +$
$+ [b_1 + (b_2 + b_3)]\sqrt{2} = a_1 + b_1\sqrt{2} + (a_2 + a_3) + [(b_2 + b_3)]\sqrt{2} = a_1 + b_1\sqrt{2} + [(a_2 + b$
$+(a_3 + b_3\sqrt{2}\,)]$.

A soma é associativa.

ii) Existe $0 + 0\sqrt{2} \in J$ tal que:
$(a + b\sqrt{2}\,) + (0 + 0\sqrt{2}\,) = (a + 0) + (b + 0)\sqrt{2} = a + b\sqrt{2}$.
Existe elemento neutro para a soma.

iii) Existe $-a + (-b)\sqrt{2} \in J$ tal que:
$a + b\sqrt{2} + (-a + (-b)\sqrt{2}\,) = [a + (-a)] + [b + (-b)]\sqrt{2} = (a - a) + (b - b)\sqrt{2} = 0 + 0\sqrt{2}$
Existe inverso aditivo.

iv)
$(a_1 + b_1\sqrt{2}\,) + (a_2 + b_2\sqrt{2}\,) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2} = (a_2 + a_1) + (b_2 + b_1)\sqrt{2}$
$= (a_2 + b_2\sqrt{2}\,) + (a_1 + b_1\sqrt{2}\,)$.
A soma é comutativa.

v)
$[(a_1 + b_1\sqrt{2}\,) \cdot (a_2 + b_2\sqrt{2}\,)] \cdot (a_3 + b_3\sqrt{2}\,) = [a_1a_2 + a_1b_2\sqrt{2} + b_1\sqrt{2}\,a_2 + b_1\sqrt{2}\,b_2\sqrt{2}\,]$

$\cdot(a_3 + b_3\sqrt{2}) = a_1a_2a_3 + a_1a_2b_3\sqrt{2} + a_1b_2\sqrt{2}\,a_3 + a_1b_2\sqrt{2}\,b_3\sqrt{2} + b_1\sqrt{2}\,a_2a_3 + b_1\sqrt{2}\,a_2b$
$+b_1\sqrt{2}\,b_2\sqrt{2}\,a_3 + b_1\sqrt{2}\,b_2\sqrt{2}\,b_3\sqrt{2} = (a_1 + b_1\sqrt{2}) \cdot [a_2a_3 + a_2b_3\sqrt{2} + b_2\sqrt{2}\,a_3 + b_2\sqrt{2}\,b_3\sqrt{2}$
$a_2a_3 + a_2b_3\sqrt{2} + b_2\sqrt{2}\,a_3 + b_2\sqrt{2}\,b_3\sqrt{2}] = (a_1 + b_1\sqrt{2}) \cdot [(a_2 + b_2\sqrt{2}) \cdot (a_3 + b_3\sqrt{2})]$.
A multiplicação é associativa.

vi) $\vdash (a_1 + b_1\sqrt{2}) \cdot [(a_2 + b_2\sqrt{2}) + (a_3 + b_3\sqrt{2})] = (a_1 + b_1\sqrt{2}) \cdot [(a_2 + a_3) + (b_2 + b$
$= a_1(a_2 + a_3) + a_1(b_2 + b_3)\sqrt{2} + b_1\sqrt{2}\,(a_2 + a_3) + b_1\sqrt{2}\,(b_2 + b_3)\sqrt{2} = a_1a_2 + a_1a_3 + a_1b$
$+ a_1b_3\sqrt{2} + b_1\sqrt{2}\,a_2 + b_1\sqrt{2}\,a_3 + b_1\sqrt{2}\,b_2\sqrt{2} + b_1\sqrt{2}\,b_3\sqrt{2} = (a_1 + b_1\sqrt{2}) \cdot (a_2 +$
$+(a_1 + b_1\sqrt{2}) \cdot (a_3 + b_3\sqrt{2})$.
Vale a distributividade à esquerda.
$\vdash [(a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2})] \cdot (a_3 + b_3\sqrt{2}) = [(a_1 + a_2) + (b_1 + b_2)\sqrt{2}] \cdot (a_3 + b$
$= (a_1 + a_2)a_3 + (b_2 + b_3)\sqrt{2}\,a_3 + (a_1 + a_2)b_3\sqrt{2} + (b_1 + b_2)\sqrt{2}\,b_3\sqrt{2} = a_1a_3 + a_2a_3 + a_3b$
$+ a_3b_3\sqrt{2} + b_3\sqrt{2}\,a_1 + b_3\sqrt{2}\,a_2 + b_3\sqrt{2}\,b_1\sqrt{2} + b_3\sqrt{2}\,b_2\sqrt{2} = (a_1 + b_1\sqrt{2}) \cdot (a_3 +$
$+(a_2 + b_2\sqrt{2}) \cdot (a_3 + b_3\sqrt{2})$.
Vale a distributividade à direita.

