Álgebras de Dimensão Finitas

Bernardo Felzenszwalb

INSTITUTO DE MATEMÁTICA PURA E APLICADA
Rua Luiz de Camões, 68
20.060 - Rio de Janeiro - RJ

PREFÁCIO

Estas notas representam o conteúdo de um curso que ministramos no Instituto de Matemática da UFRJ durante o 2º período de 1978.

O nosso objetivo é o de motivar o leitor para os trabalhos de E. Noether, R. Brauer, A. Albert e H. Hasse (v. [2]), que continuaram o estudo das álgebras com divisão a partir do ponto que haviam chegado Wedderburn e Dickson. Por sua vez, estes trabalhos deverão servir de motivação para as questões ainda sem resposta sobre produtos cruzados, que são a ferramenta principal para a construção de álgebras com divisão.

Agradecemos a oportunidade oferecida pela Comissão Organizadora do 12º Colóquio Brasileiro de Matemática, e esperamos que os objetivos, ou parte deles, sejam alcançados.

Rio de Janeiro, julho de 1979

Bernardo Felzenszwalb

ÍNDICE

pág.

Capítulo 1 - Álgebras

Capítulo 2 - O radical

Capítulo 3 - Os teoremas de estrutura

Capítulo 4 - Álgebras simples

CAPÍTULO 1

ÁLGEBRAS

A primeira definição correta de uma álgebra associativa sobre um corpo arbitrário parece ter sido dada por Dickson [9] em 1903. Começaremos este capítulo discutindo brevemente as origens desta definição, que será introduzida no §5. Aqui como no resto do texto os conceitos básicos serão apresentados com o espírito de quem está recordando algumas noções já do conhecimento do leitor, mas reservando o direito de ser repetitivo.

Como é usual, o corpo dos números reais e o corpo dos números complexos serão denotados por $\mathbb{R}$ e $\mathbb{C}$ respectivamente.

1. Os números complexos.

Historicamente existem duas razões principais para a consideração dos números complexos. Uma de natureza algébrica - a resolução da equação x^2+1 - aparece nos séculos dezesseis e dezessete quando, ainda se debatendo com os números negativos e irracionais, os europeus iniciaram a discussão sobre as "soluções impossíveis". Um outro motivo apareceu bem mais tarde com a emergência em geometria e física do conceito de quantidade direcionada ou vetor. Era desejável criar um análogo aritmético do conceito de vetor e o sistema dos números complexos surge como o candidato perfeito de uma "álgebra" para representar e operar os vetores no plano.

Muitos pesquisadores chegaram independentemente à interpretação geométrica dos números complexos. Basta citar entre eles Gauss que, como comprova o seu diário (v. Mathematische Annalen vol. 57, (1903)), tinha em 1797 pleno conhecimento desta interpretação e definitivamente a usou em suas várias demonstrações do teorema fundamental da álgebra. Entretanto, coube a Hamilton [15] em 1833 apresentar o primeiro tratamento realmente moderno dos números complexos como pares ordenados de reais. Ele ressaltou que um número complexo $\alpha + \beta i$ não é uma soma genuína; o uso do sinal de mais é um acidente histórico e βi não pode ser somado a α. O número $\alpha + \beta i$ nada mais é do que o par (α,β). Tem-se:

$$(\alpha,\beta) + (\gamma,\delta) = (\alpha+\beta,\ \beta+\delta)$$
$$(\alpha,\beta)(\gamma,\delta) = (\alpha\gamma-\beta\delta,\ \alpha\delta+\beta\gamma)$$

$$\frac{(\alpha,\beta)}{(\gamma,\delta)} = \left(\frac{\alpha\gamma+\beta\delta}{\gamma^2+\delta^2},\ \frac{\beta\gamma-\alpha\delta}{\gamma^2+\delta^2}\right) \quad \text{se} \quad (\gamma,\delta) \neq 0.$$

Desta forma os vetores do plano satisfazem todos os axiomas de um corpo. Os números reais sob a identificação $\alpha = (\alpha,0)$ aparecem como um subcorpo dos complexos e a equação $x^2+1 = 0$ tem então como soluções $i = (0,1)$ e $-i = (0,-1)$. Em particular, desaparece o mistério envolvendo o famigerado $i = \sqrt{-1}$.

Geometricamente, para um número complexo $\gamma+\delta i = (\gamma,\delta)$

$$(x,y) \to (x+\gamma,\ y+\delta)$$

significa uma translação do plano sobre si mesmo, e

$$(x,y) \to (x\gamma-y\delta,\ x\delta-y\gamma)$$

uma transformação de semelhança, isto é, uma rotação seguida de

uma homotetia, permanecendo fixa em ambas a origem. Multiplicando (γ,δ) pelo seu conjugado $(\gamma,-\delta)$ obtemos $\gamma^2+\delta^2$, o quadrado da distância de (γ,δ) a origem, e para $(\gamma,\delta) \neq 0$ temos que

$$(\gamma,\delta)^{-1} = \frac{1}{\gamma^2+\delta^2}\,(\gamma,-\delta).$$

2. A impossibilidade um número complexo tri-dimensional.

Quando várias forças agem sobre um corpo elas não estão necessariamente num plano. Assim, naturalmente, era desejável encontrar uma álgebra para representar e operar vetores em espaços de maiores dimensões. Isto motivou a procura pelos matemáticos europeus de um número complexo tri-dimensional e mais geralmente dos números hipercomplexos (álgebras).

Gauss estava convencido de que uma extensão dos números complexos que preservasse as propriedades básicas era impossível ([13] p.178). Ele não provou isto mas estava certo.

Examinaremos aqui o problema de introduzir uma multiplicação no espaço de três dimensões $\mathbb{R}^3$ de maneira que resulte uma generalização natural dos números complexos como pontos do plano $(\alpha,\beta) = \alpha+\beta i$, assim como estes são uma generalização natural dos números reais como pontos da reta sob a identificação $(\alpha,0) = \alpha$. Em outras palavras, considerando os ternos ordenados de números reais (α,β,γ) com as identificações $(\alpha,0,0) = \alpha$ e $(\alpha,\beta,0) = \alpha+\beta i$, e com as operações usuais de adição e multiplicação por escalares, a questão é: podemos definir uma multiplicação de vetores em $\mathbb{R}^3$ de modo que sejam válidos todos os axiomas de um

corpo?

Não é difícil mostrar que isto é impossível.

Com efeito, seja $(\alpha,\beta,\gamma) = \alpha+\beta i+\gamma j$ (onde, é claro, $j = (0,0,1)$) e vamos supor que uma tal multiplicação está definida. Então podemos escrever

$$ij = \alpha_o + \beta_o i + \gamma_o j$$

onde α_o, β_o e γ_o são reais. Multiplicando ambos os lados por i à esquerda, obtemos

$$-j = i^2 j = i(ij) = i(\alpha_o+\beta_o i+\gamma_o j) = \alpha_o i - \beta_o + \gamma_o ij.$$

Substituindo agora ij por $\alpha_o + \beta_o i + \gamma_o j$, segue que

$$(\alpha_o\gamma_o-\beta_o) + (\alpha_o+\beta_o\gamma_o)i + (\gamma_o^2+1)j = 0,$$

contradizendo o fato de que γ_o é real.

Note que para chegar a uma contradição usamos apenas a associatividade e distributividade da multiplicação. Mesmo não exigindo associatividade e comutatividade, divisão por vetores $\neq 0$ não é sempre possível. Por exemplo, se como antes $ij = \alpha_o + \beta_o i + \gamma_o j$ então

$$(i-\gamma_o)[\alpha_o\gamma_o-\beta_o + (\beta_o\gamma_o+\alpha_o)i + (\gamma_o^2+1)j] = 0$$

com ambos os fatores $\neq 0$.

3. Quaternios.

Após introduzir o tratamento moderno dos complexos como pares ordenados de reais, Hamilton tentou uma generalização para

ternos ordenados. Em 1843, depois de dez anos de experimentações e sem ter provado a impossibilidade no espaço de três dimensões, ele descobriu os quaternios que são de dimensão 4 sobre os reais e onde a multiplicação não é comutativa [16].

Podemos apresentar os quaternios como quádruplas de números reais.

Seja Q o espaço vetorial real de dimensão 4 que consiste de todas as quádruplas

$$a = (\alpha_0,\alpha_1,\alpha_2,\alpha_3) \qquad \alpha_i \in \mathbb{R}.$$

Colocando

$$1 = (1,0,0,0), \quad i = (0,1,0,0), \quad j = (0,0,1,0) \quad e \quad k = (0,0,0,1)$$

todo elemento a de Q tem uma única representação como

$$a = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$$

que é a representação usual de um quaternio. Hamilton definiu uma multiplicação em Q de maneira distributiva de acordo com as seguintes relações

$$(3.1) \quad i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Assim, para o produto de dois elementos arbitrários, obtemos

$$(\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k)(\beta_0+\beta_1 i+\beta_2 j+\beta_3 k)$$

$$= (\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3) + (\alpha_1\beta_0+\alpha_0\beta_1-\alpha_3\beta_2+\alpha_2\beta_3)i$$

$$+ (\alpha_2\beta_0+\alpha_3\beta_1+\alpha_0\beta_2-\alpha_1\beta_3)j + (\alpha_3\beta_0-\alpha_2\beta_1+\alpha_1\beta_2+\alpha_0\beta_3)k.$$

Não é difícil verificar que vale a lei associativa. O espaço ve-

torial Q munido desta multiplicação é chamado a <u>álgebra dos quaternios reais</u>.

É imediato que 1 age como unidade multiplicativa (desde o início suprimimos o 1 da notação). Vamos mostrar que todo quaternio não nulo tem um inverso multiplicativo. Com efeito, suponhamos que $a = \alpha_o+\alpha_1 i+\alpha_2 j+\alpha_3 k \neq 0$. Observamos primeiro que como os α_i são reais, $\alpha_o^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \neq 0$. Agora, para determinar b tal que $ab = 1$ devemos resolver o seguinte sistema

$$\begin{aligned}
\alpha_o\beta_o - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3 &= 1\\
\alpha_1\beta_o + \alpha_o\beta_1 - \alpha_3\beta_2 + \alpha_2\beta_3 &= 0\\
\alpha_2\beta_o + \alpha_3\beta_1 + \alpha_o\beta_2 - \alpha_1\beta_3 &= 0\\
\alpha_3\beta_o - \alpha_2\beta_1 + \alpha_1\beta_2 + \alpha_o\beta_3 &= 0.
\end{aligned}$$

Como o determinante deste sistema é $(\alpha_o^2+\alpha_1^2+\alpha_2^2+\alpha_3^2)^2 \neq 0$, concluimos que existe uma única solução. Uma outra maneira de ver isto é a seguinte. Por analogia com os números complexos, Hamilton definiu para cada quaternio $a = \alpha_o + \alpha_1 i + \alpha_2 j + \alpha_3 k$ um quaternio <u>conjugado</u> $\bar{a} = \alpha_o - \alpha_1 i - \alpha_2 j - \alpha_3 k$, e observou que

$$\bar{a}a = a\bar{a} = \alpha_o^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 .$$

Se definimos a <u>norma</u> de a por

$$N(a) = \alpha_o^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 ,$$

então para um quaternio $a \neq 0$ temos que $N(a) \neq 0$ e o inverso de a é dado explicitamente por

$$a^{-1} = \frac{1}{N(a)}\ \bar{a}.$$

Assim, todos os axiomas de um corpo são satisfeitos exceto a comu

tatividade pois, por exemplo, $ij \neq ji$. Este foi o primeiro exemplo de um corpo não comutativo.

Note que o corpo C está imerso em Q como o subespaço que consiste de todos os vetores da forma $\alpha_0 + \alpha_1 i$; além disso, a multiplicação em Q é compatível com a desta cópia imersa de C.

Finalmente, observamos que a multiplicação em Q induz no espaço quociente $Q/\mathbb{R}$ a estrutura usual de produto vetorial em $\mathbb{R}^3$ (aqui identificamos $\mathbb{R}$ com sua cópia imersa em Q e as imagens de i, j, k em $Q/\mathbb{R}$ com os vetores unitários ao longo dos eixos de coordenadas).

4. Os números de Cayley.

Logo após a descoberta dos quaternios por Hamilton, Cayley [7] apresentou uma generalização (os octônios) definindo uma multiplicação não comutativa e não associativa num espaço vetorial de dimensão 8 sobre os reais.

Os números de Cayley são da forma

$$a = \alpha_0 1 + \alpha_1 \varepsilon_1 + \ldots + \alpha_7 \varepsilon_7 \qquad (\alpha_i \in R),$$

e o produto de dois tais números é definido de maneira distributiva de acordo com a seguinte tábua de multiplicação dos elementos básicos $1, \varepsilon_1, \ldots, \varepsilon_7$:

	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	-1	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	e_2	$-e_3$	-1	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_2	$-e_1$	$-e_1$	-1	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	-1	e_1	e_2	e_3
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	-1	$-e_3$	e_2
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	-1	$-e_1$
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	-1

O leitor verificará facilmente que a multiplicação assim definida é de fato não associativa e não comutativa. É óbvio que o elemento básico 1 age como unidade multiplicativa. Para mostrar a existência de inversos procedemos como antes. O conjugado de $a = \alpha_0 1 + \alpha_1 e_1 + \ldots + \alpha_7 e_7$ é definido por

$$\bar{a} = \alpha_0 1 - \alpha_1 e_1 - \ldots - \alpha_7 e_7 ,$$

e o número real

$$N(a) = a\bar{a} = \alpha_0^2 + \alpha_1^2 + \ldots + \alpha_7^2$$

é a norma de a. Se $a \neq 0$ então, como os α_i são reais, $N(a) \neq 0$ e temos que

$$a^{-1} = \frac{1}{N(a)}\,\bar{a} .$$

Evidentemente, os números de Cayley da forma

$$\alpha_0 1 + \alpha_1 \varepsilon_1 + \alpha_2 \varepsilon_2 + \alpha_3 \varepsilon_3$$

nos dão uma cópia dos quaternios reais.

5. Definição e construção de álgebras.

Neste ponto é conveniente introduzir a definição de uma álgebra (associativa) sobre um corpo arbitrário. Vamos nos restringir às álgebras de dimensão finita que são os objetos da teoria clássica.

Seja K um corpo. Por uma álgebra associativa sobre K (K-álgebra ou simplesmente álgebra) nós entendemos um espaço vetorial A de dimensão finita sobre K no qual está definida uma multiplicação

$$(a,b) \to ab$$

satisfazendo as seguintes condições:

1. $(ab)c = a(bc)$
2. $a(b+c) = ab+ac$ e $(b+c)a = ba+ca$
3. $\alpha(ab) = (\alpha a)b = a(\alpha b)$

quaisquer que sejam $a,b,c \in A$ e $\alpha \in K$.

Assim, uma álgebra A n-dimensional sobre um corpo K consiste de todas as combinações lineares

$$a = \sum_{i=1}^{n} \alpha_i \varepsilon_i$$

de n elementos básicos $\varepsilon_1,\ldots,\varepsilon_n$ com coeficientes α_i em K.

Adição e multiplicação por escalares são definidas pelas operações correspondentes sobre os coeficientes, e o produto de duas tais expressões é definido pela fórmula

$$(5.1) \qquad (\sum_{i=1}^{n} \alpha_i \epsilon_i)(\sum_{i=1}^{n} \beta_i \epsilon_i) = \sum_{i,j=1}^{n} (\alpha_i \beta_j)\epsilon_i \epsilon_j,$$

juntamente com uma tábua de multiplicação dos elementos básicos $\epsilon_1, \ldots, \epsilon_n$. Portanto, se

$$(5.2) \qquad \epsilon_i \epsilon_j = \sum_{k=1}^{n} \gamma_{ijk} \epsilon_k \qquad (i,j = 1,\ldots,n),$$

a multiplicação é completamente determinada pelos n^3 escalares γ_{ijk}, chamados <u>constantes de multiplicação</u> de A com respeito a base $\epsilon_1, \ldots, \epsilon_n$.

Estas constantes não podem ser escolhidas arbitrariamente pois a multiplicação em A deve ser associativa. Agora, é imediato que a associatividade e válida se e somente se valem as seguintes relações:

$$(\epsilon_i \epsilon_j)\epsilon_k = \epsilon_i(\epsilon_j \epsilon_k) \qquad (i,j,k = 1,\ldots,n).$$

Calculando vemos que devemos ter

$$\sum_{h,\ell} (\gamma_{ijh} \gamma_{hk\ell})\epsilon_\ell = \sum_{h,\ell} (\gamma_{jkh} \gamma_{ih\ell})\epsilon_\ell.$$

Como $\epsilon_1, \ldots, \epsilon_n$ são linearmente independentes, concluimos que a associatividade da multiplicação é equivalente as n^4 equações

$$(5.3) \qquad \sum_{h=1}^{n} \gamma_{ijh} \gamma_{hk\ell} = \sum_{h=1}^{n} \gamma_{jkh} \gamma_{ih\ell} \qquad (i,j,k,\ell = 1,\ldots,n).$$

Isto nos dá um procedimento geral para a construção de álgebras. Dado um espaço vetorial A n-dimensional sobre um corpo K com

uma base $\mathfrak{e}_1,\ldots,\mathfrak{e}_n$, escolhemos n^3 elementos γ_{ijk} em K satisfazendo as equações (5.3). Definimos então uma multiplicação em A de maneira distributiva pela fórmula (5.1) de acordo com (5.2). Claramente as condições para uma álgebra são assim preenchidas. Denotaremos esta álgebra por $A = (\mathfrak{e}_1,\ldots,\mathfrak{e}_n)_K$ e diremos que as relações (5.2) dão uma tábua de multiplicação de A (com respeito a base $\mathfrak{e}_1,\ldots,\mathfrak{e}_n$).

