EXTENSÕES FINITAS E CO-EXTENSÕES CO-FINITAS SOBRE REAIS

FELISBERTO DE CAMARGO ADDISON

Orientador
Prof. Dr. John Edmonds David

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação da Universidade Estadual de Campinas, como requisito parcial para a obtenção do título de Mestre em Matemática.

Este trabalho foi realizado com auxílio financeiro do Conselho Nacional de Pesquisas (CNPq)

Janeiro 1978

À MÁRCIA

A G R A D E C I M E N T O S

Ao Prof.Dr. *John Edmonds David*, que com sua segura orientação permitiu a realização deste trabalho.

Aos meus pais, pela confiança e esforços para que eu pudesse estudar. Em particular, à minha mãe que, com a morte de meu pai, lutou heroicamente para que seus filhos terminassem os estudos.

Ao Prof.Dr. *Carlos Segovia*, pela discussão e ensinamento dado no capítulo 1.

Ao Conselho Nacional de Pesquisas (CNPq), pelo auxílio financeiro que tornou possível a realização deste trabalho.

Enfim, a todos que colaboraram, direta ou indiretamente, para que eu pudesse aperfeiçoar meus estudos.

A todos, meus imensos agradecimentos.

Felisberto de Camargo Addison

Í N D I C E

INTRODUÇÃO 1

CAPÍTULO 1 - UMA APLICAÇÃO DO TEOREMA DA FUNÇÃO INVERSA DE *HADAMARD* PARA A ÁLGEBRA 3

CAPÍTULO 2 - EXTENSÕES FINITAS SOBRE OS REAIS 8

CAPÍTULO 3 - EXTENSÕES FINITAS SOBRE OS REAIS 17

CAPÍTULO 4 - CO-EXTENSÕES CO-FINITAS SOBRE OS REAIS 26

CAPÍTULO 5 - CARACTERIZAÇÃO DOS CORPOS REALMENTE FECHADOS 37

BIBLIOGRAFIA 41

I N T R O D U Ç Ã O

Estaremos enfocando nesta tese quatro tópicos interessantes. No primeiro capítulo, mostraremos como o teorema da função inversa pode ser usado para provar um fato não conhecido de todos; que o espaço euclideano de dimensão N, $\mathbb{E}^n$ não pode ser dotado com uma estrutura de álgebra, não associativa, cancelativa e comutativa, quando $N \geqslant 3$. Estaremos interessados em definir uma operação multiplicação $(*)$, tal que $x, y \longrightarrow x * y$ sobre $\mathbb{E}^n$, satisfazendo os quatro axiomas abaixo:

(1) $x * (\lambda * y) = (\lambda * x) * y = \lambda * x * y$
(2) $x * (y * z) = x * y + x * z$
(3) $x * y = 0$ implica $x = 0$ ou $y = 0$
(4) $x * y = y * x$

Quanto ao capítulo 2, veremos fatos que são devidos a *FROBENIUS*. Este matemático, em 1887, classificou todos os anêsis com divisão, que têm o corpo dos números reais em seu centro e são de dimensão finita sobre os reais.

No capítulo 3, daremos uma outra demonstração mais sofisticada, devido a *R.S. PALAIS*, sobre os fatos descritos acima.

Em ambos os casos, mostraremos que as únicas álgebras de divisão, finitas sobre os reais, são os reais, os números complexos e a álgebra dos quatérnios de *HAMILTON*.

Definição 1
Co-extensão de um corpo F é um corpo $E \subseteq F$.

Definição 2
Co-dimensão de uma co-extensão $E \subseteq F$ é $[F:E]$.

Já no Capítulo 4, veremos que os corpos co-extensões de co-dimensão finita sobre os números complexos são de co-

-dimensão dois. Quer dizer, para qualquer corpo contido nos complexos tal que os complexos são uma extensão de dimensão finita, tem-se que esta dimensão é dois. Portanto, provaremos que os reais não têm um corpo co-extensão de co-dimensão próprio.

No capítulo 5 daremos uma caracterização dos corpos realmente fechados devidos a *Artin-Scheier*.

CAPÍTULO 1

UMA APLICAÇÃO DO TEOREMA DA FUNÇÃO INVERSA DE HADAMARD PARA A ÁLGEBRA

Vejamos algumas noções preliminares sobre aplicações bilineares.

Definição 1.1 - Sejam E, F, G espaços vetoriais normados. Uma aplicação $B: E \times F \longrightarrow G$ diz-se bilinear quando é linear separadamente em cada uma das suas variáveis, ou seja:

$$(1)\ B(x + y, z) = B(x, z) + B(y, z)$$
$$(2)\ B(x, z + w) = B(x, z) + B(x, w)$$
$$(3)\ B(\lambda x, z) = B(x, \lambda z) + \lambda B(x, z)$$

quaisquer que sejam $x, y \in E$
$z, w \in F$
$\lambda \in \mathbb{R}$

Temos então um teorema bastante simples de ser provado pelo leitor, que é o teorema 1.2.

Teorema 1.2 - Sejam E, F espaços vetoriais normados de dimensão finita. Toda aplicação bilinear $B: E \times F \longrightarrow G$ é contínua. Veja [13].

Retornando ao nosso problema, definamos uma operação multiplicação $(*)\ x, y \longrightarrow x * y$ sobre $\mathbb{E}^n$ que, para todos os escolares "λ" e vetores x, y e z, satisfaz os seguintes axiomas:

$$(1)\ x * (\lambda * y) = (\lambda * x) * y = \lambda * x * y$$
$$(2)\ x * (y + z) = x * y + x * z$$
$$(3)\ x * y = 0 \text{ implica } x = 0 \text{ ou } y = 0$$
$$(4)\ x * y = y * x$$

Provaremos o teorema crucial deste capítulo que é o teorema 1.3.

Teorema 1.3 - Para $N \geq 3$, não existe uma operação multiplicação sobre $\mathbb{E}^n$ que satisfaz (1) - (4).

O que temos de novidade em nossa prova é que, embora assumimos a comutatividade, não assumimos a lei associativa, ou seja $(x * y) * z = x * (y * z)$.

Senão vejamos: se a lei associativa estivesse junto com (1) - (4), então provaríamos a existência do elemento "e" satisfazendo $x * e = e * x = x$ para todo $x \in \mathbb{E}^n$.

Demonstração

Seja "a" um elemento não nulo e fixo de $\mathbb{E}^n$. Decorre do axioma (3) que a aplicação linear $x \longrightarrow a * x$ é não singular e tal que $a * e = a$ para algum vetor "e". Portanto, para qualquer vetor "b", temos: $a * b = (a * e) * b = a * (e * b)$. Segue-se que $b = e * b$. Também, desde que $e^2 = e$, temos $b * e = b * e^2 = (b * e) * e$, portanto $b = b * e$.

Então $\mathbb{E}^n$ será corpo de extensão finita de R (identificado com um conjunto de todos os múltiplos escalares $a * e$, $a \in \mathbb{R}$). Do *Teorema Fundamental da Álgebra*, segue-se então que $\mathbb{E}^n$ é $\mathbb{R}$ ou $\mathbb{C}$. Considerando mais geralmente, o problema análogo é da existência de álgebras, com divisão, algébricas sobre os reais. Veja [1], [2], [5] e [6].

Aliás, estes dois últimos serão mostrados nos capítulos seguintes.

Demonstração do teorema 1.3

Nossa prova consiste em mostrar que os axiomas (1) - (4) implicam que a aplicação $x \longrightarrow x^2$ é um homeomorfismo - quando $N \geq 3$, o que é obviamente um absurdo, pois o axioma (1) requer que $(-x)^2 = x^2$. A prova desta asserção depende do fato de que o espaço $\mathbb{E}^n - \{P\}$ (espaço euclideano sem um ponto) é simplesmente conexo quando $N \geq 3$.

Usaremos a seguinte versão global do teorema da função inversa, que é devido a *Hadamard* (para detalhes e referência veja [3] e [4].

Teorema 1.4 (Hadamard)

Seja f: M_1 ——— M_2 uma aplicação C^1 entre duas variedades conexas N - dimensionais, cujo jacobiano nunca se anula e que é própria no sentido de que f^{-1} (K) é compacto quando K é um subconjunto compacto de M_2. Suponha-se ainda que M_2 é simplesmente conexa. Então f é um homeomorfismo.

Lema 1.5

Qualquer que seja a aplicação bilinear B: $\mathbb{E}^n \times \mathbb{E}^n \longrightarrow \mathbb{E}^n$, em que B (x, x) = 0 implica x = 0, existe um a > 0 tal que $\forall x$, $|x| = 1$.

$$| B (x, x)| > a$$

Demonstração

Se tal não acontece, devemos ter $|B (x_n, x_n)| < \frac{1}{n}$ para uma sequência x_n, tal que $|x_n| = 1$ e $\lim x_n = x \neq 0$, logo $\lim |B (x_n, x_n)| = |B (\lim x_n, \lim x_n)| = |B (x, x)| = 0$, contradição.

Usamos o fato de que B é contínua, pois é uma aplicação bilinear.

Portanto, qualquer que seja $y \in \mathbb{E}^n$

$$(I) | B (y, y)| = |B (\frac{y}{|y|}, \frac{y}{|y|})| \ |y|^2 > a \ |y|^2$$

Continuação da prova do teorema 1.3.