vii) Existe $1 + 0\sqrt{2} \in J$ tal que:
$(1 + 0\sqrt{2}) \cdot (a + b\sqrt{2}) = 1 \cdot a + 1 \cdot b\sqrt{2} + 0\sqrt{2} \cdot a + 0\sqrt{2} \cdot b\sqrt{2} = a \cdot 1 + b\sqrt{2} \cdot 1 + a \cdot$
$+b\sqrt{2} \cdot 0\sqrt{2} = a + b\sqrt{2}$.
J é um anel com unidade.

viii) $(a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) = a_1a_2 + a_1b_2\sqrt{2} + b_1\sqrt{2}\,a_2 + b_1\sqrt{2}\,b_2\sqrt{2} = a_2a_1 + b_2$
$+a_2b_1\sqrt{2} + b_2\sqrt{2}\,b_1\sqrt{2} = (a_2 + b_2\sqrt{2}) \cdot (a_1 + b_1\sqrt{2})$.
J é um anel comutativo.

ix) Exste $\frac{a_1}{a_1^2 - 2b_1^2} - \frac{b_1}{a_1^2 - 2b_1^2}\sqrt{2}, \in J$ tal que:
$(a_1 + b_1\sqrt{2}) \cdot [\frac{a_1}{a_1^2 - 2b_1^2} - \frac{b_1}{a_1^2 - 2b_1^2}\sqrt{2}] = a_1(\frac{a_1}{a_1^2 - 2b_1^2}) - a_1(\frac{b_1}{a_1^2 - 2b_1^2}\sqrt{2}) + b_1\sqrt{2}(\frac{a_1}{a_1^2 - 2b_1^2}$
$-b_1\sqrt{2}(\frac{b_1}{a_1^2 - 2b_1^2}\sqrt{2}) = \frac{a_1^2}{a_1^2 - 2b_1^2} - \frac{a_1b_1\sqrt{2}}{a_1^2 - 2b_1^2} + \frac{a_1b_1\sqrt{2}}{a_1^2 - 2b_1^2} - \frac{2b_1^2}{a_1^2 - 2b_1^2} = \frac{a_1^2 - 2b_1^2}{a_1^2 - 2b_1^2} = 1$.
Logo $\mathbb{Q}[\sqrt{2}]$ é um corpo.

Exemplo 3.2: Provar que o polinômio $x^2 - \overline{3}$ em $\mathbb{Z}_5[x]$ é irredutível sobre o corpo $K = \mathbb{Z}_5$. Mais ainda, se $J = \mathbb{Z}_5[x] \cdot f(x)$; onde $f(x) = x^2 - \overline{3}$ então, pelo Teorema 1 (ver Apêndice 1), temos que $\mathbb{Z}_5[x]/J$ é um corpo que possui exatamente 25 elementos.
$K = \mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ e $f(x) = x^2 - \overline{3}$, temos:
$f(x) = x^2 - \overline{3}$
$f(\overline{0}) = \overline{0}^2 - \overline{3} = -\overline{3} = \overline{2}$
$f(\overline{1}) = \overline{1}^2 - \overline{3} = -\overline{2} = \overline{3}$
$f(2) = \overline{2}^2 - \overline{3} = \overline{4} - \overline{3} = \overline{1}$
$f(\overline{3}) = \overline{3}^2 - \overline{3} = \overline{4} - \overline{3} = \overline{1}$
$f(\overline{4}) = \overline{4}^2 - \overline{3} = \overline{1} - \overline{3} = -\overline{2} = \overline{3}$, Logo $f(x)$ é irredutível.
$J = \mathbb{Z}_5[x] \cdot f(x)$ com $f(x) = x^2 - \overline{3}$.
$\mathbb{Z}_5[x]/J = \{p(x) + J \mid p(x) \in \mathbb{Z}_5[x]\} = \{f(x) \cdot q(x) + r(x) + J \mid f(x), q(x), r(x) \in \mathbb{Z}_5[$
$= \{r(x) + J \mid r(x) \in \mathbb{Z}_5[x]\}$, pois $f(x) \cdot q(x) \in J$.
Então, $\mathbb{Z}_5[x]/J = \{r(x) + J \mid r(x) \in \mathbb{Z}_5[x]\}$
$= \{\overline{a}x + \overline{b} + J : \overline{a}, \overline{b} \in \mathbb{Z}_5\}$.
Dessa forma, $\overline{a}x + \overline{b}$ nos fornece 5 possibilidades para $\overline{a}$ e 5 possibilidades para $\overline{b}$, e isto nos dá que $\mathbb{Z}_5[x]/J$ é um corpo com 25 elementos.