Exemplo 1 - Os números complexos formam uma álgebra bi-dimensional sobre o corpo dos números reais. Mais geralmente, se $F \supseteq K$ é uma extensão finita de corpos, então F é uma álgebra n-dimensional sobre K onde n é o grau da extensão.

Exemplo 2 - Consideremos o espaço vetorial real de três dimensões $\mathbb{R}^3$. Seja $\mathfrak{e}_1$, $\mathfrak{e}_2$, $\mathfrak{e}_3$ uma base de $\mathbb{R}^3$ sobre $\mathbb{R}$, digamos a base canônica $\mathfrak{e}_1 = (1,0,0)$, $\mathfrak{e}_2 = (0,1,0)$, $\mathfrak{e}_3 = (0,0,1)$. Definimos uma multiplicação em R^3 pelo método descrito acima escolhendo $3^3 = 27$ números reais γ_{ijk} $(i,j,k = 1,2,3)$ da seguinte forma:

$$\gamma_{111} = \gamma_{122} = \gamma_{133} = \gamma_{212} = \gamma_{221} = \gamma_{233} = \gamma_{313} = \gamma_{323} = 1$$

e todos os outros iguais a 0.

O leitor verificará facilmente que as equações de associatividade são satisfeitas. Deste modo, obtemos uma álgebra tri-dimensional sobre os reais com a seguinte tábua de multiplicação

	$\mathfrak{e}_1$	$\mathfrak{e}_2$	$\mathfrak{e}_3$
$\mathfrak{e}_1$	$\mathfrak{e}_1$	$\mathfrak{e}_2$	$\mathfrak{e}_3$
$\mathfrak{e}_2$	$\mathfrak{e}_2$	$\mathfrak{e}_1$	$\mathfrak{e}_3$
$\mathfrak{e}_3$	$\mathfrak{e}_3$	$\mathfrak{e}_3$	0

Compare este exemplo com a discussão do §2.

Exemplo 3 - Além dos quaternios reais Hamilton [16] também introduziu biquaternios, isto é, quaternios com coeficientes complexos. Estes são números da forma

$$\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \qquad (\alpha_i \in \mathbb{C})$$

onde, como para os quaternios reais, a multiplicação é definida de maneira distributiva de acordo com as relações (3.1). Assim, obtemos uma álgebra de dimensão 4 sobre o corpo complexo. Entretanto, para os biquaternios divisão por elementos não nulos nem sempre é possível. Por exemplo,

$$(\sqrt{-1}\, j + k)(\sqrt{-1} + i) = 0$$

com ambos os fatores $\neq 0$.

Mais geralmente, podemos considerar a álgebra dos quaternios sobre um corpo K arbitrário. Estudaremos estas álgebras mais adiante.

Um exemplo especialmente importante é o seguinte:

Exemplo 4 (Transformações lineares) - Seja V um espaço vetorial n-dimensional sobre um corpo K, e denotemos por $\mathcal{L}(V)$ o conjunto das transformações lineares de V em V. Sabemos que $\mathcal{L}(V)$ é um espaço vetorial n^2-dimensional sobre K, onde para $S,T \in \mathcal{L}(V)$ a soma $S+T$ é definida por

$$v(S+T) = vS + vT \qquad v \in V,$$

e para $\alpha \in K$ o produto escalar αT é dado por

$$v(\alpha T) = (\alpha v)T = \alpha(vT) \qquad v \in V.$$

A composição de funções sugere uma multiplicação em $\mathcal{L}(V)$. Se $S,T \in \mathcal{L}(V)$ definimos o produto ST por

$$v(ST) = (vS)T \qquad v \in V.$$

Esta multiplicação é associativa, distributiva com respeito a adição, e para $\alpha \in K$

$$\alpha(ST) = (\alpha S)T = S(\alpha T).$$

Assim, $\mathcal{L}(V)$ é uma K-álgebra.

Agora, uma transformação linear $T: V \to V$ é completamente determinada pelo seu efeito sobre uma base $v_1,\ldots,v_n$ de V. Portanto, se

$$v_i T = \sum_{j=1}^{n} \beta_{ij} v_j \qquad (i=1,\ldots,n),$$

T é unicamente determinada, uma vez que fixamos a base, pelos n^2 escalares β_{ij} ou ainda, pela matriz

$$M_T = \begin{pmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ \beta_{n1} & \beta_{n2} & \cdots & \beta_{nn} \end{pmatrix}$$

Reciprocamente, se $M = (\beta_{rs})$ é uma matriz $n \times n$ sobre K arbitrária, podemos especificar uma transformação linear $T: V \to V$ de tal forma que $M = M_T$. Fazemos isto definindo para $v = \alpha_1 v_1 + \ldots + \alpha_n v_n$

$$vT = (\sum_{i=1}^{n} \alpha_i \beta_{i1}) v_1 + \ldots + (\sum_{i=1}^{n} \alpha_i \beta_{in}) v_n.$$

Deste modo concluimos que $T \to M_T$ é uma correspondencia biunívo-

ca entre $\mathcal{L}(V)$ e K_n, o conjunto de todas as matrizes $n \times n$ sobre K. Esta correspondência induz as operações usuais de matrizes, isto é, para $S,T \in \mathcal{L}(V)$ e $\alpha \in K$

$$M_{S+T} = M_S + M_T, \quad M_{\alpha T} = \alpha M_T, \quad M_{ST} = M_S M_T$$

e com estas operações K_n é uma álgebra sobre K. Assim, $\mathcal{L}(V)$ e K_n são álgebras equivalentes e vamos nos referir a estas duas álgebras indistintamente.

É claro que a matriz identidade $n \times n$

$$1_n = \begin{pmatrix} 1 & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

age como unidade multiplicativa para K_n. O corpo K é imerso em K_n por $\alpha \to \alpha 1_n$ e, assim, identificamos os escalares $\alpha \in K$ com as matrizes escalares

$$\alpha 1_n = \begin{pmatrix} \alpha & & 0 \\ & \alpha & \\ & \ddots & \\ 0 & & \alpha \end{pmatrix} .$$

As <u>matrizes unitárias</u> e_{ij} $(i,j=1,\ldots,n)$ são definidas como segue: e_{ij} é a matriz que tem 1 como coordenada na posição (i,j) e 0 em todas as outras posições. Toda matriz $(\alpha_{ij}) \in K_n$ pode ser escrita de maneira única como $(\alpha_{ij}) = \sum_{i,j} \alpha_{ij} e_{ij}$; portanto, as matrizes unitárias formam uma base de K_n sobre K. Finalmente, observamos que

$$e_{11} + e_{22} + e_{33} + \ldots + e_{nn} = 1_n$$

e

$$e_{ij}e_{k\ell} = \begin{cases} e_{i\ell} & \text{se} \quad j = k \\ 0 & \text{se} \quad j \neq k \end{cases}$$

Exemplo 5 (Álgebras de matrizes) - Matrizes sobre um corpo geram álgebras. Mais geralmente, se A é uma álgebra sobre um corpo K podemos considerar a K-álgebra das matrizes $n \times n$ com coeficientes em A, que denotaremos por A_n. Os elementos (matrizes) de A_n são da forma

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \qquad a_{ij} \in A.$$

Duas tais matrizes (a_{ij}) e (b_{ij}) são ditas iguais se e somente se $a_{ij} = b_{ij}$ para cada i e j. As operações de adição, multiplicação por escalares e multiplicação são definidas por analogia com as operações em K_n; isto é,

$$(a_{ij}) + (b_{ij}) = (c_{ij}) \quad \text{onde} \quad c_{ij} = a_{ij} + b_{ij} \quad \text{para todo } i,j;$$

$$\alpha(a_{ij}) = (a'_{ij}) \quad \text{onde} \quad a'_{ij} = \alpha a_{ij} \quad \text{para todo } i,j;$$

e

$$(a_{ij})(b_{ij}) = (d_{ij}) \quad \text{onde} \quad d_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} \quad \text{para todo } i,j.$$

O leitor verificará facilmente que se $\dim_K A = m$ então $\dim_K A_n = mn^2$.

Exemplo 6 (Álgebras de Grupo) - Seja K um corpo e seja G um

grupo finito de ordem $o(G) = n$. Se $g_1,\ldots,g_n$ são os elementos de G, seja $K(G)$ o conjunto de todas as combinações lineares formais

$$\alpha_1 g_1 + \ldots + \alpha_n g_n = \sum_{i=1}^{n} \alpha_i g_i \qquad \alpha_i \in K,$$

onde duas tais expressões $\sum_{i=1}^{n} \alpha_i g_i$ e $\sum_{i=1}^{n} \beta_i g_i$ são consideradas iguais se e somente se $\alpha_i = \beta_i$, $i = 1,\ldots,n$. Fazemos de $K(G)$ um espaço vetorial sobre K definindo adição e multiplicação por escalares pelas operações correspondentes sobre os coeficientes. Agora, a multiplicação em G sugere uma multiplicação em $K(G)$; assim, definimos

$$\left(\sum_{i=1}^{n} \alpha_i g_i\right)\left(\sum_{i=1}^{n} \beta_i g_i\right) = \sum_{k=1}^{n} \left(\sum_{g_i g_j = g_k} \alpha_i \beta_j\right) g_k$$

de acordo com os produtos $g_i g_j = g_k$ em G. Podemos considerar G contido em $K(G)$ identificando g_i com $1g_i$. Com esta identificação os elementos de grupo formam uma base de $K(G)$ sobre K e as equações de associatividade são satisfeitas. Desta forma obtemos uma álgebra n-dimensional sobre K, a <u>álgebra de grupo</u> de G sobre K.

<u>Observação</u>: Os números de Cayley formam o que chamamos de uma <u>álgebra não associativa</u>.

6. Tipos de álgebras.

Tipos especiais de álgebras são obtidos quando impomos certas restrições na estrutura multiplicativa. Assim, uma álgebra A diz-se comutativa se $ab = ba$ quaisquer que sejam $a,b \in A$. Dizemos que A é uma álgebra com unidade se existe $1 \in A$ tal que $1a = a1 = a$ para todo $a \in A$. Se um tal elemento existe ele é único e é chamado unidade de A. Se a unidade $1 = 0$, então $a = 1a = 0a = 0$ para todo $a \in A$, isto é, $A = 0$. Daqui por diante quando falamos de uma álgebra com unidade subentendemos que $1 \neq 0$.

Um elemento a de uma álgebra com unidade A diz-se inversível se ele tem um inverso multiplicativo, isto é, se existe $a' \in A$ tal que $aa' = a'a = 1$. Neste caso a' é único e será denotado por a^{-1}. Finalmente, dizemos que uma álgebra com unidade é uma álgebra com divisão se todo elemento não nulo é inversível.

O leitor deverá reconhecer nos exemplos do parágrafo anterior os tipos de álgebras aqui introduzidos. Examinaremos apenas as álgebras de grupo $K(G)$ de um grupo finito G sobre um corpo arbitrário K. Claramente, $K(G)$ é uma álgebra com unidade, a saber a identidade do grupo, e os elementos do grupo são inversíveis. É claro também que $K(G)$ é uma álgebra comutativa se e somente se G é abeliano. Suponhamos agora que $G \neq \{1\}$. Vamos mostrar que neste caso $K(G)$ não é uma álgebra com divisão. Com efeito, seja $a = \sum_{g \in G}' g$. Como os elementos de grupo são linear-

mente independentes, $a \neq 0$. Agora, para todo $g \in G$ temos $ag = a$ e portanto

$$a^2 = a\Big(\sum_{g\in G} g\Big) = \sum_{g\in G} ag = o(G)a.$$

Se a característica de K divide a ordem de G, segue que $a^2 = 0$. Por outro lado, se a característica de K não divide a ordem de G, então $b = o(G)^{-1}a \neq 1$ e $(b-1)b = 0$. Em todo caso, concluimos que existe um produto $xy = 0$ com ambos os fatores $\neq 0$.

Observações: 1) Para uma K-álgebra A com unidade 1, as relações

$$(\alpha+\beta)1 = \alpha 1+\beta 1, \quad (\alpha\beta)1 = \alpha(\beta 1) = (\alpha 1)(\beta 1) \qquad \alpha,\beta \in K$$

nos permitem identificar os escalares α com os múltiplos escalares $\alpha 1$; ou seja, K é imerso em A por $\alpha \to \alpha 1$ $(\alpha\in K)$. Em particular, isto justifica o uso que fazemos do mesmo símbolo para denotar tanto a unidade de A quanto a unidade de K.

a) Toda K-álgebra A está imersa numa K-álgebra com unidade.

De fato, se A não possui unidade, definimos no conjunto $\tilde{A} = K\times A$ as seguintes operações:

$$(\alpha,a) + (\beta,b) = (\alpha+\beta,\ a+b)$$

$$(\alpha,a)(\beta,b) = (\alpha\beta,\ ab+\beta a+\alpha b)$$

$$\gamma(\alpha,a) = (\gamma\alpha,\gamma a).$$

Deste modo, $\tilde{A}$ é uma K-álgebra com unidade $(1,0)$ e, além disso, A é imersa em $\tilde{A}$ por $a \to (0,a)$. Dizemos que $\tilde{A}$ é a álgebra obtida de A pela adjunção de uma unidade.

7. Álgebras equivalentes e recíprocas.

Não faz muito sentido comparar álgebras sobre corpos distintos. A noção de isomorfismo se aplica apenas para álgebras A e A' sobre um mesmo corpo K, e significa uma correspondência biunívoca $a \longrightarrow a'$ entre A e A' tal que

$$(7.1) \qquad (a+b)' = a'+b', \quad (\alpha a)' = \alpha a' \quad \text{e} \quad (ab)' = a'b'$$

para todo $a,b \in A$ e $\alpha \in K$. Se este for o caso, dizemos que as álgebras A e A' são equivalentes (isomorfas) e denotamos este fato por $A \simeq A'$. Um isomorfismo de uma álgebra sobre si própria é chamado um automorfismo.

Vimos que a álgebra K_n das matrizes $n \times n$ sobre um corpo K é equivalente a álgebra das transformações lineares em um espaço vetorial n-dimensional sobre K (§5).

Um outro exemplo é o seguinte. Considere o conjunto Q' de todas as matrizes em C^2 da forma

$$\begin{pmatrix} \alpha_0+\alpha_1 i & \alpha_2+\alpha_3 i \\ -\alpha_2+\alpha_3 i & \alpha_0-\alpha_1 i \end{pmatrix} \qquad \alpha_i \in \mathbb{R}.$$

Com as operações usuais de matrizes, Q' é uma álgebra sobre $\mathbb{R}$. Agora, se

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i' = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k' = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

todo elemento de Q' tem uma única representação como

$$\alpha_0 + \alpha_1 i' + \alpha_2 j' + \alpha_3 k' \qquad \alpha_i \in \mathbb{R}.$$

À luz desta representação concluimos que a álgebra Q dos quaternios reais é equivalente a Q'. É interessante observar que a norma de um quaternio é precisamente o determinante da matriz correspondente em Q'.

Deixamos para o leitor verificar que a álgebra dos biquaternios (quaternios com coeficientes complexos) é equivalente a álgebra das matrizes 2×2 sobre o corpo complexo.

Finalmente, um exemplo de um automorfismo é dado pela correspondência $\alpha+\beta i \to \alpha-\beta i$ que a cada número complexo associa o seu conjugado (aqui estamos considerando os complexos como uma álgebra sobre os reais).

Se na definição acima substituimos em (7.1) a condição $(ab)' = a'b'$ por $(ab)' = b'a'$, obtemos o que chamamos de anti-isomorfismo e dizemos que as álgebras A e A' são recíprocas (anti-isomorfas). Analogamente temos o conceito de anti-automorfismo.

Denotaremos por A^{op} a álgebra que coincide com a álgebra A como um espaço vetorial, mas com a multiplicação definida por $a.b = ba$ onde ba é o produto em A. Claramente A e A^{op} são álgebras recíprocas. Vamos nos referir a A^{op} como a álgebra oposta de A.

Note que se A é uma álgebra comutativa, então $A^{op} = A$. Isto pode ocorrer também para álgebras não comutativas. Por e-

xemplo, a correspondência

$$\alpha_o+\alpha_1 i+\alpha_2 j+\alpha_3 k \to \alpha_o-\alpha_1 i-\alpha_2 j-\alpha_3 k$$

é um anti-automorfismo da álgebra Q dos quaternios reais. Assim, podemos tomar para Q^{op} o próprio Q.

Um outro exemplo de uma álgebra não comutativa anti-isomorfa a si própria é dado pela álgebra K_n das matrizes nxn sobre um corpo K. Para ver isto basta considerar a correspondência que a cada matriz (α_{ij}) em K_n associa a sua matriz transposta, isto é, a matriz que tem α_{ji} na posição (i,j).

8. O teorema de Frobenius.

Voltamos agora a discutir a possibilidade ou não de se definir uma multiplicação num espaço vetorial de dimensão finita sobre os reais de modo que se verifiquem os axiomas de um corpo.

Em 1867 Hankel publicou uma demonstração de que nenhum sistema de números hipercomplexos satisfaz todas as propriedades básicas de um corpo. Ele escreveu ([17] pp. 106-108) "... assim está respondida a questão cuja solução foi prometida mas não dada por Gauss". Uma resposta mais precisa foi obtida dez anos depois por Frobenius [12], a saber

Teorema 8.1 - As únicas álgebras com divisão sobre os reais são (a menos de isomorfismo) o corpo dos números reais, o corpo dos números complexos e a álgebra dos quaternios reais.

Demonstração: Seguiremos a demonstração oferecida por Dickson ([11] pp. 62-64).

Seja D uma álgebra com divisão n-dimensional sobre $\mathbb{R}$. Para n=1, D é equivalente ao corpo dos números reais; logo, podemos supor que $n > 1$.