Provaremos que F (x) = B (x, x) = x^2 de $\mathbb{E}^n$ nele mesmo é própria.

Vemos que pela própria definição e pelo teorema 1.2, F é contínua.

Seja S um subconjunto compacto de $\mathbb{E}^n$, então S é fechado e limitado. Pelo visto acima, F^{-1} (S) é fechado. Falta de

monstrar que $\bar{F}^1$ (S) é limitado, para concluirmos que F é própria.

Como S é limitado, $|S| < N$, $\forall s \in S$.

Ora $\bar{F}^1(S) = \{t \mid t^2 \in S\} = \{t \in \mathbb{E}^n \mid B(t, t) \in S\}$.

Mas $B(t, t) \in S$ implica que $|B(t, t)| < N$.

Por (I) $|B(t, t)| > a|t|^2$, portanto

$N > a|t|^2$, donde $|t| < \sqrt{N/a}$

Logo $|\{t \in \mathbb{E}^n \mid B(t, t) \in S\}| < \sqrt{N/a}$. Segue-se que $\bar{F}^1(S)$ é limitado.

Usaremos a seguir o teorema 1.6, bem conhecido em topologia.

Teorema 1.6

Sejam X, Y espaços topológicos e $X \subseteq Y$. Se $S \subseteq X$, então S é compacto em X se, e somente se, S é compacto em Y.

No nosso caso, consideremos S compacto em $\mathbb{E}^n - \{0\}$. Aplicando o teorema 1.6, vemos que S é compacto em $\mathbb{E}^n$. Portanto, $\bar{F}^1(S)$ é compacto em $\mathbb{E}^n$. Usando novamente o teorema 1.6, $\bar{F}^1(S)$ é compacto em $\mathbb{E}^n - \{0\}$.

Para aplicar o teorema de *Hadamard*, seja $M_1 = M_2 = \mathbb{E}^n - \{0\}$. O axioma (3) implica que a aplicação $g(x) = x^2$ pode ser restringida a uma aplicação "f" de $\mathbb{E}^n - \{0\}$ nele mesmo. Como sabemos f é contínua e, também, pelo visto acima e desde que $\bar{f}^1(S) = \bar{F}^1(S)$, f é própria.

Usando o axioma (4) para computar $df_x(v)$ (a diferencial de f em "x" operando na direção "v")

$$df_x(v) = \lim_{h \to 0} \frac{f(x + hv) - f(x)}{h} =$$

$$= \lim_{h \to 0} \frac{(x + hv)^2 - x^2}{h} =$$

$$= \lim_{h \to 0} \frac{x^2 + xhv + hvx + h^2v^2 - x^2}{h} =$$

$$= \lim_{h \to 0} \frac{h\,(xv + vx) + h\,(hv^2)}{h} =$$

$$= \lim_{h \to 0} \frac{xv + vx + hv^2}{h} = xv + vx$$

Logo $df_x\,(v) = 2xv$ e consequentemente df_x é contínua em x. Portanto, $f \in C^1$, e pelo axioma (s), $df_x\,(v)$ é não singular para todo $x \in E^n - \{0\}$, isto é, o jacobiano de f nunca se anula. Provamos, então, que f é homeomorfismo.

Prova do teorema 1.4

O fato de que f é sobre, é bem conhecido e fácil, de ser provado, uma vez que tenham sido estabelecidas as propriedades básicas de grau topológico de aplicações. Beja [7], [8], [9] e [10].

Provaremos, agora, que f é um a um. A variedade, sendo simplesmente conexa, admite uma cobertura universal para espaço. Portanto, é suficiente mostrar que f é uma cobertura, isto é, mostraremos que cada "q" em M_2 tem uma vizinhança aberta V, tal que $\bar{f}^1\,(V)$ consista de conjuntos abertos, disjuntos, aplicados homeomorficamente pela f sobre V. Isto é, mostrado mediante uma construção dada por *Milnor* em [11, pag. 8].

Desde que f é um homeomorfismo local próprio, $\bar{f}^1(q)$ consiste de somente um número finito de pontos, digamos $p_1, p_2, \cdots, p_n$.

Seja K uma vizinhança compacta de q. Então $\bar{f}^1\,(K)$ contém vizinhanças abertas disjuntas V_i dos pontos p_i, que são aplicadas homeomorficamente pela f sobre vizinhanças abertas de q.

Seja $V = \left[f(V_1) \cap \ldots \cap f(V_n)\right] - f\left[\bar{f}^1(K) - (V_1 \cup \ldots \cup V_n)\right]$

Deixaremos para o leitor verificar que V satisfaz as condições desejadas. Com isto concluimos nossa prova.

C A P Í T U L O 2

TEOREMA DE FROBENIUS

Usaremos dois lemas importantes sobre o corpo dos números complexos.

Lema 2.1

Todo polinômio de grau "n" sobre o corpo dos números complexos tem todas as suas n - raizes no corpo dos números complexos.

Lema 2.2

Os únicos polinômios irredutíveis sobre o corpo dos números reais são de grau 1 ou 2.

Definição 2.3

Uma álgebra com divisão D é dita algébrica sobre o corpo K se:

(a) K está contido no centro de D
$z(D) = \{x \in D \mid xy = yx, \forall y \in D\}$.

(b) Todo $a \in D$ satisfaz um polinômio não trivial com coeficiente em K

Se D, como um espaço vetorial é de dimensão finita sobre um corpo K que está contido em seu centro, vem os facilmente que D é algébrico sobre K.

Contudo, pode ser que D seja algébrico sobre K, sem ser de dimensão finita sobre K.

Exemplo: Seja $a \in K \setminus K^p$, isto implica que $x^p - a$ é irredutível so

bre K. Portanto $x^{p^i} - a$ é irredutível sobre K. Seja α_i raiz de $x^{p^i} - a$.

Como $K(\alpha_i) \subsetneq K(\alpha_{i+1}) \subsetneq K(\alpha_{i+2}) \subsetneq \ldots$ temos o que queríamos demonstrar. Mais claramente: sejam Ro os números racionais e consideremos $\overline{Ro}$ (fecho algébrico dos racionais). Pelo visto acima, tomemos $a = 2$ e $p = 2$.

$$x^2 - 2,\ x^4 - 2,\ x^8 - 2,\ \ldots$$

Definição 2.4

Um anel associativo A é denominado uma álgebra sobre um corpo K, se A é um espaço vetorial sobre K, tal que:

$$k(a\,b) = (k\,a)b = a(k\,b),\ \forall\ a, b \in A \text{ e } k \in K$$

Costuma-se denotar *Hom* (V, V) por A (V).

Sempre que quisermos enfatizar o papel do corpo K, a notação é $A_K(V)$.

Definição 2.5

Uma transformação linear de V sobre K, é um elemento de $A_K(V)$.

Às vezes pode ser feita referência a A (V) como o anel, ou álgebra, das transformações lineares de V.

Para álgebras arbitrárias A, com elemento unidade sobre um corpo K, temos o análogo do teorema de *Cayley* para grupos, a saber:

Teorema 2.6

Se A é uma álgebra sobre K, com elemento unidade, então A é isomorfa a uma sub-álgebra de A (V), para algum espaço vetorial V sobre K.

O teorema ressalta o papel universal desempenhado

pelas álgebras particulares A (V), pois nestas podemos encontrar cópias isomorfas de qualquer álgebra.

Iniciaremos nossa investigação de anéis algébricos com divisão sobre o corpo real $\mathbb{R}$, determinando em primeiro lugar os que são algébricos sobre o corpo complexo.

Teorema 2.7

Seja $\mathbb{C}$ o corpo dos números complexos e suponhamos que o anel com divisão D seja algébrico sobre $\mathbb{C}$. Então $D = \mathbb{C}$.

Demonstração

Suponhamos que $a \in D$. Como D é algébrico sobre $\mathbb{C}$, $d_n a^n + d_{n-1} a^{n-1} + \ldots\ldots + d_1 a + d_o = 0$ para certos $d_o, d_1 \ldots\ldots d_n \in C$ e $d_n \neq 0$.

Ora o polinômio $p(x) = d_o + d_1 x + \ldots + d_n x^n$ em $\mathbb{C}[x]$, pelo lema 2.1 pode ser decomposto em $\mathbb{C}[x]$ num produto de fatores lineares, isto é, $p(x) = (x - b_1)(x - b_2) \ldots (x - b_n)$, onde $b_1, b_2, \ldots, b_n$ estão todos em $\mathbb{C}$.

Como $\mathbb{C}$ está no centro de D, todo elemento de $\mathbb{C}$ comuta com "a".

Logo $p(a) = (a - b_1)(a - b_2) \ldots (a - b_n)$.

Mas por hipótese $p(a) = 0$ e, então, temos

$(a - b_1)(a - b_2) \ldots (a - b_n) = 0$. Como um produto num anel com divisão é nulo, somente se um dos fatores do produto é nulo, concluimos que $a - b_k = 0$ para algum k, logo $a = b_k$, do que deduzimos que $a \in \mathbb{C}$. Portanto $D \subset \mathbb{C}$, como $\mathbb{C} \subset D$, concluimos que $D = \mathbb{C}$.

Teorema de Frobenius

Seja D um anel algébrico com divisão sobre o corpo $\mathbb{R}$, o corpo dos números reais. Então D é isomorfo a um dos três, o corpo dos números reais, o corpo dos números complexos ou o anel com divisão dos quatérnios reais.