Exemplo 3.3: Provar que o polinômio $x^3 + x + \overline{1}$ em $\mathbb{Z}_5[x]$ é irredutível sobre o corpo

$K = \mathbb{Z}_5$. Mais ainda, se $J = \mathbb{Z}_5[x] \cdot f(x)$; onde $f(x) = x^3 + x + \overline{1}$ então, pelo Teorema 1 (ver Apêndice), temos que $\mathbb{Z}_5[x]/J$ é um corpo que possui exatamente 125 elementos.

$K = \mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ e $f(x) = x^3 + x + \overline{1}$, então:

$f(x) = x^3 + x + \overline{1}$

$f(\overline{0}) = \overline{1}$

$f(\overline{1}) = \overline{3}$

$f(\overline{2}) = \overline{1}$

$f(\overline{3}) = \overline{1}$

$f(\overline{4}) = \overline{4}$

Assim $f(x)$ é irredutível sobre $\mathbb{Z}_5$.

$J = \mathbb{Z}_5[x] \cdot f(x)$, onde $f(x) = x^3 + x + \overline{1}$

$\mathbb{Z}_5[x]/J = \{p(x) + J \mid p(x) \in \mathbb{Z}_5[x]\} = \{f(x) \cdot q(x) + r(x) + J \mid f(x),\ q(x),\ r(x) \in \mathbb{Z}$

$= \{r(x) + J \mid r(x) \in \mathbb{Z}_5[x]\}$.

$\mathbb{Z}_5[x]/J = \{r(x) + J \mid r(x) \in \mathbb{Z}_5[x]\} = \{\overline{a}x^2 + \overline{b}x + \overline{c} + (f(x)) : \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_5\}$.

Dessa forma, $\overline{a}x^2 + \overline{b}x + \overline{c}$ nos fornece 5 possibilidades para $\overline{a}$, 5 possibilidades para $\overline{b}$, e 5 possibilidades para $\overline{c}$ o que nos diz que $\mathbb{Z}_5[x]/J$ é um corpo com 125 elementos.

Exemplo 3.4: Seja $p(x)$ um polinômio irredutível de grau n sobre o corpo $\mathbb{Z}_p$, p primo, e seja $J = \mathbb{Z}_p[x] \cdot p(x)$. Provar que $\mathbb{Z}_p[x]/J$ é um corpo contendo exatamente p^n elementos.

$J = \mathbb{Z}_p[x] \cdot p(x) = f(x) \cdot p(x) = (p(x))$ com $f(x) \in \mathbb{Z}_p[x]$, onde

$p(x) = a_0 + a_1x + \ldots + a_nx^n$.

$\mathbb{Z}_5[x]/(p(x)) = \{f(x) + (p(x)) \mid f(x) \in \mathbb{Z}_p[x]\} = \{p(x) \cdot q(x) + r(x) + (p(x)) \mid p(x), q(x),$

$\in \mathbb{Z}_5[x]\} = \{r(x) + (p(x)) \mid r(x) \in \mathbb{Z}_p[x]\} = \{(b_0 + b_1x + \ldots + b_{n-1}x^{n-1}) + (p(x)) \mid b_0, b$

$b_{n-1} \in \mathbb{Z}_p\}$.