Afirmamos que se $a \in D$ e $a \notin \mathbb{R}$, então existem $\gamma, \delta \in \mathbb{R}$ tais que $[1/\gamma(a+\delta)]^2 = -1$. Com efeito, os n+1 elementos $1, a, a^2, \ldots, a^n$ são linearmente dependentes sobre $\mathbb{R}$, isto é, podemos escrever $\alpha_0+\alpha_1 a+\alpha_2 a^2 +\ldots+ \alpha_n a^n$ $(\alpha_i \in \mathbb{R})$ onde nem todo α_i é nulo. Assim, a satisfaz um polinômio não nulo $f(x)$ com coeficientes reais. Pelo teorema fundamental da álgebra, $f(x) = f_1(x)\ldots f_r(x)$ um produto de fatores lineares ou quadráticos com coeficientes reais. Como $f(a) = f_1(a)\ldots f_r(a) = 0$ e D é uma álgebra com divisão, segue que a satisfaz um polinômio quadrático, digamos $a^2+\alpha a+\beta = 0$ $(\alpha, \beta \in \mathbb{R})$. Logo, para $\delta = \alpha/2$ temos que $(a+\delta)^2 = \delta^2-\beta$; além disso, $\delta^2-\beta < 0$ pois $a \notin R$. Em outras palavras, $(a+\delta)^2 = -\gamma^2$ onde $\gamma \in R$, $\gamma \neq 0$, e a afirmação segue.

É agora evidente que para n=2 podemos escolher uma base 1, I de D sobre $\mathbb{R}$ onde $I^2 = -1$. Portanto, neste caso, D é equivalente ao corpo dos números complexos. Daqui por diante consideraremos $n > 2$.

Seja 1, I, J, ... uma base de D sobre $\mathbb{R}$. Pelo que vimos acima, podemos supor que

$$I^2 = -1, \quad J^2 = -1, \ldots .$$

Agora, I+J e I-J satisfazem equações quadráticas reais, digamos

$$(I+J)^2 + \alpha_1(I+J) + \beta_1 = 0$$

(8.1)

$$(I-J)^2 + \alpha_2(I-J) + \beta_2 = 0.$$

Somando, obtemos

$$(\alpha_1+\alpha_2)I + (\alpha_1-\alpha_2)J + \beta_1 + \beta_2 - 4 = 0.$$

Como 1, I, J são linearmente independentes, isto força $\alpha_1 = \alpha_2 = 0$. Consequentemente de (8.1) segue que

$$IJ + JI = 2\mu, \quad (I+J)^2 = 2\mu-2, \quad (I-J)^2 = -2\mu-2$$

onde μ é um número real. Como I+J e I-J não são reais, temos que $\pm 2\mu-2 < 0$ e portanto

$$1-\mu^2 = 1/4\ (2\mu-2)(-2\mu-2) > 0.$$

Seja

$$i = I, \quad j = \frac{J+\mu I}{\sqrt{1-\mu^2}}.$$

Então

$$i^2 = -1, \quad j^2 = -1, \quad ij = -ji$$

e podemos tomar $1, i, j, \ldots$ para uma base de D sobre $\mathbb{R}$.

O produto ij não pode ser escrito como uma combinação linear de 1, i, j; caso contrário teríamos uma contradição (cf. §2). Assim, devemos ter $n \geq 4$ e podemos considerar $k = ij$ como o quarto elemento básico. Logo, se $n=4$ D é equivalente a álgebra dos quaternios reais.

Suponhamos agora que $n > 4$. Então D contém um quinto elemento básico ℓ tal que $\ell^2 = -1$. Como antes,

$$i\ell + \ell i = \mu_1, \quad j\ell + \ell j = \mu_2, \quad k\ell + \ell k = \mu_3$$

onde μ_1, μ_2 e μ_3 são números reais. Portanto,

$$\ell k = (\ell i)j = (\mu_1 - i\ell)j = \mu_1 j - i(\mu_2 - j\ell) = \mu_1 j - \mu_2 i + k\ell.$$

Somando ℓk em ambos os lados, obtemos

$$2\ell k = \mu_1 j - \mu_2 i + \mu_3.$$

Multiplicando agora por k à direita, segue que

$$-2\ell = \mu_1 i + \mu_2 j + \mu_3 k,$$

contradizendo o fato de que ℓ é linearmente independente de i, j, k. Com isto o teorema está demonstrado.

É interessante observar que o problema não terminou tão cedo para álgebras com divisão não associativas (= associativas ou não) sobre os reais. Uma classificação destas álgebras só se concretizou com o uso de métodos não triviais de topologia algébrica. Em 1940 Hopf [20] mostrou que a dimensão de uma álgebra com divisão não associativa sobre os reais tinha que ser uma potência de 2. Em 1957 Bott e Milnor [6] e Kervaire [23] mostraram que as únicas dimensões possíveis são 1 (os números reais), 2 (os números complexos), 4 (os quaternios reais), e 8 (os números de Cayley). Isto é, a classificação final nos dá exatamente os exemplos clássicos.

9. Álgebras com divisão.

Antes de prosseguir com os conceitos gerais necessários para o desenvolvimento da teoria, convém considerar o problema da construção de álgebras com divisão sobre um corpo arbitrário. O Exemplo 1 (§5) compreende todas as álgebras com divisão comutativas e até agora só identificamos uma algebra com divisão não comutativa, a saber, os quaternios reais. Além disso, vimos no parágrafo anterior que sobre o corpo real não há nada mais a dizer. A sugestão oferecida no Exemplo 3 (§5) de considerarmos os quaternios sobre um corpo arbitrario nem sempre produz álgebras com divisão. Vimos lá mesmo que os quaternios sobre o corpo complexo não formam uma álgebra com divisão. Na verdade, sobre o corpo complexo ou mais geralmente sobre um corpo algebricamente fechado, temos o seguinte

Lema 9.1 - Seja K um corpo algebricamente fechado. Se D é uma álgebra com divisão sobre K, então $D = K$.

Demonstração: Como estamos considerando álgebras de dimensão finita, todo elemento em D é algébrico sobre K. Seja $a \in D$; então $f(a) = 0$ para algum polinômio mônico $f(x)$ com coeficientes em K. Sendo K algebricamente fechado $f(x) = \pi(x-\alpha_i)$, $\alpha_i \in K$ e portanto $0 = f(a) = \pi(a-\alpha_i)$ (o leitor cuidadoso observará que estamos identificando os escalares α com os multiplos escalares $\alpha 1$). Como D é uma álgebra com divisão, segue que $a-\alpha_i = 0$ para algum i, e consequentemente $a = \alpha_i \in K$. Em outras palavras, $D = K$.

Voltando à discussão anterior e recordando o teorema dos quatro quadrados ([18] pp.302-303), concluimos que também os quaternios sobre um corpo de caracterísca $p \neq 0$ não formam uma álgebra com divisão. Com efeito, existem inteiros $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ tais que $p = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2$ e daí resulta que o quaternio $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \neq 0 \pmod{p}$ não é inversível. Por outro lado, para um corpo K tal que $\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 0$ $(\alpha_i \in K)$ implica $\alpha_0 = \alpha_1 = \alpha_2 = \alpha_3 = 0$, é imediato que os quaternios sobre K formam uma álgebra com divisão. Isto se verifica em particular quando K é um subcorpo de $\mathbb{R}$.

Por exemplo, seja $\mathbb{Q}(a)$ uma extensão quadrática do corpo $\mathbb{Q}$ dos números racionais. Os quaternios

$$\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \qquad \alpha_i \in \mathbb{Q}(a)$$

formam uma álgebra com divisão de dimensão 4 sobre $\mathbb{Q}(a)$ (com base 1, i, j, k) e portanto de dimensão 8 sobre $\mathbb{Q}$ (com base 1, i, j, k, a, ai, aj, ak). Mais geralmente, considerando uma extensão finita de $\mathbb{Q}$ de grau n, obtemos uma álgebra com divisão não comutativa de dimensão 4n sobre $\mathbb{Q}$.

Nos próximos dois parágrafos discutiremos brevemente álgebras com divisão de dimensão n^2. Na verdade trataremos apenas os casos n=2 e n=3.

10. Quaternios generalizados.

Seja K um corpo de característica $\neq 2$.

Teorema 10.1 - Se D é uma álgebra com divisão não comutativa de dimensão 4 sobre K, então podemos escolher uma base $1, i, j, ij$ para D com a seguinte tábua de multiplicação:

$$i^2 = \gamma, \quad j^2 = \delta, \quad ij = -ji \qquad (\gamma,\delta \in K). \tag{10.1}$$

Demonstração: Claramente todo elemento de D satisfaz um polinômio de grau ≤ 4 com coeficientes em K. Se para algum $a \in D$ o polinômio minimal é de grau 4, então $1, a, a^2, a^3$ são linearmente independentes sobre K e portanto formam uma base de D sobre K. Como as potências de a comutam entre si teríamos que D é comutativo, contrário à hipótese. Logo, todo elemento em D satisfaz um polinômio de grau ≤ 3 com coeficientes em K. Suponhamos agora que para algum $a \in D$ o polinômio minimal é de grau 3. Então $1, a, a^2$ são linearmente independentes sobre K e, além disso, existe $b \in D$ tal que $b \notin K(a)$ (isto é, b não é representável como um polinômio em a). Assim, $1, a, a^2, b$ formam uma base de D sobre K. Em particular, podemos escrever

$$ab = \alpha_0 + \alpha_1 a + \alpha_2 a^2 + \alpha_3 b \qquad (\alpha_i \in K),$$

ou o que é o mesmo

$$(a-\alpha_3)b = \alpha_0 + \alpha_1 a + \alpha_2 a^2.$$

Como $a \notin K$, temos que $a-\alpha_3 \neq 0$ e portanto

$$b = (a-\alpha_3)^{-1}(\alpha_0+\alpha_1 a+\alpha_2 a^2) \in K(a),$$

uma contradição. Logo, se $a \in D$ e $a \notin K$, o polinômio minimal de a sobre K é quadrático.

Seja $a \in D$, $a \notin K$. Pelo que acabamos de observar, 1, a é uma base de $K(a)$ sobre K. Seja $b \in D$ tal que $b \notin K(a)$. Afirmamos que 1, a, b, ab são linearmente independentes sobre K. Com efeito suponhamos que

$$\alpha_o + \alpha_1 a + \alpha_2 b + \alpha_3 ab = 0 \qquad (\alpha_i \in K);$$

então

$$(\alpha_2+\alpha_3 a)b = -\alpha_o - \alpha_1 a.$$

Se $\alpha_2+\alpha_3 a = 0$, segue que $\alpha_2 = \alpha_3 = 0$ (pois 1, a são linearmente independentes) e onsequentemente $\alpha_o = \alpha_1 = 0$ (pela mesma razão). Se $\alpha_2+\alpha_3 a \neq 0$, então

$$b = (\alpha_2+\alpha_3 a)^{-1} (-\alpha_o-\alpha_1 a) \in K(a)$$

contradizendo a escolha de b. Com isto a afirmação segue. Em outras palavras 1, a, b, ab formam uma base de D sobre K. Construiremos a partir desta a base desejada.

Sabemos que o polinômio de b sobre K é quadrático; como a característica de K é $\neq 2$, podemos escrever este polinômio na forma $x^2 + 2\alpha x + \beta$ $(\alpha, \beta \in K)$. Seja $j = b+\alpha$; então $j \notin K(a)$ pois $b \notin K(a)$. Assim, como antes, 1, a, j, aj formam uma base de D sobre K. Além disso,

$$j^2 = (b+\alpha)^2 = b^2 + 2\alpha b + \alpha^2 = \delta$$

onde $\delta = -\beta+\alpha^2 \in K$.

Seja $j_o = a^{-1}ja$; então $j_o \neq j$ (pois D não é comutativo) e

$$j_o^2 = a^{-1}j^2 a = a^{-1}\delta a = \delta = j^2.$$

Logo, para $c = j - j_o$ temos que $c \neq 0$ e $cj + j_o c = 0$. Portanto,

$$-j = c^{-1} j_o c = (ac)^{-1} j (ac).$$

Seja $i = ac$. Se $i \in K$ ou j é um polinômio em i, então j comuta com i e consequentemente $-j = j$, contradizendo o fato de que a característica de K é $\neq 2$. Assim, $i \notin K$ e $j \notin K(i)$, nos permitindo concluir que $1, i, j, ij$ constitui uma base de D sobre K.

Agora, $-j = i^{-1} j i$ e portanto $-i = jij^{-1}$. Daí segue que i e $-i$ tem o mesmo polinômio minimal. Como a característica de K é $\neq 2$ e o polinômio minimal de i é quadrático concluimos que $i^2 = \gamma \in K$. Com sto o teorema está demonstrado.

Não é para toda escolha de γ e δ em K que (10.1) determina uma álgebra com divisão. Por exemplo, se γ ou δ é um quadrado em K, o leitor verificará facilmente que uma tal álgebra não existe. Entretanto, temos o seguinte

Teorema 10.2 - Seja D uma álgebra com unidade de dimensão 4 sobre K tendo como elementos básicos $1, i, j, ij$ onde a multiplicação é determinada por (10.1). Se δ não é a norma de nenhum elemento da extensão quadrática $K(i)$, então D é uma álgebra com divisão.

Aqui a norma de $\alpha_o + \alpha_1 i \in K(i)$ é definida por

$$N(\alpha_o + \alpha_1 i) = (\alpha_o + \alpha_1 i)(\alpha_o - \alpha_1 i) = \alpha_o^2 - \gamma \alpha_1^2.$$

Demonstração: Seja $a \neq 0$ em D. Podemos escrever

$$a = \alpha_o+\alpha_1 i+\alpha_2 j+\alpha_3 ij = (\alpha_o+\alpha_1 i) + (\alpha_2+\alpha_3 i)j$$

onde os $\alpha_i \in K$ nem todos nulos. Precisamos mostrar que a é inversível.

Se $\alpha_2+\alpha_3 i = 0$, $a = \alpha_o+\alpha_1 i \neq 0$ é inversível em $K(i)$ e portanto inversível em D.

Suponhamos agora que $\alpha_2+\alpha_3 i \neq 0$. Então $\alpha_2+\alpha_3 i$ é inversível e podemos escrever

$$(\alpha_2+\alpha_3 i)^{-1}a = (\alpha_2+\alpha_3 i)^{-1}(\alpha_o+\alpha_1 i) + j.$$

Logo, para concluir que a é inversível basta mostrar que um elemento da forma $\beta_o + \beta_1 i + j$ é inversível. Ora,

$$(\beta_o+\beta_1 i+j)(\beta_o-\beta_1 i-j) = \beta_o^2 - \gamma\beta_1^2 - \delta \in K$$

e $\beta_o^2 - \gamma\beta_1^2 - \delta \neq 0$ pois caso contrário $\delta = \beta_o^2 - \gamma\beta_1^2 = N(\beta_o+\beta_1 i)$. Portanto,

$$(\beta_o+\beta_1 i+j)^{-1} = \frac{\beta_o-\beta_1 i-j}{\beta_o^2-\gamma\beta_1^2-\delta}$$

e o resultado segue.

Em particular, se $K = \mathbb{R}$ e $\gamma = \delta = -1$, D é a álgebra dos quaternios reais.

11. Álgebras cíclicas.

Vamos examinar os quaternios reais de um ponto de vista diferente do que fizemos até agora. Um quaternio real pode ser

escrito como

$$(\alpha_o+\alpha_1 i) + (\alpha_2+\alpha_3 i)j = a_1 + a_2 j$$

onde $a_1 = \alpha_o+\alpha_1 i$ e $a_2 = \alpha_2+\alpha_3 i$ são números complexos. Além disso, de $ij = -ji$ segue-se que

$$a_2 j = (\alpha_2+\alpha_3 i)j = \alpha_2 j - \alpha_3 ji = j(\alpha_2-\alpha_3 i) = j\bar{a}_2$$

onde $\bar{a}_2 = \alpha_2-\alpha_3 i$ é a imagem de a_2 pelo automorfismo $a \to \bar{a}$ que a todo complexo associa seu conjugado. Deste modo, obtemos uma nova formulação dos quaternios reais em relação a qual a multiplicação é determinada pelas seguintes relações:

$$j^2 = -1; \qquad aj = j\bar{a} \quad \text{para} \quad a \in C.$$

Assim, a multiplicação depende de uma extensão quadrática de $\mathbb{R}$, $\mathbb{R}(i) = C$, e do automorfismo $a \to \bar{a}$ desta extensão. Podemos ainda dizer que esta nova formulação dos quaternios depende da equação (cíclica) $x^2+1 = 0$ sobre $\mathbb{R}$ e do grupo (cíclico) dos automorfismos de $\mathbb{R}(i)$ sobre $\mathbb{R}$. Note que um argumento análogo se aplica para os quaternios generalizados (§10).

Isto motiva o procedimento que passamos a descrever para a construção de álgebras sobre um corpo arbitrário K.

Sejam K um corpo e $f(x)$ um polinômio de grau n com coeficientes em K, $f(x)$ irredutível sobre K. Dizemos que $f(x) = 0$ é uma <u>equação cíclica</u> sobre K se as suas raizes podem ser representadas por

$$a, \theta(a), \theta^2(a) = \theta[\theta(a)],\ldots,\theta^{n-1}(a)$$

onde a é uma raiz qualquer de $f(x)$, $\theta(x)$ é um polinômio com coeficientes em K e $\theta^n(a) = a$.

Por exemplo, $x^2+1 = 0$ é uma equação cíclica sobre $\mathbb{R}$; aqui, $\theta(x) = -x$ Um outro exemplo é dado por $x^2-x-1 = 0$ que é uma equação cíclica sobre o corpo Q dos números racionais. Se a é uma de suas raizes, a outra raiz é $\theta(a) = 1-a$ já que a soma das raizes é 1; assim, $\theta(x) = 1-x$ e $\theta^2(a) = 1-(1-a) = a$.