Demonstração

Suponhamos que $D \neq \mathbb{R}$ e que $a \in D$, tal que $a \in \mathbb{R}$. Por hipótese "a" satisfaz algum polinômio sobre $\mathbb{R}$, logo algum polinômio irredutível sobre $\mathbb{R}$, pois $\mathbb{R}$ está no centro. Em consequência do lema 2.2, "a" satisfaz uma equação linear ou quadrática sobre $\mathbb{R}$. Se esta equação é linear, "a" está em $\mathbb{R}$, contrariando nossa hipótese.

Portanto, podemos supor que $a^2 - 2\alpha a + \beta = 0$ onde $\alpha, \beta \in R$. Assim $(a - \alpha)^2 = \alpha^2 - \beta$. Afirmamos que $\alpha^2 - \beta < 0$, pois, no caso contrário, teria uma raiz quadrada real "δ" e obteríamos $a - \alpha = \pm \delta$. Portanto, $a = \alpha \pm \delta$ e consequentemente $a \in R$ contrariando nossa hipótese. Segue-se que $\alpha^2 - \beta < 0$, logo pode ser escrito sob a forma "$-\gamma^2$", onde $\gamma \in \mathbb{R}$. De $(a - \alpha)^2 = -\gamma^2$ resulta que $(\frac{(a - \alpha)}{\gamma})^2 = -1$. Assim se $a \in \mathbb{R}$, podemos determinar α, γ reais, tais que $(\frac{a - \alpha}{\gamma})^2 = -1$.

Se D é comutativo, tomemos $a \in D$ e $a \notin \mathbb{R}$ e seja $i = \frac{a - \alpha}{\gamma}$, onde $\gamma, \alpha \in \mathbb{R}$ são escolhidos de modo que $i^2 = -1$.

Portanto, D contém R (i), um corpo isomorfo ao corpo dos números complexos. Como D é comutativo e algébrico sobre $\mathbb{R}$ é, com mais razão, algébrico sobre $\mathbb{R}$ (i). Pelo teorema 2.7, concluimos que $D = \mathbb{R}$ (i). Assim se D é comutativo, ele é $\mathbb{R}$ ou $\mathbb{R}$ (i). Admitamos que D não seja comutativo. Afirmamos que o centro de D é exatamente $\mathbb{R}$. Se não o fosse, haveria um "a" no centro mas não em $\mathbb{R}$. Portanto, para certos $\alpha, \gamma \in \mathbb{R}$, $(\frac{a - \alpha}{\gamma})^2 = -1$, de modo que o centro contém um corpo dos números complexos. Contudo, pelo teorema 2,7, se os números complexos (ou um isomorfo dele) estivessem no centro de D, então $D = \mathbb{C}$, forçando D a ser comutativo.

Logo $\mathbb{R}$ é o centro de D.

Seja $a \in D$ e $a \notin \mathbb{R}$, para certos $\alpha, \gamma \in \mathbb{R}$

$i = \frac{a - \alpha}{\gamma}$ satisfaz $i^2 = -1$. Como $i \notin \mathbb{R}$, "i" não está no centro de D. Portanto, existe um elemento $b \in D_2$, tal que $c = b\,i - i\,b \neq 0$. Então $i\,c + c\,i =$

$$= i\,b\,i - i^2\,b + b\,i^2 - i\,b\,i =$$

$$= i\,b\,i + b - b - i\,b\,i = 0$$

Assim $i\,c = -\,c\,i$, como consequência

$i\,c^2 = (i\,c)\,c = (-c\,i)\,c = -c\,(i\,c) = -c\,(-c\,i) = c^2\,i$,

e, então, c^2 comuta com i. Ora "c" satisfaz alguma equação quadrática sobre $\mathbb{R}$ $c^2 + \alpha\,c + \mu = 0$. Como c^2 e μ comutam com i, $\alpha\,c$ comuta com i, consequentemente temos:

$$(\alpha\,c)\,i = i\,(\alpha\,c) = \alpha\,i\,c = \alpha\,(-c\,i) = -\alpha\,c\,i$$

logo $2\,\alpha\,c\,i = 0$; como $2\,c\,i = 0$, temos que $\alpha = 0$. Assim $c^2 + \mu = 0$, logo $c^2 = -\mu$. Como $c \notin \mathbb{R}$, visto que $c\,i = -c\,i$, podemos dizer, como o fizemos anteriormente, que "μ" é positivo e então $\mu = \nu^2$, $\nu \in \mathbb{R}$.

Portanto $c^2 = -\nu^2$, seja $j = \frac{c}{\nu}$

Então j satisfaz

$$(1)\quad j^2 = \left(\frac{c}{\nu}\right)^2 = \frac{c^2}{\nu^2} = -1$$

$$(2)\quad j\,i + i\,j = \frac{c}{\nu}\,i + i\,\frac{c}{\nu} = \frac{c\,i + i\,c}{\nu} = \frac{0}{\nu} = 0$$

Seja $k = i\,j$. Os elementos i, $j \notin \mathbb{R}$ que construimos comportam-se como os quaternios, logo:

$$T = \{d_0 + d_1\,i + d_2\,j + d_3\,k \mid d_0, d_1, d_2, d_3 \in \mathbb{R}\}$$

T é um subanel com divisão isomorfa aos quatérmios reais.

Provaremos que 1, i, j, k, definidos acima, são linearmente independentes.

Suponhamos que (II) $\alpha + \beta\,i + \gamma\,j + \delta\,k = 0$

onde $\alpha, \beta, \gamma, \delta \in \mathbb{R}$. Multiplicando (II) por i, j, k, respectivamente, obteremos

$$\begin{aligned}
\alpha + \beta\,i + \gamma\,j + \delta\,k &= 0\\
-\beta + \alpha\,i - \delta\,j + \gamma\,K &= 0\\
-\gamma + \delta\,i + \alpha\,j - \beta\,k &= 0\\
-\delta - \gamma\,i + \beta\,j + \alpha\,k &= 0
\end{aligned}$$

Se o sistema acima só tem a solução trivial nas variáveis α, β, γ, δ, ótimo, temos o que queríamos.

Suponhamos, portanto, que o sistema tenha solução não trivial. Ora, isto significa que:

$$\begin{vmatrix} \alpha & \beta & \gamma & \delta \\ -\beta & \alpha & -\delta & \gamma \\ -\gamma & \delta & \alpha & -\beta \\ -\delta & -\gamma & \beta & \alpha \end{vmatrix} = 0$$

Desenvolvendo o determinante pela primeira linha obteremos:

$$\alpha \begin{vmatrix} \alpha & -\delta & \gamma \\ \delta & \alpha & -\beta \\ -\gamma & \beta & \alpha \end{vmatrix} \quad -\beta \begin{vmatrix} -\beta & -\delta & \gamma \\ -\gamma & \alpha & -\beta \\ -\delta & \beta & \alpha \end{vmatrix} \quad +$$

$$+\gamma \begin{vmatrix} -\beta & \alpha & \gamma \\ -\gamma & \delta & -\beta \\ -\delta & -\gamma & \alpha \end{vmatrix} \quad -\delta \begin{vmatrix} -\beta & \alpha & -\delta \\ -\gamma & \delta & \alpha \\ -\delta & -\gamma & \beta \end{vmatrix} = 0$$

Ou seja:

$$\alpha\,(\alpha^3 + \beta\gamma\delta - \beta\gamma\delta + \alpha\gamma^2 + \alpha\delta^2 + \alpha\beta^2) -$$
$$-\beta\,(-\alpha\beta^2 - \beta\gamma^2 - \beta\delta^2 + \alpha\gamma\delta - \alpha\gamma\delta - \beta^3) -$$
$$-\gamma\,(-\alpha\beta\delta + \gamma^3 + \alpha\beta\delta + \gamma\delta^2 + \gamma\beta^2 + \gamma\alpha^2) -$$
$$-\delta\,(-\delta\beta^2 - \delta\gamma^2 - \delta\alpha^2 - \delta^3 + \alpha\gamma\beta - \alpha\gamma\beta) = 0$$

Logo:

$$\alpha^2\,(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) + \beta^2\,(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) +$$
$$+\gamma^2\,(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) + \delta^2\,(\alpha^2 + \beta^2 + \gamma^2 + \delta^2) = 0$$

Portanto:

$(\alpha^2 + \beta^2 + \gamma^2 + \delta^2)^2 = 0$ resultando

$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 0$ e, consequentemente,

$\alpha = \beta = \gamma = \delta = 0$ e chegamos ao que queríamos.

Portanto, 1, i, j, k são linearmente independentes.

Produzimos uma réplica T do anel com divisão dos quatérnios reais em D.

Nosso último objetivo é demonstrar que T = D.

Se $r \in D$ satisfaz $r^2 = -1$.

Seja $N(r) = \{x \in D \mid x\, r = r\, x\}$

Vemos facilmente que N (r) é um subanel com divisão; além disso, "r" e, portanto, todos os $d_0 + d_1 r$, $d_0, d_1 \in \mathbb{R}$, estão no centro de N (r).

Pelo teorema 2.7 segue-se que

$N(r) = \{d_0 + d_1 r \mid d_0, d_1 \in \mathbb{R}\}$, pois

$\{d_0 + d_1 r \mid d_0, d_1, \in \mathbb{R}\} = \mathbb{R}[r] \cong \mathbb{C}$.