Dessa forma, $b_0 + b_1x + \ldots + b_{n-1}x^{n-1}$ nos fornece p possibilidades para cada b_i, $i = 0, \ldots, n-1$, donde o corpo $\mathbb{Z}_5[x]/(p(x))$ possui p^n elementos.

Definição 3.2.: Seja F um corpo. Um corpo K é dito uma *extensão de* F se K contém F. Equivalentemente, K é uma *extensão de* F se F é um subcorpo de K.

Por exemplo, $\mathbb{R}$ sob adição e multiplicação usuais é uma extensão de $\mathbb{Q}$, e $\mathbb{Q}[\sqrt{2}]$, é uma extensão de $\mathbb{Q}$, que contém $\sqrt{2}$ e $\mathbb{Q}$, de acordo com o exemplo 3.1.

Neste capítulo, F indicará um corpo qualquer e K uma extensão de F.

Definição 3.3: O *grau* de K sobre F é a dimensão de K como espaço vetorial sobre F.

Indicaremos o grau de K sobre F por $[K : F]$. Se K é de dimensão finita como espaço vetorial sobre F, $[K : F]$ é finito, isto é, K é uma extensão finita de F.

Teorema 3.1: Se L é uma extensão finita de K e se K é uma extensão finita de F, então L é uma extensão finita de F. Além disso, $[L : F] = [L : K] \cdot [K : F]$.

Demonstração: Suponhamos que $[L : K] = m$ e que $[K : F] = n$. Seja $v_1, \ldots, v_m$ uma base de L sobre K e seja $w_1, \ldots, w_n$ uma base de K sobre F. Afirmamos que os elementos v_iw_j, onde $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$, formam uma base de L sobre F.

De fato:

Seja t um elemento qualquer de L. Como todo elemento de L é uma combinação linear de $v_1, \ldots, v_m$ com coeficientes em K, em particular, t é dessa forma. Assim, $t = k_1v_1 + \ldots + k_mv_m$ onde os elementos $k_1, \ldots, k_m$ estão todos em K. Contudo, todo elemento em K é uma combinação linear de $w_1, \ldots, w_n$ com coeficientes em F. Assim,

$$k_1 = f_{11}w_1 + \ldots + f_{1n}w_n, \ldots,\ k_i = f_{i1}w_1 + \ldots + f_{in}w_n, \ldots,\ k_m = f_{m1}w_1 + \ldots + f_{mn}w_n,$$

onde cada f_{ij} está em F.

Substituindo estas expressões para $k_1, \ldots, k_m$ em $t = k_1v_1 + \ldots + k_mv_m$ obtemos $t = (f_{11}w_1 + \ldots + f_{1n}w_n)v_1 + \ldots + (f_{m1}w_1 + \ldots + f_{mn}w_n)v_m$. Efetuando os produtos, usando as leis distributiva e associativa, chegamos a $t = f_{11}v_1w_1 + \ldots + f_{1n}v_1w_n + \ldots + f_{ij}v_iw_j + \ldots + f_{mn}v_mw_n$. Como os f_{ij} estão em F, exibimos t como uma combinação linear sobre F dos elementos v_iw_j. Portanto, os elementos v_iw_j geram o Espaço vetorial L sobre o corpo F, e então eles preenchem a primeira condição para ser uma base.

Resta ainda mostrar que os elementos v_iw_j são linearmente independentes sobre F.

Suponhamos que $f_{11}v_1w_1 + \ldots + f_{1n}v_1w_n + \ldots + f_{ij}v_iw_j + \ldots + f_{mn}v_mw_n = 0,$ onde os f_{ij} estão em F. Queremos mostrar que cada $f_{ij} = 0$. Reagrupando a expressão acima temos

$$(f_{11}w_1 + \ldots + f_{1n}w_n)v_1 + \ldots + (f_{i1}w_1 + \ldots + f_{in}w_n)v_i + \ldots + (f_{m1}w_1 + \ldots + f_{mn}w_n)v_m = 0.$$

Como os w_i estão em K e como $F \subset K,$ todos os elementos $k_i = f_{i1}w_1 + \ldots + f_{in}w_n$ estão em K. Ora, $k_1v_1 + \ldots + k_mv_m = 0$ com $k_1, \ldots, k_m \in K$. Mas, por hipótese, $v_1, \ldots, v_m$ forma uma base de L sobre K. Logo, $k_1 = k_2 = \ldots = k_m = 0$. Usando os valores explícitos dos k_i, obtemos: $f_{i1}w_1 + \ldots + f_{in}w_n = 0$ para $i = 1, 2, \ldots, m$. Mas recordando o fato de que os w_i são linearmente independentes sobre F, resulta que cada $f_{ij} = 0$. Assim, os v_iw_j são linearmente independentes sobre F. Assim os mn elementos v_iw_j formam uma base de L sobre F.