Sejam $f(x) = 0$ uma equação cíclica de grau n sobre o corpo K e a uma de suas raizes:

$$f(a) = 0,\ f[\theta(a)] = 0,\ldots,f[\theta^{n-1}(a)] = 0,\quad \theta^n(a) = a$$

Sejam $x^n-\delta = 0$ $(\delta\in K)$ uma equação binomial irredutível sobre K e b uma de suas raizes:

$$b^n = \delta.$$

Consideremos agora o espaço ve orial D n^2-dimensional sobre K que consiste de todas as combinaçoes lineares formais

$$\sum_{i,j=0}^{n-1} \alpha_{ij} b^i a^j \qquad\qquad \alpha_{ij} \in K$$

onde os elementos $b^i a^j$ $(i,j = 0,\ldots,n-1)$ são declarados linear mente independentes sobre K, e onde adição e multiplicação por escalares são definidas de maneira natural. Introduzimos uma multiplicação em D de maneira distributiva e forçando a associatividade de acordo com as seguintes relações:

$$ab = b\theta(a),\quad a^2b = ab\theta(a) = b\theta(a)^2,\ldots,a^rb = b\theta(a)^r,\ \ldots\ .$$

Assim, qualquer que seja o polinomio $g(x)$ com coeficientes em K, temos

$$g(a)b = bg[\theta(a)]$$

e, por indução,

$$g(a)b^r = b^r g[\theta^r(a)] \qquad r \geq 0.$$

Precisamos verificar que D é fechado em relação a esta multiplicação. Ora, o produto de dois elementos básicos quaisquer, $b^i a^j$ e $b^k a^\ell$, pode ser escrito como

$$(b^i a^j)(b^k a^\ell) = b^{i+k}[\theta^k(a)]^j a^\ell = b^r g(a)$$

onde $r = i+k$ e $g(x) = [\theta^k(x)]^j x^\ell$ é um polinômio com coeficientes em K. Como $b^n = \delta$ e $f(a) = 0$, podemos substituir r por um inteiro não negativo $<n$ e $g(x)$ por um polinômio de grau $<n$. Portanto, a expressão resultante para o produto de dois elementos básicos é uma combinação linear dos elementos básicos. Finalmente, o leitor verificará que de fato vale a lei associativa mostrando que

$$[(b^i a^j)(b^k a^\ell)](b^r a^s) = (b^i a^j)[(b^k a^\ell)(b^r a^s)].$$

Assim, concluimos que D é uma álgebra sobre K.

Suponhamos que $n=2$ e K é um corpo de característica $\neq 2$. Neste caso podemos tomar $f(x) = x^2 + 2\alpha x + \beta$ e, substituindo a por $a+\alpha$ se necessário, podemos supor que $a^2 = \gamma \in K$ onde γ não é um quadrado em K. Deste modo, $\theta(a) = -a$ e D é uma álgebra de dimensão 4 sobre K com uma base 1, a, b, ba onde

$$a^2 = \gamma, \quad b^2 = \delta \quad \text{e} \quad ab = -ba.$$

Se δ não é a norma de nenhum elemento da extensão quadrática

$K(a)$ então, pelo Teorema 10.2, D é uma álgebra com divisão.

Para $n=3$ temos o seguinte

Teorema 11.1 - Se $n=3$ e δ não é a norma de nenhum elemento da extensão cúbica $K(a)$, então D é uma álgebra com divisão.

Aqui a norma de $g(a) \in K(a)$ é definida por

$$N[g(a)] = g(a)g[\theta(a)]g[\theta^2(a)].$$

Demonstração: Seja $u = \sum_{i,j=0}^{2} \alpha_{ij} b^i a^j \in D$, $u \neq 0$. Podemos escrever

$$u = g_1(a) + bg_2(a) + b^2 g_3(a)$$

onde $g_i(a) = \sum_{j=0}^{2} \alpha_{ij} a^j$, $i=1,2,3$. Para mostrar que u é inversível vamos considerar três casos.

1) $g_3(a) = g_2(a) = 0$. Aqui $u = g_1(a) \neq 0$ é inversível em $K(a)$ e portanto inversível em D.

2) $g_3(a) = 0$ e $g_2(a) \neq 0$. Neste caso, $g_2(a)$ é inversível e podemos escrever

$$ug_2(a)^{-1} = g_1(a)g_2(a)^{-1} + b.$$

Seja $g(a) = -g_1(a)g_2(a)^{-1}$. Para concluir que u é inversível basta mostrar que $b-g(a)$ é inversível. Ora,

$$(b-g(a))(b^2+bg[\theta^2(a)] + g[\theta(a)]g[\theta^2(a)])$$

$$= \delta - g(a)g[\theta(a)]g[\theta^2(a)] = \delta - N[g(a)] \in K$$

e, por hipótese, $\delta - N[g(a)] \neq 0$. Logo, $b-g(a)$ é inversível

$$[b-g(a)]^{-1} = \frac{b^2+bg[\theta^2(a)]+g[\theta(a)]g[\theta^2(a)]}{\delta-N[g(a)]} .$$

3) $g_3(a) \neq 0$. Aqui podemos escrever

$$ug_3(a)^{-1} = g_1(a)g_3(a)^{-1} + bg_2(a)g_3(a)^{-1} + b^2.$$

Sejam $g(a) = g_1(a)g_3(a)^{-1}$ e $h(a) = g_2(a)g_3(a)^{-1}$. Para concluir que u é inversível basta mostrar que $g(a) + bh(a) + b^2$ é inversível. Ora,

$$\{b-h[\theta(a)]\}\{g(a)+bh(a)+b^2\}$$

$$= bg(a) + b^2h(a) + \delta - h[\theta(a)]g(a) - bh[\theta^2(a)]h(a) - b^2h(a)$$

$$= \{-h[\theta(a)]g(a)+\delta\} + b\{g(a)-h[\theta^2(a)]h(a)\}$$

$$= q(a) + bp(a).$$

Pelo segundo caso, $b-h[\theta(a)]$ é inversível e $q(a) + bp(a)$ é inversível desde que $\neq 0$. Mas $q(a) + bp(a) = 0$ implica que

$$\delta = h[\theta(a)]g(a) \quad \text{e} \quad g(a) = h[\theta^2(a)]h(a),$$

e consequentemente $\delta = N[h(a)]$, uma contradição. Logo, $q(a) + bp(a) \neq 0$ é inversível e

$$\{q(a)+bp(a)\}^{-1}\{b-h[\theta(a)]\}\{g(a)+bh(a)+b^2\} = 1.$$

Com isto o teorema está demonstrado.

Enunciamos a seguir uma condição suficiente para que D seja uma álgebra com divisão no caso geral:

Teorema - Se nenhuma potência de δ menor que a n-ésima é a norma

de um polinômio em a com coeficientes em K, então D é uma álgebra com divisão.

A demonstração deste resultado pode ser encontrada em [11] pp. 221-226.

Terminamos este parágrafo com uma receita para a construção de uma álgebra com divisão de dimensão 9 sobre o corpo Q dos números racionais, a saber, considere a álgebra cíclica definida sobre Q por

$$a^3-3a+1 = 0, \quad b^3 = 2, \quad ab = b(a^2-2).$$

12. Subálgebras.

Os subsistemas, assim como outros conceitos que introduziremos mais adiante, são definidos respeitando-se ambas as estruturas em questão:

Dizemos que um subconjunto B de uma K-álgebra A é uma subálgebra de A se B é um K-subespaço vetorial de A fechado em relação a multiplicação.

Por exemplo, o corpo C dos números complexos contém uma infinidade de R-subespaços vetoriais e uma infinidade de subcorpos. Entretanto, considerado como uma R-álgebra, C contém apenas duas subálgebras $\neq 0$, a saber R e o próprio C.

Toda álgebra A contém duas subálgebras triviais, a saber 0 e o próprio A. Toda interseção de subálgebras de A é ainda uma subálgebra de A. Se S é um subconjunto qualquer de

A, a interseção das subálgebras contendo S é chamada a <u>subálgebra de</u> A <u>gerada por</u> S.

Se A é uma K-álgebra com unidade, então o subconjunto K1 formado por todos os múltiplos escalares $\alpha 1$ ($\alpha \in K$) é uma subálgebra de A. Como já observamos no §6, podemos identificar K com K1 através da correspondência $\alpha \to \alpha 1$ ($\alpha \in K$). Com esta identificação os escalares comutam com todos os elementos de A; isto é, quaisquer que sejam $\alpha \in K$ e $a \in A$, temos

$$(\alpha 1)a = \alpha(1a) = \alpha(a1) = a(\alpha 1).$$

Já vínhamos usando este fato por algum tempo.

Em qualquer álgebra A seja Z o subconjunto que consiste de todos os elementos $z \in A$ que satisfazem a seguinte condição:

$$az = za \quad \text{para todo} \quad a \in A.$$

Não é difícil verificar que Z é uma subálgebra. Os elementos de Z são ditos <u>centrais</u> em A e Z é chamado o <u>centro</u> de A. Claramente, A é comutativa se e somente se Z = A. Se A é uma álgebra com unidade, os escalares $\alpha \equiv \alpha 1$ são centrais em A.

O centro da álgebra dos quaternios reais é precisamente $R \simeq R1$.

O centro da álgebra K_n das matrizes $n \times n$ sobre um corpo K é precisamente K; ou seja, o centro de K_n consiste de todas as matrizes escalares

$$\alpha 1_n = \begin{pmatrix} \alpha & & 0 \\ & \alpha & \\ & & \ddots \\ 0 & & \alpha \end{pmatrix} \qquad \alpha \in K.$$

Mais geralmente, se A é uma álgebra com unidade de centro Z, então o centro de A_n consiste de todas as matrizes

$$\begin{pmatrix} a & & 0 \\ & a & \\ & & \ddots \\ 0 & & a \end{pmatrix} \qquad a \in Z.$$

Neste caso, com as devidas identificações, vemos que o centro de A_n coincide com o centro de A. Isto não ocorre necessariamente para álgebras sem unidade. Por exemplo, se $A = (\epsilon_1, \epsilon_2)_K$ onde $\epsilon_1^2 = \epsilon_1\epsilon_2 = \epsilon_2\epsilon_1 = 0$ e $\epsilon_2^2 = \epsilon_2$, então

$$\begin{pmatrix} \epsilon_1 & 0 \\ 0 & 0 \end{pmatrix}$$

é um elemento central em A_2.

13. A representação regular.

Terminamos este capítulo mostrando que toda K-álgebra é equivalente a uma subálgebra da álgebra de matrizes K_n para um n apropriado.

Seja A uma K-álgebra qualquer. Para cada $a \in A$ pode-

mos associar uma transformação linear em A, a saber a <u>multiplicação à direita</u> por a:

$$R_a: x \to xa.$$

Deste modo obtemos uma aplicação $a \to R_a$ de A em $\mathfrak{L}(A)$, a álgebra das transformações lineares em A. Além disso, se $a,b \in A$ e $\alpha \in K$ então

$$(13.1) \qquad R_{a+b} = R_a+R_b, \quad R_{\alpha a} = \alpha R_a \quad \text{e} \quad R_{ab} = R_aR_b.$$

Logo, $A_R = \{R_a \mid a \in A\}$ é uma subálgebra de $\mathfrak{L}(A)$.

Suponhamos que A é uma álgebra com unidade. Então, a elementos distintos $a \neq b$ correspondem transformações lineares distintas $R_a \neq R_b$, pois $1R_a \neq 1R_b$. Assim, de (13.1) concluimos que as álgebras A e A_R são equivalentes. Se $\mathfrak{e}_1,\ldots,\mathfrak{e}_n$ é uma base de A sobre K, o isomorfismo é dado por

$$a = \Sigma\alpha_i\mathfrak{e}_i \to R_a = \Sigma\alpha_i R_{\mathfrak{e}_i}.$$

A representação de $R_{\mathfrak{e}_j}$ $(j=1,\ldots,n)$ como uma matriz $n\times n$ sobre K (com respeito a base $\mathfrak{e}_1,\ldots,\mathfrak{e}_n$) é

$$M_{R_{\mathfrak{e}_j}} = \begin{pmatrix} \gamma_{1j1} & \gamma_{1j2} & \cdots & \gamma_{1jn} \\ \gamma_{2j1} & \gamma_{2j2} & \cdots & \gamma_{2jn} \\ \cdots & \cdots & \cdots & \cdots \\ \gamma_{nj1} & \gamma_{nj2} & \cdots & \gamma_{njn} \end{pmatrix}$$

onde $\mathfrak{e}_i\mathfrak{e}_j = \sum_{k=1}^{n} \gamma_{ijk}\mathfrak{e}_k$, e A é equivalente à subálgebra de K_n gerada por estas matrizes. Esta subálgebra, também indicada por

A_R, é chamada a <u>representação regular à direita</u> de A (com respeito a base $\epsilon_1,\ldots,\epsilon_n$).

De maneira análoga, considerando para $a \in A$ a <u>multiplicação à esquerda</u> por a

$$L_a: x \to ax$$

podemos falar na <u>representação regular à esquerda</u> de A $(a \to L_a)$, indicada por A_L. Notamos entretanto que A e A_L são álgebras recíprocas, pois $L_{ab} = L_b L_a$ quaisquer que sejam $a,b \in A$.

Suponhamos agora que A é uma álgebra sem unidade, e seja como antes $\epsilon_1,\ldots,\epsilon_n$ uma base de A sobre K. Então, pela adjunção de um elemento básico ϵ_o tal que

$$\epsilon_o\epsilon_i = \epsilon_i\epsilon_o = \epsilon_i \qquad (i=0,1,\ldots,n),$$

obtemos uma álgebra $\tilde{A}$ com unidade, de dimensão $n+1$ sobre K, e contendo A como subálgebra. Assim, podemos representar $\tilde{A}$, e portanto A, como uma subálgebra de K_{n+1}.

Para concluir vejamos alguns exemplos.

1) A aplicação

$$\alpha+\beta_i \to \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$$

nos dá uma representação dos complexos como uma subálgebra de R_2.

2) A aplicação

$$\alpha_o+\alpha_1 i+\alpha_2 j+\alpha_3 k \to \begin{pmatrix} \alpha_o & \alpha_1 & \alpha_2 & \alpha_3 \\ -\alpha_1 & \alpha_o & -\alpha_3 & \alpha_2 \\ -\alpha_2 & \alpha_3 & \alpha_o & -\alpha_1 \\ -\alpha_3 & -\alpha_2 & \alpha_1 & \alpha_o \end{pmatrix}$$

nos dá uma representação dos quaternios reais como uma subálgebra de R_4.

CAPÍTULO 2

O RADICAL

As partes nilpotentes de uma álgebra representam um obstáculo para a determinação de sua estrutura. Não temos muito controle sobre estas partes pois, por exemplo, elas podem nos conduzir a relações triviais. Por outro lado, determinaremos no próximo capítulo a estrutura das álgebras sem ideais nilpotentes $\neq 0$, e portanto é desejável um processo que nos permita passar de uma álgebra qualquer para uma álgebra deste tipo. Nosso objetivo aqui será descrever um tal processo.

14. Homomorfismos, ideais e álgebras quocientes.

Sejam A e A' duas álgebras sobre o mesmo corpo K. Uma aplicação

$$\varphi: A \to A'$$

é chamada um homomorfismo se preserva tanto a estrutura de espaço vetorial quanto a estrutura multiplicativa de A, isto é,

$$\varphi(a+b) = \varphi(a)+\varphi(b), \quad \varphi(\alpha a) = \alpha\varphi(a), \quad \varphi(ab) = \varphi(a)\varphi(b)$$

quaisquer que sejam $a,b \in A$ e $\alpha \in K$. Um isomorfismo (§7) é então um homomorfismo bijetivo.

Seja $\varphi: A \to A'$ um homomorfismo.

O conjunto de todos os elementos $\varphi(a)$ quando a percorre

A recebe o nome de <u>imagem</u> de φ e será indicado por $\mathrm{Im}\,\varphi$. Claramente $\mathrm{Im}\,\varphi$ é uma subálgebra de A'; φ é sobrejetivo se e somente se $\mathrm{Im}\,\varphi = A'$.

O <u>núcleo</u> ou <u>kernel</u> de φ é o conjunto de todos os elementos $a \in A$ tais que $\varphi(a) = 0$, e será indicado por $\mathrm{Ker}\,\varphi$. O leitor verificará facilmente que $\mathrm{Ker}\,\varphi$ é um subespaço vetorial de A invariante em relação à multiplicação à esquerda e à direita por elementos de A (isto é, se $a \in A$ e $b \in \mathrm{Ker}\,\varphi$ então os produtos ab e ba estão em $\mathrm{Ker}\,\varphi$). Em particular, $\mathrm{Ker}\,\varphi$ é uma subálgebra de A. É também imediato que φ é injetivo se e somente se $\mathrm{Ker}\,\varphi = 0$.

Continuamos com mais algumas definições.

Um subconjunto $\mathfrak{B}$ de uma álgebra A diz-se um <u>ideal à esquerda</u> de A se $\mathfrak{B}$ é um subespaço vetorial de A invariante em relação à multiplicação à esquerda por elementos de A ($ab \in \mathfrak{B}$ para todo $a \in A$ e $b \in \mathfrak{B}$). De maneira análoga define-se <u>ideal à direita</u>. Por exemplo, se A é uma álgebra qualquer e $a \in A$, os "múltiplos" à esquerda e à direita de a

$$Aa = \{xa \mid x \in A\} \quad \text{e} \quad aA = \{ax \mid x \in A\}$$

são respectivamente ideais à esquerda e à direita de A.