Assim, se $r\, x = x\, r$, então $x = d_0 + d_1 r$ para certos $d_0, d_1 \in \mathbb{R}$.

Suponhamos que $\mu \in D$ e $\mu \notin \mathbb{R}$. Para certos $\alpha, \beta \in R$ $w = \frac{\mu - \alpha}{\beta}$ satisfaz $w^2 = -1$. Afirmamos que $w\, i + i\, w$ comuta com "w" e com "i". De fato:

$$(w\, i + i\, w)\, w = w\, i\, w + i\, w^2 = w\, i\, w - i =$$
$$= w\, i\, w + w^2\, i = w\, i\, w + w\, w\, i =$$
$$= w\,(i\, w + w\, i)$$

$$(w\, i + i\, w)\, i = w\, i^2 + i\, w\, i = -w + i\, w\, i =$$
$$= i^2\, w + i\, w\, i = i\,(i\, w) + i\, w\, i =$$
$$= i\,(w\, i + i\, w)$$

Pela observação do parágrafo anterior,

$$w\, i + i\, w = d_0' + d_1' i = d_0 + d_1 w.$$

Se $w \notin T$, esta última relação implica que $d_1 = 0$, pos caso contrário $w = (d_0' - d_0)/d_1 + d_1'/d_1\, i$ e, portanto, poderíamos resolver w em dunção de i.

Assim: $w\, i + i\, w = d_0 \in \mathbb{R}$. Analogamente

$$w\,j + j\,w = \beta_0 \in \mathbb{R}.$$

$$w\,k + k\,w = \gamma_0 \in \mathbb{R}.$$

Seja $z = w + \frac{d_0}{2}\,i + \frac{\beta_0}{2}\,j + \frac{\gamma_0}{2}\,k$, então

$$z\,i + i\,z = w\,i + \frac{d_0}{2}\,i^2 + \frac{\beta_0}{2}\,j\,i + \frac{\gamma_0}{2}\,k\,i +$$

$$+ i\,w + \frac{d_0}{2}\,i^2 + \frac{\beta_0}{2}\,i\,j + \frac{\gamma_0}{2}\,i\,k =$$

$$= w\,i + i\,w + \frac{d_0}{2}\,(i^2 + i^2) + \frac{\beta_0}{2}\,(i\,j + j\,i) +$$

$$+ \frac{\gamma_0}{2}\,(k\,i + i\,k) =$$

$$= d_0 - d_0 + \frac{\gamma_0}{2}\,(i\,j\,i + i\,i\,j) =$$

$$= \frac{\gamma_0}{2}\,(-i^2\,j + i^2\,j) = 0$$

Analogamente: $z\,j + j\,z = 0$

$z\,k + k\,z = 0$

Destas relações, obtemos $z = 0$. De fato:

$$0 = z\,k + k\,z = z\,i\,j + i\,j\,z =$$
$$= z\,i\,j + i\,z\,j - i\,z\,j + i\,j\,z =$$
$$= (z\,i + i\,z)\,j + i\,(-z\,j + j\,z).$$

Contudo, $i \neq 0$ e, como estamos num anel com divisão, segue-se que

$$z\,j - j\,z = 0, \quad \text{Mas } z\,j + j\,z = 0.$$

Logo $2zj = 0$, como $2j \neq 0$, pelo mesmo raciocínio acima, temos necessariamente $z = 0$.

Portanto: $0 = z = w + \frac{d_0}{2}\,i + \frac{\beta_0}{2}\,j + \frac{\gamma_0}{2}\,K$

donde $w = (-\frac{d_0}{2})\,i + (\frac{-\beta_0}{2})\,j - (\frac{-\gamma_0}{2})\,k$

e $w \in T$, contradizendo $w \notin T$. Assim temos $w \in T$. Como

$$w = \frac{\mu - \alpha}{\beta} \qquad \mu = \beta w + \alpha \quad \text{e, então, } \mu \in T.$$

Demonstramos que todo elemento em D está em T. Como $T \subset D$, concluímos que $D = T$. Desde que T é isomorfo aos quatérnios reais, obtemos agora que D é isomorfo ao anel com divisão dos quatérnios reais.

C A P Í T U L O 3

CLASSIFICAÇÃO DAS ÁLGEBRAS COM DIVISÃO SOBRE OS REAIS SEGUNDO R.S. PALAIS

Seja D uma álgebra com divisão de dimensão finita sobre o corpo dos números reais $\mathbb{R}$.

Uma maneira de estabelecer o teorema fundamental da álgebra, é dizer que se D é comutativo (isto é, um corpo), então D é isomorfo sobre os reais ou a $\mathbb{R}$ ou ao corpo dos números complexos $\mathbb{C}$. Um famoso teorema de *Frobenius* (demonstrado no capítulo 2) assegura que se D é não comutativo, então existe uma única possibilidade, ou seja, D é isomorfo sobre $\mathbb{R}$, a álgebra dos quatérnios de *Hamilton*. Esta é uma álgebra Q, de dimensão quatro, gerada como um espaço vetorial pela base de elementos 1, i, j, k que satisfazem a seguinte tábua de multiplicação:

$$i^2 = j^2 = k^2 = -1$$
$$ij = -ji = k$$
$$jk = -kj = i$$
$$ki = -ik = j$$

A prova é conceitual e elementar simultaneamente. Ao lado do inevitável uso do teorema fundamental da álgebra, usaremos somente fatos simples sobre os auto valores de transformações lineares.

Notemos, primeiramente, que o subespaço de Q de dimensão dois, gerado por "1" e "i", é isomorfo aos números complexos. Q é um espaço vetorial sobre $\mathbb{C}$ (usando a multiplicação à esquerda por uma operação escalar).

Além disso, $\mathbb{C}$ é claramente $\{x \in D \mid xi = ix\}$, en-

quanto que o espaço complementar bi-dimensional, gerado por "j" e "k", é justamente $\{x \in D \mid xi = -ix\}$.

Estas observações é que vão motivar nossa prova.

Seja "1" denotando o elemento unidade de D. Podemos pensar em $\mathbb{R}$ embebido em D pela aplicação $x \longrightarrow x \cdot 1$
Podemos assumir $D \neq \mathbb{R}$.
Seja "d" um elemento de D, mas que não esteja em $\mathbb{R}$ e seja $\mathbb{R}<d>$, denotando o subespaço vetorial bi-dimensional gerado por "1" e "d", $\mathbb{R}<d> = \mathbb{R} + \mathbb{R}.d$.

Lema 3.1

$\mathbb{R}<d>$ é um subconjunto maximal comutativo de D, consistindo de todos os elementos de D que comutam com "d". Além disso é um corpo isomorfo a C.

Existência de uma subálgebra A de D da dimensão maximal, que inclui $\mathbb{R}<d>$ e é comutativa.

Lema 3.2

Toda cadeia estritamente crescente de subespaços vetoriais em D é de comprimento finito.

Demonstração

Seja $0 \neq V_1 \subsetneq V_2 \subsetneq \ldots \subsetneq V_n$

com V_1 subespaços vetoriais de D, $i = 1, 2, \ldots n$

$$V_1 \underset{\mathbb{R}}{\leqslant} D$$

Seja $0 \neq d_1 \in V_1$, $d_2 \in V_2 \setminus V_1$, $\ldots$, $d_i \in V_i \setminus V_{i-1}$

Vamos provar que $\{d_1, d_2, \ldots, d_n\}$ são linearmente independentes.
Seja $c_1d_1 + c_2d_2 + \ldots + c_nd_n$, tal que $_i = 1, 2, \ldots, n$, $c_i \in \mathbb{R}$

e "t" o primeiro índice, tal que $c_t \neq 0$.

Então $c_t d_t = -c_1 d_1 - c_2 d_2 - \ldots - c_{t-1} d_{t-1}$

$$d_t = (\frac{-c_1}{c_t}) d_1 + (\frac{-c_2}{c_t}) d_{2t} \ldots + (\frac{-c_{t-1}}{c_t}) d_{t-1}$$

Como para i = 1, 2, ..., t-1

$$d_i \quad V_i \subseteq V_{t-1}$$

temos que $d_i \in V_{t-1}$, $V_i = 1, 2, \ldots, t-1$

Logo $d_t = \sum_{i-1}^{t-1} (\frac{-c_i}{t}) d_i \quad \varepsilon \quad V_{t-1}$

o que é absurdo.

Portanto, $c_i = 0$, e os d_i são linearmente independentes e $n \leq \dim_{\mathbb{R}} D$

Corolário 3.3

Seja $\mathbb{R} \langle d \rangle \subsetneq A_1 \subsetneq A_2 \ldots \subsetneq A_n \subseteq D$

onde A_i são $\mathbb{R}$ - subálgebras de D, então $n \leq \dim_{\mathbb{R}} D$

Demonstração

Como sabemos, se A é $\mathbb{R}$ - subálgebra de D, então A é $\mathbb{R}$ - subespaço vetorial de D.
Portanto, $A_1 \subsetneq A_2 \subsetneq A_3 \subsetneq \ldots \subsetneq A_n$ é cadeia estritamente crescente de $\mathbb{R}$ - subespaços vetoriais de D. Pelo lema 3.2 $n \leq \dim_{\mathbb{R}} D$.

Daremos a seguir o lema que usaremos e que é de fácil demonstração, sendo portanto deixado ao leitor mais interessado demonstrá-lo.