Portanto, $[L : F] = mn$. Como $m = [L : K]$ e $n = [K : F],$ obtemos $[L : F] = [L : K]\ [K : F]$. ■

Corolário 3.1.1: Se L é uma extensão finita de F e se K é um subcorpo de L que contém F, então $[K : F] \mid [L : F]$.

Demonstração: Se K é um subcorpo de L que contém F, então pela definição de extensão, K é uma extensão de F. $[L : F]$ é finito, logo a dimensão de L como espaço vetorial sobre F é finita. Sendo K subespaço de L sobre F, temos que $[K : F]$ é finito. Como F é subespaço de K e $[L : F]$ é finito então $[L : K]$ é finito. Assim pelo Teorema 3.1 $[K : F] \mid [L : F]$. ■

Assim, por exemplo, se $[L : F]$ é um número primo, então não podem existir corpos entre F e L a não ser F e L.

Extensões algébricas

Definição 3.4: Um elemento $a \in K$ é dito *algébrico sobre F* se existem elementos $\alpha_0, \ldots, \alpha_n$ em F, não todos nulos, tais que $\alpha_0 + \alpha_1a + \ldots + \alpha_na^n = 0$.

Se o polinômio $q(x) \in F[x],\ q(x) = \beta_mx^m + \beta_{m-1}x^{m-1} + \ldots + \beta_0,$ então, para todo elemento $b \in K,$ por $q(b)$ indicaremos o elemento $\beta_mb^m + \beta_{m-1}b^{m-1} + \ldots + \beta_0$ de K. Diz-se que o elemento b satisfaz $q(x)$ se $q(b) = 0$.

Assim, $a \in K$ é algébrico sobre F se, e somente se, existe um polinômio não nulo $p(x) \in F[x]$, para o qual $p(a) = 0$.

Um número complexo é dito um número algébrico se ele é algébrico sobre o corpo dos números racionais, já que todo número complexo é algébrico sobre o corpo dos números reais (Teorema Fundamental da Álgebra).

Exemplo 3.5: $\alpha = i \in \mathbb{C}$ é algébrico sobre $\mathbb{Q}[x]$, pois α é raiz de $p(x) = x^2 + 1,$ onde

$p(x) \in \mathbb{Q}[x]$.

Exemplo 3.6: Dado $f(x) \in \mathbb{Q}[x]$ tal que $f(x) = x^3 - 2$, vemos que $\sqrt[3]{2} \in \mathbb{R}$ é algébrico sobre $\mathbb{Q}$ pois $f(\sqrt[3]{2}) = 0$.

Sejam K uma extensão de F e $a \in K$. Seja Ω a coleção de todos os subcorpos de K que contém F e a. Ω é não vazio, pois o próprio K é um elemento de Ω. Ora, a intersecção de um número qualquer de subcorpos de K é novamente um subcorpo de K. Assim, a intersecção de todos os subcorpos de K que são elementos de Ω é um subcorpo de K. Indicaremos esse subcorpo por $F(a)$.

Certamente, ele contém F e a, pois isto é verdadeiro para todo subcorpo de K que é membro de Ω. Além disso, pela definição de intersecção, todo subcorpo de K em Ω contém $F(a)$ e ao mesmo tempo $F(a)$ está em Ω. Assim $F(a)$ é o menor subcorpo de K que contém F e a. Denominamos $F(a)$ o subcorpo obtido pela *adjunção* de a a F. Como exemplo, $\mathbb{Q}(\sqrt{2})$.

Consideremos, agora, todos os elementos em K que podem ser expressos na forma $\beta_0 + \beta_1 a + \ldots + \beta_s a^s$, onde os β_i podem variar livremente sobre F e s é qualquer inteiro não negativo. Como todo elemento não nulo de K, é inversível, podemos definir U como o conjunto de todas as frações de elementos que podem ser expressos como acima. U é um subcorpo de K.