Um subconjunto $\mathfrak{B}$ de uma álgebra A diz-se um <u>ideal bilateral</u> ou simplesmente <u>ideal</u> de A se $\mathfrak{B}$ é simultaneamente um ideal à esquerda e à direita de A. Neste sentido, o núcleo de um homomorfismo $\varphi: A \to A'$ é um ideal de A. Se A é uma álgebra comutativa e $a \in A$, os múltiplos à esquerda e à direita de

a coincidem e formam um ideal de A.

Todo ideal lateral ou bilateral de uma álgebra A é em particular uma subálgebra de A. Toda álgebra A contém dois ideais triviais, a saber, 0 e o próprio A. Toda interseção de ideais à esquerda (direita ou bilaterais) de A é ainda um ideal à esquerda (direita ou bilateral) de A. Se S e um subconjunto qualquer de A, a interseção de todos os ideais à esquerda (direita ou bilaterais) de A que contém S é chamada o <u>ideal à esquerda</u> (<u>direita ou bilateral</u>) <u>gerado por</u> S.

Veremos a seguir que todo ideal de uma K-álgebra A é o núcleo de algum homomorfismo.

Com efeito, seja $\mathfrak{B}$ um ideal de A. Definimos em A uma relação binária (congruência módulo $\mathfrak{B}$) da seguinte forma.

$$a \equiv a' \pmod{\mathfrak{B}} \quad \text{se} \quad a-a' \in \mathfrak{B}.$$

Trata-se evidentemente de uma relação de equivalência. Aqui, a classe de equivalência determinada por um elemento $a \in A$ é

$$\bar{a} = a+\mathfrak{B} = \{a+b \mid b \in \mathfrak{B}\}.$$

Definimos então operações de adição, multiplicação por escalares e multiplicação sobre estas classes da seguinte forma:

$$\bar{a} + \bar{a'} = \overline{a + a'}, \qquad \alpha\bar{a} = \overline{\alpha a}, \qquad \bar{a}\bar{a'} = \overline{aa'}.$$

Não é difícil verificar que esta definição não depende da escolha dos representantes. Deste modo, obtemos uma K-álgebra chamada <u>álgebra quociente</u> de A pelo ideal $\mathfrak{B}$, que indicaremos por $A/\mathfrak{B}$. Finalmente, a aplicação natural $a \to \bar{a}$ de A sobre $A/\mathfrak{B}$ é um

homomorfismo cujo núcleo é precisamente $\mathfrak{B}$.

Note que para cada ideal $\mathfrak{J}$ de A contendo $\mathfrak{B}$, $\mathfrak{J}/\mathfrak{B} = \{\bar{a} \mid a \in \mathfrak{J}\}$ é um ideal de $A/\mathfrak{B}$. Reciprocamente, se $\mathfrak{J}$ é um ideal do quociente $A/\mathfrak{B}$, existe um único ideal $\mathfrak{J}$ de A contendo $\mathfrak{B}$ tal que $\mathfrak{J} = \mathfrak{J}/\mathfrak{B}$, a saber, $\mathfrak{J} = \{a \in A \mid \bar{a} \in \mathfrak{J}\}$.

Para concluir, observamos que dados um homomorfismo $\varphi: A \to A'$, j a aplicação natural de A no quociente $A/\mathrm{Ker}\,\varphi$ e i a inclusão de $\mathrm{Im}\,\varphi$ em A', então existe um único isomorfismo $\bar{\varphi}: A/\mathrm{Ker}\,\varphi \to \mathrm{Im}\,\varphi$ tal que o diagrama

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & A' \\ {\scriptstyle j}\downarrow & & \uparrow{\scriptstyle i} \\ A/\mathrm{Ker}\,\varphi & \xrightarrow{\bar{\varphi}} & \mathrm{Im}\,\varphi \end{array}$$

é comutativo (isto é, $\varphi = i \circ \bar{\varphi} \circ j$).

15. Ideais nilpotentes.

Se a é um elemento qualquer de uma álgebra A indicamos o produto aa por a^2, aaa por a^3, e assim por diante. Dizemos que a é nilpotente se $a^m = 0$ para algum inteiro positivo m.

Se $\mathfrak{B}$ e $\mathfrak{C}$ são ideais à esquerda (direita ou bilaterais) de A, indicamos por $\mathfrak{BC}$ o subgrupo aditivo de A gerado pelos produtos bc onde $b \in \mathfrak{B}$, $c \in \mathfrak{C}$. Em outras palavras, $\mathfrak{BC}$ consiste de todas as somas finitas

$$b_1c_1 + b_2c_2 + \ldots + b_rc_r \qquad b_i \in \mathfrak{B},\ c_i \in C,\ r \geq 1.$$

É imediato que $\mathfrak{B}C$ é um ideal à esquerda (direita ou bilateral) de A. Definimos as potências de $\mathfrak{B}$ indutivamente por

$$\mathfrak{B}^n = \mathfrak{B}^{n-1}\mathfrak{B} \quad \text{onde} \quad \mathfrak{B}^1 = \mathfrak{B}.$$

Assim, $\mathfrak{B}^n$ consiste de todas as somas finitas

$$\sum_{i=1}^{r} b_{i_1} b_{i_2} \ldots b_{i_n} \qquad b_{i_j} \in \mathfrak{B},\ r \geq 1.$$

Dizemos que $\mathfrak{B}$ é <u>nilpotente</u> se alguma potência de $\mathfrak{B}$ é zero. Neste caso, o menor inteiro m tal que $\mathfrak{B}^m = 0$ é chamado o <u>índice de nilpotência</u> de $\mathfrak{B}$.

Evidentemente, dizer que $\mathfrak{B}^m = 0$ equivale a dizer que o produto de quaisquer m elementos de $\mathfrak{B}$ é zero, Portanto, se $\mathfrak{B}$ é nilpotente segue-se que todos os elementos de $\mathfrak{B}$ são nilpotentes. Reciprocamente, temos o seguinte

<u>Teorema 15.1</u> - Seja A uma álgebra n-dimensional sobre um corpo K e seja $\mathfrak{B}$ um ideal lateral de A. Se todo elemento de $\mathfrak{B}$ é nilpotente, então $\mathfrak{B}$ é nilpotente e o índice de nilpotência de $\mathfrak{B}$ é no máximo n+1.

<u>Demonstração</u>: Suponhamos que $\mathfrak{B}$ é um ideal à esquerda de A cujos elementos são nilpotentes. Sejam $a_1, \ldots, a_{n+1} \in \mathfrak{B}$ e consideremos a seguinte cadeia de subespaços de A:

$$\mathfrak{B} \supseteq \mathfrak{B}a_{n+1} \supseteq \mathfrak{B}a_n a_{n+1} \supseteq \ldots \supseteq \mathfrak{B}a_1 \ldots a_n a_{n+1}.$$

Como $\dim_K A = n$ temos que $\mathfrak{B} = \mathfrak{B}a_{n+1}$ ou para algum r, $2 \leq r \leq n+1$, $\mathfrak{B}a_r \ldots a_n a_{n+1} = \mathfrak{B}a_{r-1}a_r \ldots a_n a_{n+1}$. Em todo caso,

para algum s, $1 \leq s \leq n+1$, existe $b \in \mathfrak{B}$ tal que $a_s \cdots a_{n+1} = b(a_s \cdots a_{n+1})$. Multiplicando à esquerda por potências de b, obtemos $a_s \cdots a_{n+1} = b^t(a_s \cdots a_{n+1})$ para todo $t \geq 1$. Daí resulta que $a_s \cdots a_{n+1} = 0$, pois por hipótese b é nilpotente, e consequentemente $a_1 a_2 \cdots a_{n+1} = 0$. Como estes são $n+1$ elementos arbitrários de $\mathfrak{B}$, concluimos que $\mathfrak{B}^{n+1} = 0$ e o teorema está demonstrado.

Exemplo 1 - Seja A um espaço vetorial não nulo sobre um corpo K. Se definimos $ab = 0$ quaisquer que sejam $a,b \in A$, obtemos uma álgebra nilpotente com índice de nilpotência 2.

Exemplo 2 - Seja $A = (\varepsilon_1, \varepsilon_2)$ uma álgebra bi-dimensional sobre um corpo K com a seguinte tábua de multiplicação:

$$\varepsilon_1^2 = \varepsilon_2, \quad \varepsilon_1\varepsilon_2 = \varepsilon_2\varepsilon_1 = \varepsilon_2^2 = 0.$$

Então A é uma álgebra nilpotente com índice de nilpotência 3. Note que podemos representar A como uma subálgebra de K_3 da seguinte forma:

$$\alpha_1\varepsilon_1 + \alpha_2\varepsilon_2 \to \begin{pmatrix} 0 & \alpha_1 & \alpha_2 \\ 0 & 0 & \alpha_1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Exemplo 3 - Seja K um corpo e n um inteiro >1. Seja A a subálgebra de K_n que consiste de todas as matrizes triangulares estritamente superiores,

$$\begin{pmatrix} 0 & a_{12} & a_{13} & \cdots & a_{1n} \\ 0 & 0 & a_{23} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & a_{n-1\,n} \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \qquad a_{ij} \in K.$$

Então A é uma álgebra nilpotente com índice de nilpotência n+1.

Observação: Se a e b são elementos que comutam entre si (isto é, ab = ba) então para todo inteiro positivo n temos que $(ab)^n = a^n b^n$; além disso, podemos desenvolver o binômio

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + \ldots + b^n .$$

Logo, neste caso, se a ou b é nilpotente segue-se que o produto ab é nilpotente; se a e b são ambos nilpotentes, a soma a+b é também nilpotente. Isto não acontece necessariamente quando $ab \neq ba$. Por exemplo, sejam

$$a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} .$$

Então $a^2 = b^2 = 0$, mas para todo inteiro $n > 1$

$$(ab)^n = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad (a+b)^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

portanto ab e a+b não são nilpotentes.

Assim, concluímos que os elementos nilpotentes numa álge-

bra comutativa formam um ideal, o que não ocorre em geral nas álgebras não comutativas.

Seja A uma álgebra comutativa e seja N o ideal formado pelos elementos nilpotentes de A. Então N contém todo ideal nilpotente de A; além disso, pelo Teorema 15.1, N é por si próprio um ideal nilpotente. Neste sentido, dizemos que N é um ideal nilpotente maximal. Claramente, N é o único ideal nilpotente maximal de A.

No próximo parágrafo veremos que em qualquer álgebra, comutativa ou não, existe sempre um ideal com estas propriedades.

16. O ideal nilpotente maximal.

Se $\{\mathfrak{B}_\gamma\}$ é uma coleção qualquer de ideais à esquerda (direita ou bilaterais) de uma álgebra A, definimos a soma dos $\mathfrak{B}_\gamma$, $\Sigma\, \mathfrak{B}_\gamma$, como o conjunto de todas as somas finitas

$$b_{\gamma_1} + b_{\gamma_2} + \ldots + b_{\gamma_r} \qquad\qquad b_{\gamma_i} \in \mathfrak{B}_{\gamma_i}.$$

Em outras palavras, $\Sigma\, \mathfrak{B}_\gamma$ é o ideal à esquerda (direita ou bilateral) de A gerado pela união dos $\mathfrak{B}_\gamma$.

Vamos mostrar que a soma de todos os ideais nilpotentes de uma álgebra A é ainda um ideal nilpotente de A e, além disso, esta soma contém todo ideal lateral nilpotente de A. Para começar, temos o seguinte

Lema 16.1 - Se $\mathfrak{B}_1$ e $\mathfrak{B}_2$ são ideais à esquerda (direita) nilpotentes de A, então $\mathfrak{B}_1+\mathfrak{B}_2$ é um ideal à esquerda

(direita) nilpotente de A.

Demonstração: Sejam m_1 e m_2 os índices de nilpotência de $\mathfrak{B}_1$ e $\mathfrak{B}_2$ respectivamente. Mostraremos que $\mathfrak{B}_1+\mathfrak{B}_2$ é nilpotente com índice de nilpotência menor ou igual a m_1+m_2-1. Com efeito, seja $m = m_1+m_2-1$. Os elementos de $(\mathfrak{B}_1+\mathfrak{B}_2)^m$ são somas de produtos $a = a_1a_2\ldots a_m$ com fatores em $\mathfrak{B}_1$ ou $\mathfrak{B}_2$. Suponhamos que r dos fatores estão em $\mathfrak{B}_1$. Como $\mathfrak{B}_1$ e $\mathfrak{B}_2$ são ideais à esquerda (direita) de A, grupando os fatores de maneira apropriada podemos escrever

$$a = \ldots x_1x_2\ldots x_r\ldots = \ldots y_1y_2\ldots y_{m-r}\ldots$$

onde $x_1,\ldots,x_r \in \mathfrak{B}_1$ e $y_1,\ldots,y_{m-r} \in \mathfrak{B}_2$. Se $r \geq m_1$ o fato de que $\mathfrak{B}_1^{m_1} = 0$ força $a = 0$. Se $r < m_1$ então $m-r = (m_1+m_2-1) - r \geq m_2$ e consequentemente $a = 0$, pois $\mathfrak{B}_2^{m_2} = 0$. Em todo caso, concluimos que $(\mathfrak{B}_1+\mathfrak{B}_2)^m = 0$ como queriamos demonstrar.

Uma consequência imediata é o seguinte

Corolário - Se $\mathfrak{B}$ é um ideal à esquerda (direita) nilpotente de A, então $\mathfrak{B}$ gera um ideal bilateral nilpotente de A, a saber, $\mathfrak{B} + \mathfrak{B}A$ (respectivamente $\mathfrak{B} + A\mathfrak{B}$).

Demonstração: Suponhamos que $\mathfrak{B}$ é um ideal à esquerda nilpotente de A, digamos que $\mathfrak{B}^m = 0$. Então

$$(\mathfrak{B}A)^m = \mathfrak{B}A\mathfrak{B}A\ldots\mathfrak{B}A = \mathfrak{B}(A\mathfrak{B})(A\mathfrak{B})\ldots(A\mathfrak{B})A \subseteq \mathfrak{B}^mA = 0$$

e, pelo Lema, concluimos que $\mathfrak{B} + \mathfrak{B}A$ é um ideal nilpotente.

Seja agora N a soma de todos os ideais nilpotentes de A. Se $a \in N$ então $a = \mathfrak{B}_{\gamma_1} + \ldots + \mathfrak{B}_{\gamma_r}$, uma soma finita de ideais

nilpotentes de A. Pelo Lema 16.1 extendido de dois para qualquer número finito de ideais, segue-se que a é um elemento nilpotente. Assim, pelo Teorema 15.1, N é um ideal nilpotente de A. Finalmente, pelo colorário acima, N contém todo ideal lateral nilpotente de A. Acabamos de provar o

Teorema 16.2 - Todo ideal lateral ou bilateral nilpotente de uma álgebra A está contido em um (único) ideal nilpotente maximal de A, indicado por $N(A)$.

$N(A)$ é chamado o radical de A.

O próximo resultado nos diz que tomando-se o quociente pelo radical podemos passar de uma álgebra qualquer, A, para uma álgebra sem ideais nilpotentes $\neq 0$.

Teorema 16.3 - $N(A/N(A)) = 0$.

Demonstração: Suponhamos que $\bar{\mathfrak{B}}$ é um ideal nilpotente de $\bar{A} = A/N(A)$, digamos que $\bar{\mathfrak{B}}^m = 0$. Seja $\mathfrak{B}$ o ideal correspondente de A tal que $\bar{\mathfrak{B}} = \mathfrak{B}/N(A)$. Então $\mathfrak{B}^m \subseteq N(A)$ e consequentemente $\mathfrak{B}^{mn} \subseteq N(A)^n$ para todo $n \geq 1$. Como $N(A)$ é nilpotente segue-se que $\mathfrak{B}$ é um ideal nilpotente de A. Assim, $\mathfrak{B} \subseteq N(A)$ e portanto $\bar{\mathfrak{B}} = 0$. Em outras palavras, $\bar{A}$ não contém ideais nilpotentes $\neq 0$ e o teorema está demonstrado.

No caso especial de uma álgebra comutativa A, este resultado nos diz que $A/N(A)$ não contém elementos nilpotentes.

Para concluir, seja K um corpo e seja

$$A = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \mid \alpha, \beta \in K \right\}.$$

O leitor verificará facilmente que

$$N(A) = \left\{ \begin{pmatrix} 0 & \beta \\ 0 & 0 \end{pmatrix} \mid \beta \in K \right\}.$$

Assim, $A/N(A) \simeq K \oplus K$ (a soma direta de duas cópias de K).

17. Elementos propriamente nilpotentes.

Já vimos que numa álgebra comutativa o radical é precisamente o conjunto de todos os elementos nilpotentes. Daremos a seguir uma caracterização análoga para o radical de uma álgebra qualquer, comutativa ou não. Para isso precisamos de uma definição.

Dizemos que um elemento a de uma álgebra A é <u>propriamente nilpotente</u> se ax e xa são nilpotentes para todo $x \in A$.

Note que se a é propriamente nilpotente, então $aa = a^2$, e portanto a, é nilpotente. Entretanto, pode ocorrer que um elemento nilpotente não é propriamente nilpotente (exemplifique).

Note também que a definição acima é redundante pois ax é nilpotente se e somente se xa é nilpotente. Com efeito, basta observar que para todo inteiro positivo n, $(ax)^{n+1} = a(xa)^n x$ e $(xa)^{n+1} = x(ax)^n a$.

Assim, pelo Teorema 15.1, concluimos que a é propriamente nilpotente se e somente se aA é um ideal à esquerda nilpoten

te ou, equivalentemente, Aa é um ideal a direita nilpotente.

É claro que todo elemento em $N(A)$ é propriamente nilpotente. Mais do que isso, temos o seguinte

Teorema 17.1 - $N(A)$ é precisamente o conjunto de todos os elementos propriamente nilpotentes de A.