Lema 3.4

Seja B $\mathbb{R}$ - álgebra e A $\subseteq$ B, A $\mathbb{R}$ - subálgebra de B.

$$A[x] = \{ \sum_{i=0}^{n} a_i x^i \mid n \in z^+ \cup \{0\},\ a_i \in A \}$$

Se $x \in B$ comuta com A, então:

(1) $A[x]$ é fechado em relação à soma e multiplicação de D. Logo $A[x]$ é $\mathbb{R}$ - subálgebra de D.

($x + y \in A[x]$, $x - y \in A[x]$, $xy \in A[x]$.

qualquer que seja $x, y \in A[x]$).

(2) Se x comuta com A, então A é comutativo; assim sendo, $A[x]$ também é comutativo.

Concluimos que $A[x]$ é uma $\mathbb{R}$ - subálgebra de B comutativa.

Colorário 3.5

Existe uma $\mathbb{R}$ - subálgebra de D maximal.

Demonstração por construção.

$\mathbb{R} < d > \subseteq \mathbb{R}[d]$.

Se $\mathbb{R} < d >$ não é maximal, existe $A_1 \neq D$, tal que $\mathbb{R} < d > \subsetneq A_1 \subsetneq D$, A_1 $\mathbb{R}$ - subálgebra de D.

Se A_1 não é maximal, existe $A_2 \neq D$ tal que $\mathbb{R} < d > \subsetneq A_1 \subsetneq A_2 \subsetneq D$

Assim pode-se construir $A_1 \subsetneq A_2 \subsetneq \ldots \subsetneq A_i$.

Pelo corolário 3.3, como temos uma cadeia estritamente crescente de $\mathbb{R}$ - subálgebras de D, existe um índice "t", tal que o processo pare em t.

Portanto, $\mathbb{R} < d > \subseteq A_1 \subsetneq A_2 \subsetneq \ldots \subsetneq A_t \subsetneq D$

e A_t é maximal.

Demonstração do lema 3.1

Escolhendo uma subálgebra A de D de dimensão maximal, que inclui $\mathbb{R} < d >$ e é comutativa.

Se $x \in D$ comuta com todos elementos de A, então $A[x]$ é comutativo e $A[x]$ deve ser igual a A, pois temos:

$A \subseteq A[x] \subseteq D$, $A[x]$ $\mathbb{R}$ - subálgebra comutativa de D. Como A é maximal entre as R - subálgebras comutativas de D, segue-se que

$$A = A[x] \quad \text{ou} \quad A[x] = D.$$

Ora, $A[x] = D$ é absurdo, pois D não é comutativo; logo $A = A[x]$ e $x \in A$. Em particular, se $x \neq 0$, "x" comuta com A, então x^{-1} comuta com todos os elementos de A (pois $xy = yx$ se, e somente se, $yx^{-1} = x^{-1}y$) e portanto $x^{-1} \in A$.

Concluimos que $x \in A$, $x \neq 0$ implica que $x^{-1} \in A$. Então A é corpo.

Pelo *Teorema Fundamental da Álgebra*, A é isomorfo a $\mathbb{C}$ sobre $\mathbb{R}$.

Em particular, como $\dim_{\mathbb{R}} A = d$, $\dim_{\mathbb{R}} \mathbb{R} < d > = d$ e $\mathbb{R} < d > \subseteq A$, segue-se que $\mathbb{R} < d > = A$.

Finalmente, se $x \in D$ comuta com "d", ele comuta com todos os elementos de $\mathbb{R} < d > = A$, portanto pertence a $\mathbb{R} < d >$.

De acordo com o lema 3.1, podemos escolher um elemento "i" $\in D$, tal que $i^2 = -1$ e podemos identificar $\mathbb{R} < i >$ com $\mathbb{C}$.

Olhamos, agora, D não meramente como um espaço vetorial sobre $\mathbb{R}$, mas também como um espaço vetorial sobre $\mathbb{C}$, bem como uma operação escalar de $\mathbb{C}$ em D, como uma multiplicação à esquerda. Por outro lado, a multiplicação à direita por "i", pode ser interpretada como uma transformação linear (complexa) T, sobre o espaço vetorial (complexa) T, sobre o espaço vetorial (complexo) D, isto é, definimos.

Definição 3.6

$Tx \equiv xi$

Desde que $T^2x = TTx \equiv Txi \equiv (xi)i = -x$, segue-se que $T^2 = -(\text{Identidade})$ e os únicos auto valores de T são $+i$ e $-i$.

Denotando por D^+ e D^- os correspondentes auto-espaços, temos:

Definição 3.7

$D^+ = \{x \in D \mid xi = ix\} = \mathbb{R} < i >$

$D^- = \{x \in D \mid xi = -ix\}$

Naturalmente $D^+ \cap D^- = \{0\}$. Seja $x \in D^+$, $x \in D^-$; como $xi = -xi$, temos que $2xi = 0$. Desde que $2i \neq 0$ e estamos numa álgebra com divisão, concluimos que $x = 0$.

Lema 3.8

$D = D^+ \oplus D^-$

Demonstração

Segue-se imediatamente da decomposição:

$x = \frac{1}{2}(x - ixi) + \frac{1}{2}(x + ixi), \forall x \in D$

onde $x - ixi \in D^+$ e $x + ixi \in D^-$, pois,

$(x - ixi)i = xi - ixi^2 = xi + ix$ e

$i(x - ixi) = ix - i^2xi = xi + ix$

Também

$(x + ixi)i = xi + ixi^2 = xi - ix$ e

$i(x + ixi) = ix + i^2xi = ix - xi = -(xi - ix)$

Lema 3.9

$D^+ = \mathbb{C}$ e $x, y \in D^-$ implica $xy \in D^+$.

Demonstração

$D^+ = \mathbb{C}$, segue-se imediatamente do lema 3.1 com d = i

Da definição 3.7, x, y ε D^- implica xy ε D^+, pois

$$x(y\ i) = x(-i\ y) = -(x\ i)y = i\ x\ y$$

De $D^- = \{0\}$, então, pelos lemas 3.8 e 3.9, temos $D = \mathbb{C}$.

Portanto, podemos assumir que $D^- \neq \{0\}$ e mostraremos que D deve ser isomorfo a Q. Primeiro, mostraremos que sobre os reais a dimensão de D é quatro, isto é, sobre D^+ (corpo isomorfo a $\mathbb{C}$), D é de dimensão dois, como veremos a seguir:

Lema 3.10

$$\dim_{D^+} D^- = 1 \text{ e } \dim_{\mathbb{R}} D = 4$$

D^- é D^+ - espaço vetorial ($x \in D^+ = \mathbb{C}$, $y \in D^-$ implica $x\ y \in D^-$)

Demonstração

Escolheremos qualquer elemento "a" ≠ 0, a ε D^-.

Então a multiplicação à direita por "a" dá uma transformação linear sobre D^+, que é não singular (sua inversa é uma multiplicação à esquerda por a^{-1}). Podemos construir um isomorfismo entre D^- e D^+, assim definido:

$$D^- \xrightarrow[T]{D^+ - \text{iso}} D^+$$

T aplicação linear definida por Tx = x a

pois $T(x + cy) = (x + cy)a = xa + cya =$

$$= T(x) + cT(y).$$

Então $D^+ \cong D^-$ sobre D^+

Logo $\dim_{D^+} D^- = \dim_{D^-} D^+ = 1$

$$\dim_{D^+} D = \dim_{D^+} D^+ + \dim_{D^+} D^- = 1 + 1 = 2$$

Portanto $\dim_{\mathbb{R}} D = (\dim_{D} D)\ (\dim_{\mathbb{R}} D^{+}) = 2 \cdot 2 = 4$

Lema 3.11

Seja "a" do lema 3.10. Então (1) $a^2 \in R$
(2) $a^2 < 0$

Demonstração

Pelo lema 3.1 $\mathbb{R} < a >$ é um corpo contendo a^2, mas também pelo lema 3.9, desde que $a \in D^{-}$, $a^2 = a \cdot a \in D^{+}$. Portanto, $a^2 \in D^{+} \cap \mathbb{R} < a >$ e veremos facilmente que $D^{+} \cap \mathbb{R} < a > = \mathbb{R}$. Senão vejamos. Seja $r_0 + r_1 a \in D^{+} \cap \mathbb{R} < a >$, tal que

$r_0, r_1 \in \mathbb{R}$ e $a \in D^{-}$. Então

$i\ (r_0 + r_1 a) = (r_0 + r_1 a)i$, logo

$ir_0 + ir_1 a = r_0 i + r_1 ai$. Portanto

$ir_1 a = r_1 ai = r_1(-ia) = -ir_1 a$

Segue-se que $2ir_1 a = 0$ e portanto $r_1 = 0$. Se $a^2 > 0$, ele tem duas raizes quadradas em $\mathbb{R}$, portanto três raizes quadradas no corpo $\mathbb{R} < a >$ (existe "d" raiz tal que $d \in \mathbb{R} < a >$, $d \notin \mathbb{R}$), que é impossível pela teoria dos corpos. Portanto $a^2 < 0$ e existe um $r \in \mathbb{R}$ tal que

$$a^2 = -r^2, \text{ logo } \left(\frac{a}{r}\right)^2 = \frac{a^2}{r^2} = -1. \quad \text{Seja } j = \frac{a}{r}.$$

Pelo lema 3.11, um possível múltiplo real positivo de "a" é um elemento $j \in D^{-}$ satisfazendo $j^2 = -1$.