U certamente contém F e a, logo $U \supset F(a)$. Por outro lado, qualquer subcorpo de K que contém F e a, em virtude do fechamento com relação à adição e à multiplicação, contém necessariamente todos os elementos $\beta_0 + \beta_1 a + \ldots + \beta_s a^s$. Como $F(a)$ é um corpo, contém todas as frações de tais elementos. Portanto, $F(a) \supset U$.

Dessa forma as relações $U \subset F(a)$ e $U \supset F(a)$ indicam que $U = F(a)$.

Teorema 3.2: O elemento a em K é algébrico sobre F se, e somente se, $F(a)$ é uma extensão finita de F.

Demonstração:

($\Leftarrow$)

Suponhamos que $F(a)$ seja uma extensão finita de F e que $[F(a) : F] = m$. Consideremos os elementos $1, a, a^2, \ldots, a^m$, eles estão todos em $F(a)$ e assim existem $m + 1$ elementos da forma a^i em $F(a)$. Pela Proposição 2.5. estes elementos são linearmente dependentes sobre F. Portanto, existem elementos $\alpha_0, \alpha_1, \ldots, \alpha_m$ em F, não todos nulos, tais que $\alpha_0 1 + \alpha_1 a + \alpha_2 a^2 + \ldots + \alpha_m a^m = 0$. Logo, a é algébrico sobre F e satisfaz o polinômio não nulo $p(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_m x^m$ em $F[x]$ de grau no máximo $m = [F(a) : F]$. Isto mostra a primeira parte do teorema.

($\Rightarrow$)

Suponhamos que a em K seja algébrico sobre F. Por hipótese, a satisfaz algum polinômio não nulo em $F[x]$. Seja $p(x)$ um polinômio de $F[x]$ de grau positivo e mínimo tal que $p(a) = 0$. Afirmamos que $p(x)$ é irredutível sobre F. De fato, suponhamos que $p(x) = f(x)g(x)$, onde $f(x), g(x) \in F[x]$, então $0 = p(a) = f(a)g(a)$ e, como $f(a)$ e $g(a)$ são elementos do corpo K, o fato de que seu produto é 0 implica $f(a) = 0$ ou $g(a) = 0$. Como $p(x)$ é de grau positivo mínimo, com $p(a) = 0$, concluímos que $gr[f(x)] \geq gr[p(x)]$ ou $gr[g(x)] \geq gr[p(x)]$. Mas isto mostra a irredutibilidade de $p(x)$.

Definimos a aplicação ψ de $F[x]$ em $F(a)$ tal que todo $h(x) \in F[x]$, $\psi[h(x)] = h(a)$. ψ é um homomorfismo de $F[x]$ em $F(a)$. Pela definição de ψ, $N(\psi) = \{h(x) \in F[x] \mid h(a) = 0\}$. Além disso, $p(x)$ é um elemento de grau mínimo no ideal $N(\psi) \subset F[x]$. Como todo elemento em $N(\psi)$ é mútiplo de $p(x)$, e como $p(x)$ é irredutível, $N(\psi)$ é um ideal maximal de $F[x]$. $F[x]/N(\psi)$ é um corpo (ver apêndice). Ora, $F[x]/N(\psi)$ é isomorfo à imagem de $F[x]$ por meio de ψ. Assim, demonstramos que a imagem de $F[x]$ por meio de ψ é um subcorpo de $F(a)$. Esta imagem contém $\psi(x) = a$ e, para todo

$\alpha \in F,\ \psi(\alpha) = \alpha$. Assim, a imagem de $F[x]$ por meio de ψ é um subcorpo de $F(a)$ que contém F e a; pela definição de $F(a)$ concluímos que a imagem de $F[x]$ por meio de ψ é $F(a)$. Mais sucintamente, $F[x]/N(\psi)$ é isomorfo a $F(a)$.