A demonstração cabe ao leitor (sugestão: basta mostrar que os elementos propriamente nilpotentes formam um ideal nilpotente de A).

18. Duas propriedades do radical.

Seja $\mathfrak{B}$ um ideal de uma álgebra A. Então, em particular, $\mathfrak{B}$ é também uma álgebra e podemos perguntar se o radical de $\mathfrak{B}$ está relacionado de alguma forma com o radical de A. Claramente $N(A) \cap \mathfrak{B} \subseteq N(\mathfrak{B})$, pois $N(A) \cap \mathfrak{B}$ é um ideal nilpotente de $\mathfrak{B}$. Agora, se $N(\mathfrak{B})^m = 0$ e a é um elemento qualquer de $N(\mathfrak{B})$,

$$(Aa)^{2m} = [(AaA)a]^m \subseteq (\mathfrak{B}a)^m \subseteq N(\mathfrak{B})^m = 0;$$

consequentemente a é um elemento propriamente nilpotente de A. Assim, concluimos que $N(\mathfrak{B}) \subseteq N(A) \cap \mathfrak{B}$. Isto nos dá o seguinte

Teorema 18.1 - Se $\mathfrak{B}$ é um ideal de uma álgebra A então

$$N(\mathfrak{B}) = N(A) \cap \mathfrak{B}.$$

O resultado é falso se supomos apenas que $\mathfrak{B}$ é um ideal lateral de A. Por exemplo, consideremos a álgebra K_2 das matrizes 2×2 sobre um corpo K. Não é difícil verificar que

$N(K_2) = 0$ (ou se quiser use o próximo teorema). Entretanto, se

$$\rho = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix} \mid \alpha, \beta \in K \right\}$$

então ρ é um ideal à direita de K_2 e $N(\rho) \neq N(K_2) \cap \rho = 0$ pois

$$N(\rho) = \left\{ \begin{pmatrix} 0 & \beta \\ 0 & 0 \end{pmatrix} \mid \beta \in K \right\} \neq 0.$$

Uma outra pergunta interessante é se podemos relacionar o radical de uma álgebra A com o radical da álgebra A_n das matrizes $n \times n$ com coeficientes em A. A resposta é dada pelo seguinte

Teorema 18.2 - $N(A_n) = N(A)_n$.

Demonstração: É imediato que $N(A)_n$ é um ideal nilpotente de A_n; portanto, $N(A)_n \subseteq N(A_n)$. Resta mostrar que $N(A_n) \subseteq N(A)_n$. Primeiro observamos que pela adjunção de uma unidade se necessário e considerando os elementos de A como matrizes escalares, podemos escrever toda matriz de A_n como $\sum_{i,j=1} a_{ij}e_{ij}$ onde os a_{ij} estão em A e os e_{ij} são as matrizes unitárias usuais. A seguir notamos que se $\sum_{i,j=1} a_{ij}e_{ij} \in N(A_n)$ então os a_{ij} são nilpotentes. Com efeito, para $k, \ell = 1, \ldots, n$,

$$(a_{k\ell}e_{1k})\left(\sum_{i,j=1}^{n} a_{ij}e_{ij}\right)(a_{k\ell}e_{\ell 1}) = a_{k\ell}^3 e_{11} \in N(A_n)$$

pois $N(A_n)$ é um ideal de A_n. Daí resulta que $a_{k\ell}^3$, e portanto $a_{k\ell}$, é nilpotente. Agora, como para todo $x \in A$

$$x\left(\sum_{i,j=1}^{n} a_{ij}e_{ij}\right) = \sum_{i,j=1}^{n} (xa_{ij})e_{ij} ,$$

segue-se que os coeficientes das matrizes de $N(A_n)$ são elementos propriamente nilpotentes de A. Assim, concluimos que $N(A_n) \subseteq N(A)_n$ e o teorema está demonstrado.

CAPÍTULO 3

OS TEOREMAS DE ESTRUTURA

Podemos dividir as álgebras em duas classes, a saber, as nilpotentes e as não nilpotentes. Não tratamos aqui as álgebras nilpotentes. Para uma álgebra não nilpotente consideramos o seu radical, que é por sua vez uma álgebra nilpotente. Tomando-se o quociente pelo radical, obtemos o que chamamos de álgebra semisimples. Toda álgebra semisimples é uma soma direta de álgebras simples e estas são álgebras de matrizes com coeficientes em álgebras com divisão. Este é o conteúdo dos teoremas de estrutura de Wedderburn.

19. Álgebras semisimples.

Dizemos que uma álgebra A é semisimples se A não contém ideais nilpotentes $\neq 0$. Equivalentemente, A é semisimples se o radical de A, $N(A)$, é nulo.

Para toda álgebra A, o quociente $A/N(A)$ é semisimples (§16). Se A é uma álgebra semisimples, todo ideal de A é semisimples e a álgebra A_n das matrizes $n \times n$ com coeficientes em A é também semisimples (§18).

Um bom número de exemplos pode ser obtido a partir do seguinte:

Teorema de Maschke - Seja G um grupo finito e K um corpo de característica 0 ou característica p onde p não divide a ordem de G. Então a álgebra de grupo $K(G)$ é semisimples.

Demonstração: Sejam $g_1 = 1, g_2, \ldots, g_n$ os elementos de G. Se $a = \sum_{i=1}^{n} \alpha_i g_i \in K(G)$ podemos escrever $R_a = \sum_{i=1}^{n} \alpha_i R_{g_i}$ onde para $x \in K(G)$, R_x é a multiplicação à direita por x. Seja N o radical de $K(G)$ e suponhamos que $a = \sum_{i=1}^{n} \alpha_i g_i \in N$, $a \neq 0$. Como N é um ideal, podemos supor que $\alpha_1 \neq 0$ pois caso contrário, multiplicando a pelo g_i^{-1} apropriado obtemos o elemento desejado. Como $a \in N$, a é nilpotente e portanto $R_a = \sum_{i=1}^{n} \alpha_i R_{g_i}$ é uma transformação linear nilpotente. Logo, o traço de R_a ($\operatorname{tr} R_a$) é zero e podemos escrever

$$0 = \operatorname{tr} R_a = \alpha_1 \operatorname{tr} R_1 + \alpha_2 \operatorname{tr} R_{g_2} + \ldots + \alpha_n \operatorname{tr} R_{g_n}.$$

Mas se $g \in G$ e $g \neq 1$, $\operatorname{tr} R_g = 0$ pois $g_i g \neq g_i$ $(i=1,\ldots,n)$. Como $\operatorname{tr} R_1 = \circ(G)$ segue-se que $\alpha_1 \circ(G) = 0$. Consequentemente, como $\alpha_1 \neq 0$, devemos ter $\circ(G) = 0$ em K. Isto só é possível se a característica de K é $p \neq 0$ e divide a ordem de G, contrário às nossas hipóteses. Assim, concluimos que $N = 0$ e o teorema está demonstrado.

Finalmente, observamos que se G é um grupo finito e K é um corpo de característica $p \neq 0$ onde p divide a ordem de G, então $K(G)$ não é semisimples. Com efeito, se $a = \sum_{g \in G} g$ então a é um elemento não nulo central em $K(G)$; além disso, $ag = a$ para todo $g \in G$. Logo, como p divide a ordem de G,

$a^2 = \sum_{g\in G} ag = \circ(G)a = 0$. Como a é central, segue-se que $K(G)a$ é um ideal nilpotente $\neq 0$ de $K(G)$. Assim, $K(G)$ não é semi-simples.

20. Idempotentes.

Dizemos que um elemento $e \neq 0$ de uma álgebra A é um idempotente se $e^2 = e$. Os elementos idempotentes desempenham um papel fundamental na teoria das álgebras Já em 1870 num trabalho pioneiro de B. Peirce [27] encontramos uma prova racional da existência de idempotentes em álgebras não nilpotentes. Provaremos isto agora.

Teorema 20.1 - Se A é uma lgebra nã nilpotente então A contém um elemento idempotente.

Demonstração: Seja $a \in A$ um elemento não nilpotente. Pelo Teorema 15.1 um tal elemento existe. Consideremos a seguinte cadeia de subespaços de A:

$$Aa \supseteq Aa^2 \supseteq \ldots \supseteq Aa^n \supseteq \ldots .$$

Como A é de dimensão finita, existe um inteiro $m \geq 1$ tal que

$$(*) \qquad Aa^m = Aa^{m+1} = \ldots = Aa^{2m} = Aa^{2m+1} = \ldots .$$

Seja $B = Aa^m$ Então $b = a^{m+1} = aa^m \in B$ e de $(*)$ segue-se que $Bb = B$. Em particular, existe $e \in B$ tal que $eb = b$. Multiplicando por e à esquerda, obtemos $(e^2-e)b = 0$. Agora, como $Bb = B$, a transformação linear em B dada por $x \to xb$ é sobrejetiva. Como B é de dimensão finita, esta transformação é tam-

bém injetiva. Assim, de $(e^2-e)b = 0$ concluimos que $e^2 = e$. Resta mostrar que $e \neq 0$. Ora, se $e = 0$ então $0 = eb = b = a^{m+1}$ contradizendo o fato de que a não é nilpotente Isto completa a demonstração.

O próximo resultado é de grande importância.

Teorema 20.2 - Seja A uma álgebra semisimples e seja $\mathfrak{B} \neq 0$ um ideal à esquerda (direita) de A. Então $\mathfrak{B} = Ae$ (respectivamente $\mathfrak{B} = eA$) para algum idempotente e.

Demonstração: Seja $\mathfrak{B} \neq 0$ um ideal à esquerda de A. Como A é semisimples, $\mathfrak{B}$ não é nilpotente. Logo, pelo teorema anterior, $\mathfrak{B}$ contém elementos idempotentes. Se $e \in \mathfrak{B}$ é um idempotente seja $\mathrm{an}_{\mathfrak{B}}(e) = \{b \in \mathfrak{B} \mid be = 0\}$ o anulador à esquerda de e em $\mathfrak{B}$. É imediato que $\mathrm{an}_{\mathfrak{B}}(e)$ é um ideal à esquerda de A.

Suponhamos que $e_o \in \mathfrak{B}$ é um idempotente tal que $\mathrm{an}_{\mathfrak{B}}(e_o) \neq 0$. Então $\mathrm{an}_{\mathfrak{B}}(e_o)$ contém um idempotente e_1. Como $e_o^2 = 0$, $e_1^2 = e_1$ e $e_1 e_o = 0$, segue-se que $f_o = e_o + e_1 - e_o e_1$ é um elemento idempotente em $\mathfrak{B}$. Além disso, $\mathrm{an}_{\mathfrak{B}}(f_o)$ está contido em $\mathrm{an}_{\mathfrak{B}}(e_o)$ pois dado $a \in \mathfrak{B}$ tal que $af_o = 0$, então

$$0 = (af_o)e_o = a(e_o+e_1-e_oe_1)e_o = ae_o^2 = ae_o.$$

Como $e_1 f_o = e_1(e_o+e_1-e_oe_1) = e_1^2 = e_1$, concluimos que $\mathrm{an}_{\mathfrak{B}}(e_o) \supsetneq \mathrm{an}_{\mathfrak{B}}(f_o)$. Se $\mathrm{an}_{\mathfrak{B}}(f_o) \neq 0$, repetimos a discussão com f_o no lugar de e_o; deste modo, obtemos

$$\mathrm{an}_{\mathfrak{B}}(e_o) \supsetneq \mathrm{an}_{\mathfrak{B}}(f_o) \supsetneq \mathrm{an}_{\mathfrak{B}}(g_o)$$

onde $g_o \in \mathfrak{B}$ é um idempotente. Como A é de dimensão finita este processo termina. Assim, $an_{\mathfrak{B}}(e) = 0$ para algum idempotente $e \in \mathfrak{B}$. Neste caso $b = be$ qualquer que seja $b \in \mathfrak{B}$, pois $(b-be)e = 0$. Portanto, $\mathfrak{B} = Ae$ e o teorema está demonstrado.

Corolário 1 - Se A é uma álgebra semisimples e $\mathfrak{B} \neq 0$ é um ideal de A, então $\mathfrak{B} = Ae = eA$ onde e é um idempotente central de A.

Demonstração: Como $\mathfrak{B}$ é simultaneamente um ideal à esquerda e à direita de A, existem idempotentes $e_1, e_2 \in \mathfrak{B}$ tais que $be_1 = b$ e $e_2 b = b$ para todo $b \in \mathfrak{B}$. Em particular, $e_1 = e_2 e_1 = e_2$. Logo, $e = e_1 = e_2$ é uma unidade para $\mathfrak{B}$ e $\mathfrak{B} = Ae = eA$. Agora, se $a \in A$ então ambos os produtos ae e ea estão em $\mathfrak{B}$, pois $\mathfrak{B}$ é um ideal de A. Assim, o fato de que e é uma unidade para $\mathfrak{B}$ implica que $ae = e(ae)$ $(ea)e = ea$. Em outras palavras, e comuta com todos os elementos de A e o resultado segue.

Terminamos esta seção com o seguinte

Corolário 2 - Se A é uma álgebra semisimples então A tem elemento unidade.

21. Decomposição em componentes simples.

Dizemos que uma álgebra A é simples se $A^2 \neq 0$ e os únicos ideais de A são os triviais.

Seja A uma álgebra simples. Como A^2 é um ideal de A,

a condição $A^2 \neq 0$ é equivalente à condição $A^2 = A$. Segue-se que $A = A^2 = A^3 = \ldots$ e portanto A não contém ideais nilpotentes $\neq 0$.

Assim, toda álgebra simples é semisimples. Em particular toda algebra simples tem unidade.

Nosso objetivo a seguir é mostrar que toda álgebra semisimples é uma soma direta de álgebras simples. Para isso, introduziremos inicialmente o conceito de ideal minimal.

Dizemos que um ideal $\mathfrak{B}$ de uma álgebra A é um ideal minimal de A se $\mathfrak{B} \neq 0$ e não existe nenhum ideal $\mathfrak{B}'$ de A tal que $0 \neq \mathfrak{B}' \subsetneq \mathfrak{B}$.

Nos três lemas subsequentes A é uma álgebra semisimples.

Lema 21.1 - Se $\mathfrak{B}$ é um ideal minimal de A então $\mathfrak{B}$ é uma álgebra simples.

Demonstração: Claramente $\mathfrak{B}^2 \neq 0$ pois por hipótese A é semisimples. Resta mostrar que os únicos ideais de $\mathfrak{B}$ são os triviais. Suponhamos que $\mathfrak{J} \neq 0$ é um ideal de $\mathfrak{B}$. Então $\mathfrak{B}\mathfrak{J}\mathfrak{B}$ é um ideal de A e está contido em $\mathfrak{B}$. Se $\mathfrak{B}\mathfrak{J}\mathfrak{B} = 0$ segue-se que $\mathfrak{J}^3 = 0$, contradizendo o fato de que $\mathfrak{B}$ como um ideal de uma álgebra semisimples é também uma álgebra semisimples; logo, $\mathfrak{B}\mathfrak{J}\mathfrak{B} \neq 0$. Assim, pela minimalidade de $\mathfrak{B}$ concluimos que $\mathfrak{B} = \mathfrak{B}\cdot\mathfrak{B} \subseteq \mathfrak{J}$ e portanto $\mathfrak{J} = \mathfrak{B}$. Com isto o lema está demonstrado.

Lema 21.2 - Se $\mathfrak{B}_1, \ldots, \mathfrak{B}_r$ são ideais minimais de A distintos dois a dois, a soma $\mathfrak{B}_1 + \ldots + \mathfrak{B}_r$ é direta. Em par-

ticular, A contém apenas um número finito de ideais minimais.

Demonstração: Sabemos que $\mathfrak{B}_i = e_iA = Ae_i$ onde e_i é um idempotente central em A, $i = 1,\ldots,r$ (cf. §20). Observamos a seguir que os idempotentes $e_1,\ldots,e_r$ são dois a dois ortogonais, isto é, $e_ie_j = 0$ se $i \neq j$. Com efeito, $\mathfrak{B}_i \cap \mathfrak{B}_j$ é um ideal de A e está contido tanto em $\mathfrak{B}_i$ quanto em $\mathfrak{B}_j$. Se $e_ie_j \neq 0$ teríamos $\mathfrak{B}_i \cap \mathfrak{B}_j \neq 0$ e a minimalidade de $\mathfrak{B}_i$ e $\mathfrak{B}_j$ implicaria que $\mathfrak{B}_i = \mathfrak{B}_i \cap \mathfrak{B}_j = \mathfrak{B}_j$, contradizendo as hipóteses.

Suponhamos agora que $e_1a_1 + \ldots + e_ra_r = 0$ $(a_i \in A)$. Multiplicando esta expressão à esquerda por e_i e usando o fato de que $e_ie_j = 0$ para $i \neq j$, obtemos $e_ia_i = e_i^2a_i = 0$. Em outras palavras a soma $\mathfrak{B}_1 + \ldots + \mathfrak{B}_r$ é direta. Finalmente, a última asserção do lema segue do fato de que A é de dimensão finita.

Lema 21.3 - Se $\mathfrak{B}_1,\ldots,\mathfrak{B}_r$ são todos os ideais minimais de A, então $A = \mathfrak{B}_1 \oplus \ldots \oplus \mathfrak{B}_r$.