Definindo $k = ij \in D^{-}$, temos $(ij)i = -i(ij)$.

Desde que "a", "j" e "k" $\in D^{-}$ e como $\{j, k\} \xrightarrow{j} \{-1, -i\}$ base de D^{+} sobre $\mathbb{R}$, vemos que "j" e "k" formam uma base de D sobre $\mathbb{R}$. Portanto, pelo lema 3.8, os elementos 1, i, j, k formam uma base de D sobre $\mathbb{R}$.

Desde que $j, k \in D^{-}$, eles não comutam com i. Juntamente com

$$i^2 = j^2 = -1$$

$$k^2 = (ij)\ (ij) = ij(-ji) =$$
$$= -ij^2i = i^2 = -1$$

$$ij = -ji = k$$
$$jk = jij = -jji = -j^2i = i$$
$$Kj = ijj = ij^2 = -i$$

$$ki = iji = i(-ij) = -i^2 = j$$
$$ik = iij = i^2j = -j$$

Vemos que 1, i, j, k satisfazem a tabela multiplicativa dada para os quatérnios reais.

C A P Í T U L O 4

CO-EXTENSÕES DE CO-DIMENSÃO FINITA SOBRE OS NÚMEROS COMPLEXOS

Definição 4.1

Co-extensão de um corpo K é um corpo $E \subseteq K$.

Definição 4.2

Co-dimensão de uma co-extensão $E \subseteq K$ é $[K : E]$.

Teorema 4.3

Seja F um corpo algebricamente fechado e M um subcorpo que é de co-dimensão finita em F. Então $F = M(\sqrt{-1})$.

Demonstração

Seja $L = M(\sqrt{-1}) \subseteq F$, temos $[F : L] < +\infty$
Devemos mostrar que L = F. Portanto, podemos supor, sem perda de generalidade, que $L \neq F$.

Definição 4.4

Um corpo K é perfeito se a característica de K é zero ou é $p \neq 0$ e $K^p = K$.

Lema 4.5

L é perfeito.

Demonstração

Podemos supor sem perda de generalidade que
Car (L) = $p \neq 0$.

Suponhamos que existe um elemento $b \in L$ que não é uma p-ésima potência de um elemento de L. Então, para cada $n > 0$ $x^{p^n} - b$ é irredutível em $L[x]$ pelo teorema 4.5.2. Isto mostra a existência de uma extensão algébrica de L de dimensão p^n sobre L. Desde que "n" é arbitrário, isto contradiz o que nós admitimos. Pois sendo F algebricamente fechado, existirá um "a_n" T tal que a_n é raiz de

$$x^{p^n} - b \in F[x]$$

Ora $L \subseteq L(a_n) \subseteq F$, então

$$[L(a_n) : L] \mid [F : L] < +\infty$$

Portanto, $[L(a_n) : L]$ é limitada $\forall_n$.

Mas $[L(a_n) : L] = p^n$, que tende para o infinito, o que é absurdo.

Portanto não existe "b", que não é uma p-ésima potência em L. Segue-se que L é perfeito.

Definição 4.6

P é separável sobre K se qualquer que seja $g(x) \in K[x]$ irredutível, tal que "g" tem raiz em P, temos que $g' \neq 0$, onde P e K são corpos.

Lema 4.7

F/L é separável.

Demonstração

De fato, F/L perfeito implicará F/L separável. Suponhamos sem perda de generalidade que car (L) = $p \neq 0$.

Seja $g(x) \in L[x]$ irredutível sobre L.

Se $g' = 0$, então "p" divide os expoentes de g(x) que tenham coeficientes não nulos.

Logo $g(x) = f(x^p)$ e $f(x) \in L[x]$.

Mas $f(x) = h^p(x)$ onde $h(x) \in L[x]$ e como $L^p = L$.

Portanto, $g(x) = h^p(x^p) = (h(x))^p$, $h(x) \in L[x]$, o que é absurdo.

Definição 4.8

P/K é normal se $f(x) \in K[x]$ irredutível e "a" $\in P$, tal que $f(a) = 0$, implica que todas as raizes de $f(x) \in P$.

Lema 4.9

T é normal sobre L.

Demonstração

Trivialmente, pois F é algebricamente fechado.

Lema 4.10

T/L é *Galois*, quer dizer F/L é finito, normal e separável.

Demonstração

Segue-se dos lemas 4.7 e 4.9.

Continuação da prova do teorema 4.3. Seja G o grupo de *Galois* de F sobre L.

$$|G| = [F : L] \neq 1 \text{ pois } L \neq F.$$

Segue-se que G é diferente de um.
G contêm um subgrupo H cíclico de ordem prima "q".

Seja $E = F^H$. Pela teoria de *Galois* $[F : F^H] = |H| = q$, logo

$$[F : E] = q.$$

Claramente as únicas extensões algébricas de E são E e F.
Como "q" é primo, segue-se que a característica de M não é q. Pois, se assim acontecer, F será uma q-extensão cíclica de E de característica q. A existência de tal extensão de E implicará na existência de *extensões de Galois cíclicas* de E, de grau q^n, $\forall_{n \geq 1}$, pelo Teorema 4.5.3.

Seja E_n extensão de Galois cíclica de E, de grau q^n. Como E_n/E é Galois, isto implica que $E_n = E(a)$. Então "a" é algébrico sobre E de grau q^n. O polinômio minimal, $f_n(x)$, de "a" sobre E pertence a E x e tem grau q^n, e também é irredutível.

Seja b_n raiz de $f_n(x)$ em F. Segue-se que $[E(b_n) : E] = q^n$, que vai para o infinito com n, o que é absurdo, pois como
$E \quad E(b_n) \quad F$, $E(b_n) : E \mid F : L < +\infty$. Concluimos que

$V_n > 1$, $E(b_n) : E$ é limitada.

Portanto, $car(M) \neq q$

Isto implica que F, algebricamente fechado, contém "q" distintas raizes de 1, pois $(x^q - 1)' = q\, x^{q-1} \neq 0$.

Seja $a \in F$ com $a^q - 1 = 0$

Desde que $a^q - 1 = (a - 1)(a^{q-1} + a^{q-2} + \ldots + a + 1) = 0$
$a = 1$ ou $a^{q-1} + a^{q+2} + \ldots + a + 1 = 0$

Portanto $E(a) : E < q - 1$.
Como $E(a) : E \mid F : E = q$,
temos $E(a) : E = 1$ e $a \in E$.

Segue-se que todas as q-ésimas raizes de 1, estão contidas em E. Como F é cíclico sobre E de dimensão q, pelo teorema 4.5.4 existe $\alpha \in E$ tal que $F = E(\sqrt[q]{\alpha})$.

Consideremos o polinômio $g(x) = \prod_{i=1}^{q^2} (x - a^i b)$, onde "a" é uma q^2 - raiz primitiva de 1 e "b" é um elemento de F, tal que $b^{q^2} = \alpha$.
Como a inclusão $a^i b \in E$ implica que E contém um elemento $(a^i b)^q = \beta$, tal que $\beta^q = (a^i b)^{q^2} = (a^i)^{q^2} b^{q^2} = (a^{q^2})^i \alpha = \alpha$, vemos que nenhum $a^i b \in E$ $(1 < i < q^2)$, pois teriamos $\frac{\sqrt[q]{\alpha}}{\beta}$ uma q-ésima raiz de 1. Portanto $\frac{\sqrt[q]{\alpha}}{\beta} \in E$ e então $\sqrt[q]{\alpha} \in E$, absurdo. Desde que $g(x) = x^{q^2} - \alpha$ pertence a E x , segue-se que g(x) não é irredutível em E x .
Seja $g = g_1 \cdot g_2 \cdots g_t$, g_i irredutíveis em E x .

Seja $r \in F$ tal que $g_i(r) = 0$.

Como $E \subseteq E(r) \subseteq F$ e $[F : E] = q$, segue-se que $E(r) = E$ ou $E(r) = F$. Ora $E(r) = E$ implica que $r \in E$. Isto é, um absurdo, pois nenhuma raiz de $g(x)$ está em E.

Logo $E(r) = F$ e como consequência grau $g_i(x) = q$.

Portanto $g_1 = \prod_{i \in S} (x - a^i b)$ onde

$S \subseteq \{1, \ldots, q^2\}$ e $|S| = q$.

Se β é o termo constante de $g_1(x)$, então $\beta = b^q c$, onde "c" é uma potência de "a". Como $(b^q)^q = \alpha$, temos $b^q = e\sqrt[q]{\alpha}$ onde "e" é uma q-ésima raiz de 1. Portanto $F = E(\sqrt[q]{\alpha}) = E(b^q)$. Segue-se que $F = E(b^q) = E(\beta b^{-q})$ pois $\beta \in E$.

Desde que $\beta^{-q} = c$, concluimos que $F = E(c)$.

Como E contém todas as q-ésimas raizes de 1, vemos que "c" é uma q^2 - raiz primitiva de 1.

Seja M_o um corpo primo de F e consideremos o sub - corpo $M_o(c)$ de F.

Se M_o é o corpo R_o dos números racionais, sabemos que a dimensionalidade do corpo das q^m - raizes de 1 é $\phi(q^m)$ teorema 4.5.5 e isto vai para o infinito com "m".