Como, $N(\psi) = (p(x))$, o ideal gerado por $p(x)$, afirmamos que a dimensão de $F[x]/N(\psi)$, como espaço vetorial sobre F, é exatamente igual a $gr[p(x)]$. Em vista do isomorfismo entre $F[x]/N(\psi)$ e $F(a)$ obtemos o fato de que $[F(a) : F] = gr[p(x)]$. Portanto, $[F(a) : F]$ é certamente finito. ■

Definição 3.5: Um elemento $a \in K$ é dito *algébrico de grau n* sobre F se ele satisfaz um polinômio não nulo sobre F de grau n, mas não satisfaz nenhum polinômio de grau menor.

Teorema 3.3: Se $a \in K$ é algébrico de grau n sobre F, então $[F(a) : F] = n$.

Demonstração: Como $a \in K$ é algébrico sobre F, então pela demonstração do Teorema anterior, temos que $[F(a) : F]$ é exatamente o grau do polinômio satisfeito por a e de grau mínimo, $p(x)$. Por hipótese, $a \in K$ é algébrico de grau n, isto significa que $p(x)$ possui grau n. Desses dois fatos temos, $[F(a) : F] = gr[p(x)] = n$. ■

Teorema 3.4: Se $a, b \text{ em } K$ são algébricos sobre F, então $a \pm b, ab \text{ e } a/b \ (se\ b \neq 0)$ são todos algébricos sobre F. Em outras palavras, os elementos em K que são algébricos sobre F formam um subcorpo de K.

Demonstração: Suponhamos que a seja algébrico de grau m sobre F e que b seja algébrico de grau n sobre F. Pelo Teorema 3.3, o subcorpo $T = F(a)$ de K é de grau m sobre F. Ora, b é algébrico de grau n sobre F, ele é algébrico de grau no máximo n sobre T que contém F. Assim, o subcorpo $W = T(b)$ de K, pelo Teorema 3.3, também é de grau no máximo n sobre T. Mas $[W : F] = [W : T]\ [T : F]$ pelo Teorema 3.1; portanto, $[W : F] \leq mn$ e então W é uma extensão finita de F. Contudo, a e b estão em W, logo, $a \pm b,\ ab$ e a/b estão em W. Pelo Teoerma 3.2, como $[W : F]$ é finito, estes elementos são algébricos sobre F. ■

Corolário 3.4.1: Se a e b em K são algébricos sobre F de graus $m \ e \ n$, respectivamente, então $a \pm b,\ ab,\ e\ a/b \ (para\ b \neq 0)$ são algébricos sobre F de graus no máximo mn.

Demonstração: Da demonstração do Teorema anterior, temos que $[W : F] \leq mn$. Logo todo elemento em W satisfaz um polinômio de grau no máximo mn sobre F. ■

Definição 3.6: A extensão K de F é denominada uma *extensão algébrica de F* se todo elemento em K é algébrico sobre F.

Seja $f(x) \in F[x]$ e $\alpha_1, \ldots, \alpha_r$ as raízes distintas de $f(x)$ em K, onde K é uma extensão de F.

Consideremos $F_0 \subset F_1 = F_0(\alpha_1) \subset F_2 = F_1(\alpha_2) \subset \ldots \subset F_r = F_{r-1}(\alpha_r)$. Dessa forma, vemos que F_r é o menor subcorpo de K que contém F e $\alpha_1, \ldots, \alpha_r$.

Denotaremos F_r por $F(\alpha_1, \ldots, \alpha_r)$.

Teorema 3.5: Se L é uma extenção algébrica de K e se K é uma extensão algébrica de F, então L é uma extensão algébrica de F.

Demonstração: Seja u um elemento arbitrário de L. Temos que u satisfaz algum polinômio $x^n + \sigma_1 x^{n-1} + \ldots + \sigma_n,\ \sigma_1, \ldots, \sigma_n \in K$. Más, K é algébrico sobre F, então se usarmos várias vezes o Teorema 3.3, concluímos que $M = F(\sigma_1, \ldots, \sigma_n)$ é uma extensão finita de F. Como u satisfaz o polinômio $x^n + \sigma_1 x^{n-1} + \ldots + \sigma_n$ cujos coeficientes estão em M, pois M é o menor subcorpo de L que contém K e $\sigma_1, \ldots, \sigma_n$, então u é algébrico sobre M. Assim, pelo Teorema 3.2, temos que $M(u)$ é uma extensão finita de F. Logo u é algébrico sobre F e,

portanto, L é uma extensão algébrica de F.■