Demonstração: Pelo lema anterior basta mostrar que $A = \mathfrak{B}_1 + \ldots + \mathfrak{B}_r$. Como antes, $\mathfrak{B}_i = e_iA = Ae_i$ onde os e_i são idempotentes centrais em A tais que $e_ie_j = 0$ se $i \neq j$. Seja $e = e_1 + \ldots + e_r$. Uma simples verificação revela que e é um idempotente central em A; além disso, $e_ie = e_i$, $i = 1,\ldots,r$. Afirmamos que $e = 1$, a unidade de A. Com efeito, suponhamos por absurdo que $e \neq 1$. Então $\mathfrak{B} = (1-e)A = A(1-e)$ é um ideal não nulo de A. Como tal, $\mathfrak{B}$ contém um ideal minimal de A, digamos $\mathfrak{B}_{i_o}$. Assim, podemos escrever $e_{i_o} = (1-e)a$ para algum $a \in A$. Multiplicando à esquerda por e_{i_o}, obtemos $e_{i_o} = e_{i_o}^2 =$

$= e_{i_o}(1-e)a = 0$ pois $e_{i_o}e = e_{i_o}$. Com esta contradição concluimos que de fato $e = 1$. Logo, para todo $a \in A$, $a = 1a = e_1a + \ldots + e_ra$ e consequentemente $A = \mathfrak{B}_1 + \ldots + \mathfrak{B}_r$ como queriamos demonstrar.

Acabamos de provar o teorema de Wedderburn sobre a estrutura das álgebras semisimples.

Teorema 21.4 - Toda álgebra semisimples é uma soma direta de álgebras simples.

Este resultado terá uma forma bem mais interessante assim que determinarmos a estrutura das álgebras simples.

22. A simplicidade de D_n.

Seja D uma álgebra com divisão e n um inteiro positivo. Vamos examinar a álgebra D_n das matrizes $n \times n$ com coeficientes em D. Começaremos com o seguinte

Lema 22.1 - D_n é uma álgebra simples.

Demonstração: Claramente a multiplicação em D_n não é trivial, isto é, $D_n^2 \neq 0$. O resultado seguirá se mostrarmos que os únicos ideais de D_n são os triviais. Suponhamos então que $U \neq 0$ é um ideal de D_n. Seja $u \in U$, $u \neq 0$. Se e_{ij} $(i,j = 1,\ldots,n)$ são as matrizes unitárias usuais de D_n, podemos escrever $u = \sum_{i,j=1}^{n} a_{ij}e_{ij}$ onde os a_{ij} estão em D e $a_{k\ell} \neq 0$ para algum k e algum ℓ. Como U é um ideal de D_n, $w = \sum_{r=1}^{n} a_{k\ell}e_{rr} = \sum_{r=1}^{n} e_{rk}ue_{\ell r} \in U$. Como $a_{k\ell} \neq 0$, w é uma ma-

triz inversível com $w^{-1} = \sum_{r=1}^{n} a_{k\ell}^{-1} e_{rr}$; logo, $1_n = w^{-1}w \in U$ onde 1_n é a matriz identidade. Daí resulta que $D_n = D_n 1_n \subseteq U$ e portanto $U = D_n$. Isto conclui a demonstração.

Vemos então que a disposição dos ideais bilaterais de D_n não apresenta dificuldades.

O que podemos dizer sobre os ideais laterais de D_n? Se $n = 1$ a resposta é imediata: os únicos ideais laterais de D são os triviais. Assim, daqui por diante vamos supor $n > 1$.

Sejam $\rho_1, \rho_2, \ldots, \rho_n$ os ideais à direita de D_n gerados pelas matrizes unitárias idempotentes $e_{11}, e_{22}, \ldots, e_{nn}$ respectivamente (isto é, $\rho_i = e_{ii}D_n$). Explicitamente

$$\rho_i = \left\{ \begin{pmatrix} 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ a_{i1} & a_{i2} & \ldots & a_{in} \\ 0 & 0 & \ldots & 0 \end{pmatrix} \;\middle|\; a_{ij} \in D \right\}$$

Note que $D_n = \rho_n \oplus \ldots \oplus \rho_n$, a soma direta dos ρ_i.

Afirmamos que os ρ_i são ideais à direita minimais de D_n. Para provar isto basta mostrar que o ideal à direita gerado por um elemento não nulo arbitrário de ρ_i é o próprio ρ_i. Seja pois $u = \sum_{j=1}^{n} a_{ij}e_{ij} \neq 0$ em ρ_i. Então $a_{ik} \neq 0$ para algum k e, se $v \in \rho_i$ temos que $u(a_{ik}^{-1} e_{ki})v = v$. Logo, $uD_n = \rho_i$ como queríamos e a afirmação segue.

Seja agora $\rho \neq 0$ um ideal à direita arbitrário de D_n. Como D_n é semisimples, $\rho = eD_n$ para alguma matriz idempotente e.

Por uma mudança de base, portanto um automorfismo interno de D_n, podemos colocar e numa forma diagonal, digamos $e \to f = e_{i_1 i_1} + \ldots + e_{i_r i_r}$ (aqui estamos considerando os elementos de D_n como transformações lineares em um espaço vetorial n-dimensional sobre D). Logo, $\rho = eD_n \simeq fD_n$; ou seja, $\rho \simeq \rho_{i_1} \oplus \ldots \oplus \rho_{i_r}$.

Assim, concluimos que todo ideal à direita de D_n é uma soma direta de ideais à direita minimais; todo ideal à direita minimal é isomorfo a algum ρ_i e os ρ_i são isomorfos entre si.

Finalmente, observamos que uma conclusão análoga vale para os ideais à esquerda de D_n. Basta considerar os ideais à esquerda minimais $\lambda_i = D_n e_{ii}$, $i = 1, \ldots, n$.

23. O Lema de Schur.

Apresentaremos agora um lema necessário para a demonstração do teorema principal sobre as álgebras simples. Primeiro uma definição.

Seja V um espaço vetorial sobre um corpo K e seja $\mathcal{S}$ um conjunto de transformações lineares em V. Um subespaço W de V diz-se $\mathcal{S}$-<u>invariante</u> se $WS \subseteq W$ para todo $S \in \mathcal{S}$. Dizemos que V e um $\mathcal{S}$-<u>espaço simples</u> se $V \neq 0$ e os únicos subespaços $\mathcal{S}$-invariantes são os triviais, isto é, 0 e o próprio V. Mantendo a notação temos o seguinte

<u>Lema 23.1</u> - Se V é um $\mathcal{S}$-espaço simples, e $T: V \to V$ é uma transformação linear não nula tal que $TS = ST$ para

todo $S \in \mathcal{S}$, entao T é inversível. Além disso, $T^{-1}S = ST^{-1}$ para todo $S \in \mathcal{S}$.

Demonstração: Como V é um $\mathcal{S}$-espaço simples e $T \neq 0$, basta mostrar que o núcleo e a imagem de T são subespaços $\mathcal{S}$-invariantes. De fato, se este for o caso, segue-se que o núcleo é zero, a imagem é todo o espaço V, e portanto T é inversível. Além disso, é imediato que de $TS = ST$ resulta $ST^{-1} = T^{-1}S$. Ora, se $vT = 0$ e $S \in \mathcal{S}$ então $vST = vTS = 0$; assim, o núcleo de T é realmente $\mathcal{S}$-invariante. Agora, se v' é um elemento na imagem de T então $v' = vT$ para algum $v \in V$. Logo, $v'S = vTS = vST$ está na imagem de T para todo $S \in \mathcal{S}$. Deste modo, a imagem de T é também $\mathcal{S}$-invariante e a demonstração está completa.

24. A estrutura das álgebras simples.

Estamos em condições de provar o teorema de Wedderburn sobre a estrutura das álgebras simples.

Teorema 24.1 - Se A é uma algebra simples então A é equivalente a D_n, a álgebra das matrizes $n \times n$ com coeficientes numa álgebra com divisão D. Além disso, n é único assim como D a menos de isomorfismo.

A demonstração será dividida em uma sequência de lemas e observações e até a sua conclusão denotaremos por A uma álgebra simples sobre um corpo K. Recordamos que como tal, A possui unidade.

Seja ρ um ideal à direita minimal de A. Então ρ é invariante em relação à multiplicação à direita por elementos de A, $R_a: x \to xa$. Assim, podemos considerar R_a $(a \in A)$ como transformações lineares em ρ. Aqui, por abuso de notação, estamos indicando R_a e sua restrição ao subespaço ρ pelo mesmo símbolo.

Lema 24.2 - Se $a \in A$ e $R_a = 0$ em ρ, então $a = 0$. Assim, $a \to R_a$ é uma imersão de A em $\mathfrak{L}(\rho)$, a álgebra das transformações lineares em ρ sobre K. Além disso, ρ é um A-espaço simples.

Demonstração: Vamos examinar o anulador à direita de ρ em A, isto é, $\mathfrak{B} = \{x \in A \mid \rho x = 0\}$. Claramente $\mathfrak{B}$ é um ideal bilateral de A e a simplicidade de A força $\mathfrak{B} = 0$ ou $\mathfrak{B} = A$. Como $\rho 1 \neq 0$, necessariamente $\mathfrak{B} = 0$. Ora, dizer que $R_a = 0$ em ρ equivale a dizer que $\rho a = 0$ e portanto, pelo que acabamos de deduzir, $a = 0$. O resultado segue naturalmente, a última asserção decorrendo do fato de que ρ é um ideal à direita minimal de A.

Seja agora

$$D = \{T \in \mathfrak{L}(\rho) \mid TR_a = R_aT \text{ para todo } a \in A\},$$

o centralizador de A em $\mathfrak{L}(\rho)$. Claramente D é uma subálgebra de $\mathfrak{L}(\rho)$. Como ρ é um A-espaço simples, o lema de Schur nos diz que D é uma álgebra com divisão. Podemos considerar ρ como um espaço vetorial à direita sobre D onde para $a \in \rho$ e $T \in D$, a ação aT é simplesmente a imagem de a pela transformação linear T.

Lema 24.3 - Se $x_1,\ldots,x_n \in \rho$ são linearmente independentes sobre D, então a soma $\rho x_1 + \ldots + \rho x_n$ é direta. Em particular, como A é de dimensão finita sobre K, ρ é de dimensão finita sobre D.

Demonstração: Primeiro o leitor deverá observar que as multiplicações à esquerda $L_b: x \to bx$ $(b \in \rho)$ são elementos de D. Agora, dizer que $b_1x_1 + \ldots + b_nx_n = 0$ $(b_i \in \rho)$ é equivalente a dizer que $x_1L_{b_1} + \ldots + x_nL_{b_n} = 0$. Como por hipótese $x_1,\ldots,x_n$ são linearmente independentes sobre D, o resultado segue.

Lema 24.4 - Se $x_1, \ldots, x_n$ é uma base de ρ sobre D e $y_1,\ldots,y_n$ são elementos arbitrários de ρ, então existe $a \in A$ tal que $x_ia = y_i$, $i = 1,\ldots,n$.

Demonstração: Basta mostrar que existem $a_1,\ldots,a_n \in A$ tais que $x_1a_i = y_i$ e $x_ja_i = 0$ para $i \neq j$, pois neste caso $a = a_1 + \ldots + a_n$ é o elemento desejado. Mostraremos, por exemplo como obter a_n (o mesmo argumento pode ser usado para determinar $a_1,\ldots,a_{n-1}$). Para isso, consideremos o ideal à esquerda de A, $\lambda = Ax_1 + \ldots + Ax_{n-1}$. Pelo Teorema 20.2, $\lambda = Ae$ onde e é um idempotente. Como $e(1-e) = 0$, temos que $x_i(1-e) = 0$ para $i = 1,\ldots,n-1$. Se $x_n(1-e) = 0$ então $R_{1-e} = 0$ em ρ e consequentemente, pelo Lema 24.2, $1-e = 0$.

Daí resulta que $\lambda = A$ e podemos escrever $c_1x_1 + \ldots + c_{n-1}x_{n-1} = 1$ $(c_i \in A)$. Multiplicando esta expressão à esquerda por x_n, obtemos $x_1L_{x_nc_1} + \ldots + x_{n-1}L_{x_nc_{n-1}} = x_n$. Isto contradiz a independência linear de $x_1,\ldots,x_n$ sobre D, pois $x_nc_i \in \rho$ e portanto

$L_{x_n c_i} \in D$. Assim, concluimos que $x_n(1-e) \neq 0$. Logo, $x_n(1-e)A \neq 0$ e a minimilidade de ρ força $x_n(1-e)A = \rho$. Em particular existe $b \in \rho$ tal que $x_n(1-e)b = y_n$. Colocando $a_n = (1-e)b$ o problema está resolvido.

Corolário - $A \simeq D_n$ onde $n = \dim_D \rho$

Demonstração: Seja $a \in A$. Como $R_a T = TR_a$ para todo $T \in D$, é imediato que $R_a \in \mathcal{L}_D(\rho)$, a álgebra das transformações lineares em ρ sobre D. Assim, temos um homomorfismo $\varphi: A \to \mathcal{L}_D(\rho)$. Pelo Lema 24.2 φ é injetivo e pelo Lema 24.4 φ é sobrejetivo. Deste modo $A \simeq \mathcal{L}_D(\rho)$. Como $\mathcal{L}_D(\rho) \simeq D_n$, onde $n = \dim_D \rho$, o resultado segue.

Para completar a demonstração do Teorema 24.1 precisamos verificar a unicidade de n e D.

Lema 24.5 - Se $D_n \simeq \Delta_m$ onde D e Δ são álgebras com divisão, então $n = m$ e $D \simeq \Delta$.

Demonstração: Seja $\varphi: D_n \to \Delta_m$ o isomorfismo. Seja

$$e = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix} \in D_n$$

e seja $f = \varphi(e)$. Como eD_n é um ideal à direita minimal de D_n, $f\Delta_m$ é um ideal à direita minimal de Δ_m. Por uma mudança de base, portanto um automorfismo de Δ_m, f pode ser colocado na forma

$$\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

onde I_r é a matriz identidade $r \times r$. A minimalidade de $f\Delta_m$ força $r = 1$. Assim, sem perda de generalidade, podemos supor que

$$f = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Logo, $D \simeq eD_n e \simeq f\Delta_m f \simeq \Delta$. Agora, como eD_n é n-dimensional sobre D, $f\Delta_m$ é m-dimensional sobre Δ, e $D \simeq \Delta$, segue-se que $n = m$.

Isto conclui a demonstração do teorema de Wedderburn.

25. A estrutura das álgebras semisimples.

Como toda álgebra semisimples é uma soma direta de álgebras simples, o teorema que acaabamos de provar tem como consequência imediata o seguinte

Teorema 25. 1 - Se A é uma álgebra semisimples então $A \simeq D_{n_1}^{(1)} \oplus \dots \oplus D_{n_r}^{(r)}$ onde $D^{(i)}$ é uma álgebra com divisão e $D_{n_i}^{(i)}$ é a álgebra das matrizes $n_i \times n_i$ com coeficientes em $D^{(i)}$, $i = 1, \dots, r$.

CAPÍTULO 4

ÁLGEBRAS SIMPLES

Uma álgebra A diz-se simples central sobre um corpo K se A é uma álgebra simples de centro K.

26. Produto tensorial de álgebras.

Sejam A e B álgebras sobre um corpo K. Seja $A \otimes_K B$ o produto tensorial de A e B como espaços vetoriais sobre K. Definimos uma multiplicação em $A \otimes_K B$ distributivamente de acordo com

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2.$$

Desta forma $A \otimes_K B$ é uma álgebra sobre K. Quando não houver ambiguidade escreveremos simplesmente $A \otimes B$ omitindo o corpo em questão.

Observação: 1) O produto tensorial de álgebras é associativo e comutativo

$$(A \otimes B) \otimes C \simeq A \otimes (B \otimes C), \qquad A \otimes B \simeq B \otimes A.$$

2) Sejam A, A', B, B' álgebras sobre K. Se

$$\varphi_1 : A \to A' \quad \text{e} \quad \varphi_2 : B \to B'$$

são homomorfismos, então a aplicação

$$\varphi_1 \otimes \varphi_2 : A \otimes B \to A' \otimes B'$$

definida por $\varphi_1 \otimes \varphi_2(a \otimes b) = \varphi_1(a) \otimes \varphi_2(b)$, é um homomorfismo.

3) Sejam A e B álgebras sobre K. Se B possui unidade, a aplicação $a \to a \otimes 1$ é um homomorfismo injetivo de A em $A \otimes B$; assim, podemos identificar A com $A \otimes 1$. Analogamente, se A possui unidade podemos identificar B com $1 \otimes B$.

Antes de prosseguir com o nosso estudo é conveniente apresentarmos dois lemas que serão usados com bastante frequência.

Lema 26.1 - Sejam A uma álgebra sobre um corpo K, A_n a álgebra das matrizes $n \times n$ com coeficientes em A e K_n a álgebra das matrizes $n \times n$ sobre K. Então $A_n \simeq A \otimes_K K_n$.

Demonstração: Sejam e_{ij} as matrizes unitárias de K_n. Pela adjunção de uma unidade (se necessário), todo elemento de A_n pode ser escrito de maneira única como $\Sigma a_{ij} e_{ij}$, $a_{ij} \in A$. É imediato que a aplicação

$$\Sigma\, a_{ij} e_{ij} \to \Sigma\, a_{ij} \otimes e_{ij}$$

é um isomorfismo de A_n sobre $A \otimes K_n$.

Lema 26.2 - $K_n \otimes_K K_m \simeq K_{nm}$.

Demonstração: Sejam e_{ij} e $f_{k\ell}$ $(i,j = 1,\ldots,n;\ k,\ell = 1,\ldots,m)$ as matrizes unitárias de K_n e K_m respectivamente. Então $e_{ij} \otimes f_{k\ell}$ é uma base de $K_n \otimes K_m$ com a mesma tábua de multiplicação que as matrizes unitárias de K_{nm}, etc...