Se M_o tem característica p, então $p \neq q$ e o corpo das q^m-ésimas raizes de 1 sobre M_o contém pelo menos q^m-elementos. Novamente a dimensionalidade deste corpo sobre M_o aproxima-se do infinito com "m". Em qualquer caso, segue-se que existe um inteiro positivo "m", tal que $M_o(c)$ contém uma q^m-ésima raiz primitiva, mas não a q^{m+1}-ésima primeira raiz primitiva de 1.

Como "c" é uma Q^2-raiz primitiva de 1, $m \geq 2$. O corpo F contém uma q^{m+1}-ésima primeira raiz primitiva de 1, digamos "d" (d^q é uma q^m raiz primitiva de 1).

Seja h(x) o polinômio minimal de "d" sobre E. Desde que "c" $\notin$ E e existe "i", tal que $d^i = c$, $d \notin E$. Ademais o grau de h(x) é

igual a "q". Também h(x) é um fator de $x^{q^{m+1}} - 1 = \prod_{i=1}^{q^{m+1}} (x - d^i)$

Além disso, os coeficiente de h(x) estão contidos em $M_o(d)$. Portanto, eles estão contidos no corpo $N = M_o(d) \cap E$.

Segue-se que h(x) é irredutível sobre $N \subseteq E$ e $[M_o(d) : N] = q$.

A seguir consideremos o subcorpo $N_1 = M_o(t)$, onde $t = d^q$, de $M_o(d)$. Evidentemente "t" é uma q^m-ésima raiz primitiva de 1. Ademais, N_1 contém "q" distintas q-ésimas raizes de 1. Pois se z é uma q^l-ésima raiz de 1 com $i \leq m$, então $z \in \langle t \rangle$ e existe "j" tal que $t^j = z$.
Por outro lado $M_o(d) = N_1(d)$ e $N_1 \subseteq M_o(d)$ onde $d^q = t \in N_1$.

Vemos facilmente que $M_o(d) \neq N_1 = M_o(t)$. Pois como $M_o(t) \subset M_o(d)$ e desde que $M_o(c)$ contém todas as q^m-ésimas raizes de 1 por definição, $M_o(c)$ então conteria "d" uma q^{m+1}-ésima primeira raiz primitiva de 1, contrariando nossa hipótese.

Demonstraremos que $M_o(d)$ é cíclico de dimensão "q" sobre N_1.

Seja $\prod_{i=1}^{q} (x - v^i d) = X^q - t \in N_1[x]$, onde "v" é uma q-ésima raiz primitiva de 1. Isto é separável, então $M_o(d) / N_1$ é Galois. Calculemos $[M_o(d) : N_1]$.

Seja f(x) o polinômio minimal de "d" sobre N_1. Temos
$f(x) \mid x^q - t = \prod_{i=1}^{q} (x - v^i d)$, "v" é uma q-ésima raiz primitiva de 1. O termo constante de f é igual a $\pm v^j d^\ell \in N_1$ com grau $f(x) = \ell \leq q$.

Como $t \in N_1$, $v^j \in N_1$ e consequentemente $d^\ell \in N_1$. Se $\ell < q$, então $o(d^\ell) = o(d)$. Portanto d^ℓ é uma q^{m+1}-ésima raiz primitiva de 1.

Em vista disto, existe "i" tal que $d = (d^\ell)^i \in N_1 \subseteq M_o(c)$, absurdo, pois $N_1 \subseteq M_o(c) \not\subseteq M_o(d)$.

Logo $\ell = q$ e $[M_o(d) : N_1] = q$.

Então $M_o(d) / N_i$ é Galois cíclico.

Agora $N_1 \neq N$.

Pois se $N_1 = N$. Então $t \in N \subsetneq E$ e $t \in E$, mas existe "i" tal que $c = t^i$ e como "t" é uma q^m-ésima raiz primitiva de 1 e $m \geq 2$, e "c" é uma q^2-ésima raiz primitiva de 1, segue-se que $c \in E$, absurdo.

Provamos que o corpo $M_o(d)$ das q-ésimas primeira raiz de 1 sobre o corpo primo, contém dois distintos subcorpos N e N_1, sobre os quais sua dimensão é q.

Segue-se que o grupo de Galois $M_o(d)$ sobre M_o não é cíclico.

Pelo teorema 4.5.6 e 4.5.7, o único caso possível é ter características zero e $q = 2$.

Então o elemento "c" antes considerado é uma 4-ésima (q^2 com $q = 2$) raiz primitiva de 1.

Por outro lado, E contém L, que contém $\sqrt{-1}$ e como $\sqrt{-1}$ é uma 4-ésima raiz primitiva de 1, segue-se que $c \in E$, absurdo. Isto mostra que $L = M(\sqrt{-1}) = F$.

Teoremas usados neste capítulo

Teorema 4.5.1

Se "p" é um número primo e "a" um elemento de K que não é uma p-ésima raiz em K, então $x^p - a$ é irredutível sobre K.

Demonstração

Suponhamos que não seja, e consideremos f um fator irredutível de $x^p - a$ de grau $k (o < k < p)$. Seja "c" o termo - constante de f. As raizes de $x^p - a$ (em um corpo de raizes), todas têm a forma ru, onde u é uma raiz fixa e $r^p = 1$. Desde que $\pm c = s\, u^k$, $s^p = 1$ e existem inteiros m e n tal que $mk + np = 1$, temos que $u = u^{mk}\, u^{np} = (u^k)^m\, (u^p)^n = (\pm \frac{c}{s})^m\, a^n$.

Portanto u pertence a K. Desde que sua p-ésima potência é a, chegamos a uma contradição.

Teorema 4.5.2

Seja "p" um primo e "a" um elemento em K, que não é uma p-ésima potência em K com car (K) = p ≠ 0. Então $x^{p^n} - a$ é irredutível sobre K, $\forall_{n \geq 1}$.

Demonstração

Seja "v" uma raiz de $x^{p^n} - a$ e escrevamos $u = v^{p^{n-1}}$. Temos $u^p = a$, logo $[K(u) : K] = p$ (pois $x^p - a$ é irredutível sobre K teorema 4.5.1).

Se mostrarmos que "v" tem grau p^{n-1} sobre K (u), segue-se que "v" tem grau p^n sobre K e $x^{p^n} - a$ é irredutível sobre K.

Que "v" tem grau p^{n-1} sobre K (u) é verdade por indução sobre n, desde que u não é uma p-ésima potência em K (u). Se tal acontece

$$u = (c_o + c_1 u + \ldots + c_{u-1} u^{p-1})^p =$$

$$= (c_o^p + c_1^p u^p + \ldots + c_{u-1}^p u^{(p-1)p} =$$

$$= c_o^p + c_1^p a + \ldots + c_{u-1}^p a^{p-1}.$$ Logo u ε K, contradição.

Teorema 4.5.3

Seja S um corpo de característica p ≠ 0. Então existem extensões cíclicas de p^m - dimensão, m = 1, 2 ..., sobre S se, e somente se, existem tais extensões de dimensão "p".

Demonstração

Veja [14, pag. 139].

Teorema 4.5.4

Assuma que S tem "n" raizes distintas de 1 e seja P/S corpo de extensão, cíclico de dimensão "n".

Então P = S(d), onde $d^n = \alpha \in S$.

Demonstração

As hipóteses sobre P são que P/S é Galois com grupo de galois G, que é cíclico de ordem "n". Como P é separável sobre S, ele tem um elemento primitivo, desta forma $P = S(\theta)$.

Seja "s" um gerador de G e "d" o resolvente de Lagrange.

$$d = \theta + \theta^{s}\,\delta^{-1} + \theta^{s^2}\,\delta^{-2} + \ldots + \theta^{s^{n-1}}\,\delta^{-(n-1)}$$

onde "δ" é uma "n"-ésima raiz primitiva de 1.

Então $d^{s} = \theta^{s} + \theta^{s^2}\,\delta^{-1} + \theta^{s^3}\,\delta^{-2} + \ldots + \theta^{s^{n}}\,\delta^{-(n-1)} =$

$= \delta\,(\theta + \theta^{s}\,\delta^{-1} + \theta^{s^2}\,\delta^{-2} + \ldots + \theta^{s^{n-1}}\,\delta^{-(n-1)} =$

$= \delta d$

Então $d^{s^k} = \delta^{k}\,d^{k} = \delta^{k}\,d$, desta forma "d"tem "n" distintas conjugadas e, portanto, seu polinômio minimal é de grau "n". Consequentemente $P = S(d)$.

Seja $d^{n} = \alpha$, então $(d^{n})^{s} = (d^{s})^{n} = (\delta d)^{n} =$

$= \delta^{n} d^{n} = d^{n} = \alpha$, logo $\alpha^{s} = \alpha$ portanto $\alpha \in S$ e $d = \sqrt[n]{\alpha}$

Teorema 4.5.5

Seja $P^{(m)}$ corpo ciclotônico de ordem "m" sobre os racionais R_o.

Então o grupo de Galois de $P^{(m)}/R_o$ é isomorfo a U(m) o grupo multiplicativo das unidades do anel $I/_{(m)}$.

Demonstração

Veja [14, pag. 113].

OBSERVAÇÃO

(1) Foi definido corpo ciclotônico de ordem "m" sobre o corpo S, como sendo o corpo das raizes sobre S de um poli-

nômio $x^m - 1$.

(2) Se a característica de S não é um divisor de - "m", então o grupo de Galois do corpo ciclotônico, é isomorfo a um subgrupo do grupo multiplicativo. $U_{(m)}$ das unidades do anel $I/_{(m)}$.

Aqui assumimos que o corpo base $S = R_o$, o corpo dos números racionais, e seja $p^{(m)}$ o corpo ciclotônico das m-ésimas raizes de 1 sobre R_o (I anel dos inteiros).

Teorema 4.5.6

Qualquer subgrupo finito H de um grupo multiplicativo K^* de um corpo K, é um grupo cíclico.

Demonstração

Indiquemos por "n" a ordem de H e seja $a \in H$ um elemento de ordem máxima "s". Decorre do teorema de Lagrange que $s \mid n$, logo $s \leqslant n$.

Consideremos o polinômio $f(x) = x^s - 1 \in K[x]$.

Vemos facilmente que $f(y) = 0$, $\forall\, y \in H$, logo $s = \text{grau } f \geqslant n$ e então $s = n$. Portanto, o elemento "a" tem ordem $n = |H|$, logo H é cíclico.

Como decorrência temos:

Se K é um corpo finito, então o grupo multiplicativo K^* do corpo K é cíclico.

Teorema 4.5.7

Seja $m = p^n$, p (primo) e $P^{(m)}$ o corpo das m-ésimas raizes de 1 sobre R_o, o corpo dos números racionais.

Então o grupo de Galois G de $P^{(m)}/R_o$ é cíclico, exceto quando $p = 2$ e $n \geqslant 3$, neste caso G é produto direto de grupos cíclicos de ordem 2 ou de ordem 2^{n-2}.

Demonstração

Veja [14, pag. 115].

C A P Í T U L O 5

CARACTERIZAÇÃO DOS CORPOS REALMENTE FECHADOS - ARTIN - SCHEIER

Inicialmente daremos algumas definições.

Definição 5.1

Um corpo ordenado K é um corpo K junto com um subconjunto P (o conjunto dos elementos positivos) de K, tal que:

(1) $0 \notin P$

(2) Se $\ell \in K$, então ou $\ell \in P$, $\ell = 0$, ou $-\ell \in P$.

(3) P é fechado sob a adição e multiplicação.

Definição 5.2

Um corpo K é chamado *formalmente real* se as únicas relações da forma $\sum_{i=1}^{n} \ell_i^2 = 0$ em K são aquelas para as quais

$$\ell_i = 0 \quad \forall i = 1, 2, \ldots, n.$$

É imediato que K é formamente real se, e somente - se, -1 não é uma soma de quadrados de elementos em K. Se a ca - racterística de K é $p \neq 0$, então $0 = 1^2 + 1^2 + \ldots + 1^2$ (p termos) portanto é claro que corpos formalmente reais são necessariamente de característica zero.

Definição 5.3

Um corpo K é chamado *realmente fechado*, se K é formalmente real e nenhuma extensão algébrica própria de K é formalmente real.

Como consequência da definição 5.3, vemos facilmen

te que se K é corpo realmente fechado, então qualquer elemento de K ou é um quadrado ou o negativo de um quadrado.

Teorema 5.4

Se K é um corpo tal que $\sqrt{-1} \notin K$ e $K(\sqrt{-1})$ é algebricamente fechado, então K é realmente fechado.

Demonstração

Suponhamos que K satisfaz as condições acima. Notemos que os polinômios irredutíveis de grau positivo em $K[x]$ têm graus 1 ou 2. Seja $f(x)$ tal polinômio e r uma raiz de $f(x)$ contida em $M = K(\sqrt{-1})$. Desde que $[K(r) : K] = \text{grau } f(x)$ e $[K(r) : K] \mid [M : K] = 2$ segue-se que $[K(r) : K] = 1$ ou 2 e, portanto, grau $f(x) = 1$ ou 2 como asseguramos.

Sejam "a" e "b" $\in K$, $a \neq 0$, $b \neq 0$, e consideremos o seguinte polinômio $g(x)$, $g(x) = (x^2 - a)^2 + b^2 = (x^2 - a - bi)\ (x^2 - a + bi)$

Desde que

$$(x^2 - (a + bi)) = (x - (a + bi)^{1/2})\ (x + (a + bi)^{1/2}) \quad \text{e}$$

$$(x^2 - (a - bi)) = (x - (a - bi)^{1/2})\ (x + (a - bi)^{1/2}),$$

segue-se que

$$g(x) = (x - (a + bi)^{1/2})\ (x + (a + bi)^{1/2}) \cdot$$

$$(x - (a - bi)^{1/2})\ (x + (a - bi)^{1/2}) \quad \text{onde } i = \sqrt{-1}.$$

Este polinômio pertence a $K[x]$ e não tem fatores lineares em $K[x]$, visto que $a + bi$, $-a - bi$, $a - bi$ e $-a + bi$ não pertence a K. Portanto, $g(x)$ é produto de dois polinômios quadráticos irredutíveis.

Um possível divisível por $(x - (a + bi)^{1/2})$ não pode ser

$(x - (a + bi)^{1/2})\ (x + (a + bi)^{1/2}) = x^2 - (a + bi)$, pois isto implicará que $a + bi \in K$, o que é absurdo.

Portanto o polinômio em questão é

$$\text{ou} \quad (x - (a + bi)^{1/2})\ (x - (a - bi)^{1/2}) =$$

$$= x^2 - ((a + bi)^{1/2} + (a - bi)^{1/2})\ x + (a^2 + b^2)^{1/2}$$

$$\text{ou} \quad (x - (a + bi)^{1/2})\ (x + (a - bi)^{1/2}) =$$

$$= x^2 + ((a - bi)^{1/2} - (a + bi)^{1/2})\ x - (a^2 + b^2)^{1/2}$$

As duas possibilidades implicam que $(a^2 + b^2)^{1/2}$ pertence a K. Desde que "a" e "b" são elementos arbitrários e não nulos de K, provamos que a soma de dois quadrados de elementos de K é um quadrado em K. A indução mostra que cada soma de quadrados é um quadrado em K.

Desde que - 1 não é um quadrado, isto implica que - 1 não é soma de quadrados em K e, ademais, K é formalmente real. Se P é uma extensão algébrica própria de K, então P é isomorfo a $M = K(\sqrt{-1})$. Então P não é formalmente real e ademais K é realmente fechado. Isto completa nossa prova.

Teorema 5.5

Se K é um corpo realmente fechado, então $\sqrt{-1} \notin K$ e $K(\sqrt{-1})$ é algebricamente fechado.

Demonstração

Veja [14, pag. 275].

Portanto, temos uma caracterização de corpos K realmente fechados pela propriedade básica, que $\sqrt{-1} \notin K$ e $K(\sqrt{-1})$ é algebricamente fechado.

Teorema 5.6

Seja F um corpo algebricamente fechado e K um subcorpo próprio, que é de co-dimensão finita em F. Então K é realmente fechado e $F = K(\sqrt{-1})$.

Demonstração

Tomemos $L = K(\sqrt{-1}) \subseteq F$. Devemos mostrar que $L = F$ e a demonstração é a mesma feita no teorema 4.3. Como concluimos em tal demonstração que $K(\sqrt{-1}) = F$ que é algebricamente fechado e $\sqrt{-1}$ não pertence a K, usando o teorema 5.4, concluimos que K é realmente fechado. Portanto, K é realmente fechado e $F = K(\sqrt{-1})$.

B I B L I O G R A F I A

(1) C. W. CURTIS, The four and eight square problem and division algebras, in Studies in Modern Algebra, MAA. Studies in Mat., Vol. 2, (A.A. Albert, ed.), Prentice Hall, Englewood Cliffs. N.J., 1968.

(2) S. EILENBERG and N. STEENROD, Foudations of Algebraic Topology, Princeton V. Press, Princeton, N.J., 1952.

(3) W. B. GORDON, On the diffeomoiphisms of euclidean space, this Monthly, 79 (1972) 755-759.

(4) W. B. GORDON, Addendum to the above, this Monthly, 80(1973) 674.

(5) I. N. HERSTEIN, Topics in Algebra, Blaisdell, Ealtham, Mass. 1964.

(6) R. S. PALAIS, The classification of real division algebras, this Monthly, 75 (1968) 366-368.

(7) M. S. BERGER and M.S. BERGER, Perspectives in Non-Linearity, Benjamin, New York, 1968.

(8) A. NIJENHUIS and R.W. RICARDSON, Jr., A theorem on maps with non-negative Jacobians, Mich. Math. J.: 9 (1962) 173 -176.

(9) S. STERNBERG, Lectures on Differential Geometry, Prentice Hall, Englewood Cliffs, New Jersey, 1964.

(10) S. STERNBERG and R.G. SWAN, On maps with non-negative Jacobian, Mich. Mat., J., 6(1959) 339-342.

(11) J. MILNOR, Topology from the Differentiable Viewpoint, V. Press of Virginia, Charlotteswille, Va., 1965.

(12) A. ALBERT, The Structure of Algebra, AMS Colloquium Publi cation, 1939.

(13) ELON LAGES LIMA, Análise no espaço R^N.

(14) NATHAN JACOBSON, Algebra Vol. III. Theory of Fields.

(15) IRVING KAPLANSKY, Theory of Fields.