27. A álgebra de multiplicações.

Sejam A uma algebra sobre um corpo K, $\mathfrak{L}(A)$ a álgebra das transformações lineares em A sobre K, e A_R e A_L as representações regulares à direita e à esquerda de A em $\mathfrak{L}(A)$ respectivamente. Os elementos de A_R são as multiplicações à direita, $R_a: x \to xa$, e os elementos de A_L são as multiplicaçoes à esquerda, $L_a: x \to ax$ $(a \in A)$. A subálgebra $\mathfrak{M}$ gerada por A_R e A_L em $\mathfrak{L}(A)$ é naturalmente chamada a álgebra de multiplicação de A. Não é difícil ver que

$$\mathfrak{M} = \{R_a + L_b + \Sigma R_{a_i} L_{b_i} \mid a,b,a_i,b_i \in A\},$$

pois $R_a R_b = R_{ab}$, $L_a L_b = L_{ba}$ e $R_a L_b = L_b R_a$. Mais ainda, se A é uma álgebra com unidade então

$$\mathfrak{M} = A_R A_L = \{\Sigma R_{a_i} L_{b_i} \mid a_i, b_i \in A\},$$

pois neste caso podemos escrever $R_a = R_a L_1$ e $L_b = R_1 L_b$.

Mostraremos que se A é uma álgebra simples central sobre K, então $\mathfrak{M} = \mathfrak{L}(A)$. Para isso, precisamos do seguinte

Sublema - Se A é uma álgebra simples e x, y são dois elementos de A com $x \neq 0$, então existe $T \in \mathfrak{M}$ tal que $xT = y$.

Demonstração: Como $x \neq 0$, AxA é um ideal não nulo de A. Logo, a simplicidade de A força $AxA = A$. Em particular, podemos escrever $\Sigma b_i x a_i = y$ $(a_1, b_i \in A)$ e o resultado segue com $T = \Sigma R_{a_i} L_{b_i}$.

Vamos agora ao

Teorema 27.1 - Se A é uma álgebra simples central sobre K, $x_1,\ldots,x_n \in A$ são linearmente independentes sobre K, e $y_1,\ldots,y_n$ são elementos arbitrários de A, então existe $T \in \mathfrak{M}$ tal que $x_iT = y_i$, $i = 1,\ldots,n$.

Demonstração. O teorema estará demonstrado se encontrarmos $T_1,\ldots,T_n \in \mathfrak{M}$ tais que $x_iT_i = 1$ e $x_jT_i = 0$ para $i \neq j$, pois neste caso $T = T_1R_{y_1} + \ldots + T_nR_{y_n}$ é a transformação desejada Se $n = 1$ a existência de T_1 é garantida pelo sublema. Prosseguindo por indução, vamos supor que $T_1,\ldots,T_{n-1}$ estão determinadas. Mostraremos como obter T_n. Para isso, dividiremos o problema em duas partes.

Suponhamos primeiro que para algum i, $1 \leq i \leq n-1$, $x_nT_i \notin K$. Neste caso, como por hipótese K é o centro de A, existe $a \in A$ tal que $(x_nT_i)a - a(x_nT_i) \neq 0$. Seja $S = T_iR_a - T_iL_a$. Então $S \in \mathfrak{M}$, $x_iS = 0$ para $i = 1,\ldots,n-1$ e $x_nS \neq 0$. Pelo sublema. existe $\tilde{S} \in \mathfrak{M}$ tal que $x_nS\tilde{S} = 1$ e o problema está resolvido com $T_n = S\tilde{S}$.

Suponhamos agora que $x_nT_i = \alpha_i \in K$, $i = 1,\ldots,n-1$. Seja $S = T_1R_{x_1} + T_2R_{x_2} + \ldots + T_{n-1}R_{x_{n-1}} - I$ onde $I = R_1 = L_1$ é a transformação identidade. Então $S \in \mathfrak{M}$ e $x_iS = 0$ para $i = 1,\ldots,n-1$. Mas $x_nS \neq 0$ pois caso contrário $\alpha_1x_1 + \alpha_2x_2 + \ldots + \alpha_{n-1}x_{n-1} - x_n = 0$, contradizendo a independência linear dos x_i sobre K. Pelo sublema, existe $\tilde{S} \in \mathfrak{M}$ tal que $x_nS\tilde{S} = 1$ e podemos tomar $T_n = S\tilde{S}$. Isto conclui a demonstração do teorema.

Corolário - Se A é uma álgebra simples central sobre K, então $\mathfrak{M} = \mathfrak{L}(A)$.

A partir deste resultado, obtemos o importante

Teorema 27.2 - Se A é uma álgebra simples central sobre K, então $A \otimes_K A^{op} \simeq K_n$ onde $n = \dim_K A$.

Demonstração: Sabemos que $A \simeq A_R$ e $A^{op} \simeq A_L$. Logo, $A \otimes A^{op} \simeq A_R \otimes A_L$. Sabemos também que $\mathfrak{L}(A) \simeq K_n$ onde $n = \dim_K A$. Agora, como todo elemento de A_R comuta com todo elemento de A_L, a aplicação $\varphi: A_R \otimes A_L \to \mathfrak{L}(A)$, $\varphi(\Sigma R_{a_i} \otimes L_{b_i}) = \Sigma R_{a_i} L_{b_i}$, é um homomorfismo. Pelo corolário acima, $\mathfrak{M} = A_R A_L = \mathfrak{L}(A)$ e portanto φ é sobrejetivo. Como $\dim_K \mathfrak{L}(A) = (\dim_K A)^2 = \dim_K A_R \otimes A_L$, segue-se que o núcleo de φ é zero e consequentemente φ é um isomorfismo. Assim,

$$A \otimes A^{op} \simeq A_R \otimes A_L \simeq A_R A_L = \mathfrak{L}(A) \simeq K_n$$

e o teorema está demonstrado.

Por exemplo, se Q é a álgebra dos quaternios reais, $Q \otimes_{\mathbb{R}} Q \simeq \mathbb{R}_4$.

28. Álgebras simples sob $\otimes$.

Neste parágrafo consideraremos o produto tensorial de álgebras simples.

Começamos com o seguinte

Teorema 28.1 - Seja A uma álgebra simples sobre um corpo K e seja B uma álgebra arbitrária sobre K com unidade. Então existe uma correspondência biunívoca entre os ideais

de B e os ideais de $A \otimes_K B$, a saber, $U \to A \otimes_K U$.

Demonstração: É imediato que se U é um ideal de B, $A \otimes U$ é um ideal de $A \otimes B$. Mostraremos inicialmente que todo ideal de $A \otimes B$ pode ser obtido desta forma. Seja pois W um ideal de $A \otimes B$ e seja $U = \{u \in B \mid a \otimes u \in W \text{ para todo } a \in A\}$. Claramente U é um subespaço vetorial de B. Além disso, como W é um ideal, dados $a \in A$, $b \in B$ e $u \in U$ temos que $a \otimes ub = (a \otimes u)(1 \otimes b)$ e $a \otimes bu = (1 \otimes b)(a \otimes u)$ estão em W. Logo, U é um ideal de B. Agora, por definição, $A \otimes U \subseteq W$. Gostaríamos de mostrar que $W \subseteq A \otimes U$. Seja então $w \in W$ e vamos escrever $w = \sum_{i=1}^{m} x_i \otimes y_i$ onde $x_i \in A$, $y_i \in B$ e onde os x_i são linearmente independentes sobre K. Seja a um elemento arbitrário de A e seja $T: A \to A$ uma transformação linear tal que $x_1T = a$ e $x_iT = 0$ para $i = 2,\ldots,m$. Pelas considerações do §27 esta transformação é um elemento da álgebra de multiplicações de A, digamos $T = \Sigma R_{a_j} L_{a'_j}$ $(a_j, a'_j \in A)$. Deste modo,

$$\begin{aligned}
\sum_j (a'_j \otimes 1)w(a_j \otimes 1) &= \sum_j \left(\sum_i a'_j x_i a_j \otimes y_i\right) \\
&= \sum_i \left(\sum_j a'_j x_i a_j\right) \otimes y_i \\
&= \sum_i x_i T \otimes y_i \\
&= a \otimes y_1.
\end{aligned}$$

Daí resulta que $a \otimes y_1 \in W$, pois W é um ideal de $A \otimes B$. Como a é arbitrário segue-se que $y_1 \in U$. Analogamente, $y_2,\ldots,y_m \in U$. Portanto, $w \in A \otimes U$ e $W = A \otimes U$.

Suponhamos agora que $U \neq V$ são ideais de B, digamos $U \not\subset V$. Seja $u \in U$ tal que $u \notin V$. Então $1 \otimes u \in A \otimes U$. Mas $1 \otimes u \notin A \otimes V$. Caso contrário podemos escrever $1 \otimes u = \Sigma\, a_i \otimes v_i$ onde $a_i \in A$, $v_i \in V$ e onde os v_i são linearmente independentes sobre K. Como $u \notin V$, u é linearmente independentes dos v_i e das propriedades do produto tensorial segue-se que $1 = 0$, uma contradição. Assim, concluimos que $A \otimes U \not\subset A \otimes V$ e a aplicação $U \to A \otimes U$ é biunívoca. Isto completa a demonstração.

Corolário - Se A é uma álgebra simples central sobre K e B é uma álgebra simples sobre K, então $A \otimes_K B$ é simples.

Antes de prosseguir observamos que a hipótese de que o centro de A coincide com K é necessária. Em geral o produto de álgebras simples não é simples. Por exemplo, seja $F \supseteq K$ uma extensão finita de corpos e consideremos o homomorfismo $\varphi: F \otimes_K F \to F$, $\varphi(\Sigma\, \alpha_i \otimes \beta_i) = \Sigma\, \alpha_i\beta_i$. Se $\alpha \in F$ e $\alpha \notin K$, o elemento $\alpha \otimes 1 - 1 \otimes \alpha \neq 0$ está no núcleo de φ. Como φ não é identicamente nulo, segue-se que o núcleo de φ é um ideal próprio não nulo de $F \otimes_K F$. Portanto $F \otimes_K F$ não é simples.

Dando seguimento, introduzimos o conceito de centralizador.

Seja A uma álgebra e seja S um subconjunto de A. O centralizador de S em A, indicado por $C_A(S)$, é o subconjunto de A formado por todos os elementos $a \in A$ que satisfazem a seguinte condição:

$$as = sa \quad \text{para todo} \quad s \in S.$$

Claramente $C_A(S)$ é uma subálgebra de A. Note que C_A (centro de A) = A e $C_A(A)$ = centro de A. Note também que se $\varphi: A \to A'$ é um isomorfismo de álgebras, então $\varphi(C_A(S)) = C_{A'}(\varphi(S))$.

Lema 28.2 - Sejam A e B álgebras sobre K com unidades e sejam S e T subálgebras de A e B respectivamente, contendo as unidades. Então $C_{A\otimes_K B}(S\otimes_K T) = C_A(S) \otimes_K C_B(T)$.

Demonstração: Seja $u \in C_{A\otimes B}(S\otimes T)$. Podemos escrever $u = \Sigma a_i \otimes b_i$ onde tanto os $a_i \in A$ como os $b_i \in B$ são linearmente independentes sobre K. Agora, para todo $s \in S$ temos que

$$0 = u(s \otimes 1) - (s \otimes 1)u = \Sigma (a_i s - s a_i) \otimes b_i .$$

Como os b_i são linearmente independentes sobre K, segue-se que os a_i comutam com todo $s \in S$, isto é, os a_i estão em $C_A(S)$. Analogamente, os b_i estão em $C_B(T)$. Em outras palavras, $C_{A\otimes B}(S\otimes T) \subseteq C_A(S) \otimes C_B(T)$. Como a inclusão reversa é imediata, concluimos que vale a igualdade.

Se identificamos, como é usual, K com $K(1\otimes 1) = K \otimes_K K$, o corolário do Teorema 28.1 e o lema acima nos dão o importante

Teorema 28.3 - Se A e B são álgebras simples centrais sobre K, então $A \otimes_K B$ é simples central sobre K.

Para concluir, enunciamos a seguinte recíproca:

Teorema 28.4 - Sejam A e B álgebras sobre K com unidades. Se $A \otimes_K B$ é simples, então A e B são simples. Se $A \otimes_K B$ é simples central sobre K, então A e B são simples centrais sobre K.

A demonstração cabe ao leitor.

29. A dimensão de uma álgebra simples sobre o seu centro.

Seja K um corpo. A dimensão de K_n sobre o seu centro, K, é um quadrado perfeito. Veremos que este é o caso para toda álgebra simples.

Lema 29.1 - Seja $F \supseteq K$ uma extensão de corpos, não necessariamente finita. Se A é uma álgebra simples central sobre K, então $A \otimes_K F$ é uma álgebra simples central sobre F.

Demonstração: Observamos primeiro que $A \otimes_K F$ é uma F-álgebra onde $\alpha(a \otimes \beta) = a \otimes \alpha\beta$, $\dim_F A \otimes_K F = \dim_K A$, e $(a \otimes \beta)(a' \otimes \beta') = aa' \otimes \beta\beta'$. Agora, mesmo que $F \supseteq K$ não seja uma extensão finita, o argumento do Teorema 28.1 se aplica para concluirmos que $A \otimes_K F$ é simples sobre F. Além disso, podemos também usar o (argumento do) Lema 28.2 para calcular o centro de $A \otimes_K F$:

$$C_{A \otimes_K F}(A \otimes_K F) = C_A(A) \otimes_K C_F(F) = K \otimes_K F \simeq F.$$

Com isto o lema está demonstrado.

Teorema 29.2 - Se A é uma álgebra simples central sobre K, então $\dim_K A$ é um quadrado perfeito.

Demonstração: Pelo teorema de Wedderburn $A \simeq D_n$ onde D é uma álgebra com divisão de centro K. Como $D_n \simeq D \otimes_K K_n$, temos que

$$\dim_K A = (\dim_K D)(\dim_K K_n) = (\dim_K D)n^2.$$

Portanto, o resultado segue se mostrarmos que $\dim_K D$ é um quadrado perfeito. Seja $\bar{K}$ o fecho algébrico de K. Pelo lema anterior $\bar{D} = D \otimes_K \bar{K}$ é uma álgebra simples central sobre $\bar{K}$. Como $\bar{K}$ é algebricamente fechado, segue-se que $\bar{D} \simeq \bar{K}_m$ (cf. §§9, 24). Logo, $\dim_K = D = \dim_{\bar{K}} \bar{D} = m^2$ e o teorema está demonstrado.

30. O grupo de Brauer.

Seja K um corpo e sejam A e B álgebras simples centrais sobre K. Pelo teorema de Wedderburn $A \simeq D_n$ e $B \simeq \Delta_m$ onde D e Δ são álgebras com divisão de centro K. Dizemos que A é similar a B, $A \sim B$, se D e Δ são isomorfas. Trata-se evidentemente de uma relação de equivalência. Podemos reformular esta relação da seguinte forma:

Lema 30.1 - $A \sim B$ se e somente se existem inteiros positivos r e s tais que $A \otimes_K K_r \simeq B \otimes_K K_s$.

Demonstração: Como antes, sejam $A \simeq D_n$ e $B \simeq \Delta_m$. Sabemos que $D_n \simeq D \otimes K_n$ e $\Delta_m \simeq \Delta \otimes K_m$. Se $A \sim B$ então $D \simeq \Delta$ e portanto

$$A \otimes K_m \simeq D \otimes K_n \otimes K_m \simeq \Delta \otimes K_m \otimes K_n \simeq B \otimes K_n.$$

Reciprocamente, suponhamos que $A \otimes K_r \simeq B \otimes K_s$. Então $D_{nr} \simeq \Delta_{ms}$ e pela unicidade no teorema de Wedderburn, $D \simeq \Delta$; isto é, $A \sim B$.

Corolário - Se $A \sim A'$ e $B \sim B'$ então $A \otimes_K B \sim A' \otimes_K B'$.

Demonstração: Pelo lema, existem inteiros positivos r_i, s_i $(i=1,2)$ tais que $A \otimes K_{r_1} \simeq A' \otimes K_{s_1}$ e $B \otimes K_{r_2} \simeq B' \otimes K_{s_2}$. Logo, $(A \otimes B) \otimes K_{r_1 r_2} \simeq (A' \otimes B') \otimes K_{s_1 s_2}$ e portanto $A \otimes B \sim A' \otimes B'$, como queríamos.

Seja $B(K)$ o conjunto das classes de equivalência das álgebras simples centrais sobre K segundo a relação $\sim$. Se A é uma tal álgebra vamos denotar a sua classe por $[A]$. Definimos uma operação em $B(K)$ da seguinte forma: $[A][B] = [A \otimes_K B]$. Pelo corolário acima esta definição não depende da escolha particular dos representantes. Agora, pelas propriedades do produto tensorial esta operação é associativa e comutativa. Além disso, é imediato que a classe de equivalência determinada pelo corpo K age como identidade, isto é $[A][K] = [A]$. Finalmente, pelo Teorema 27.2, $[A][A^{op}] = [K]$ onde A^{op} é a álgebra oposta de A.

Resumimos nossas observações no seguinte

Teorema 30.2 - $B(K)$ é um grupo abeliano em relação a $\otimes$.

$B(K)$ é chamado o grupo de Brauer do corpo K. Claramente, todo elemento de $B(K)$ é determinado por uma única (a menos de isomorfismo) álgebra com divisão de centro K. Com efeito, se A é simples central sobre K então $[A] = [D]$, onde D é a álgebra com divisão dada pelo teorema de Wedderburn.

Assim, pelo teorema de Frobenius, o grupo de Brauer do corpo dos números reais consiste apenas de dois elementos, um determinado pelos reais e outro pelos quaternios (cf. § 8). Para um corpo algebricamente fechado K, temos que $B(K) = \{[K]\}$ (§9).

Finalmente, se $F \supseteq K$ é uma extensão de corpos, a aplicação $[A] \to [A \otimes_K F]$ de $B(K)$ em $B(F)$ é um homomorfismo de grupos. Deixamos os detalhes para o leitor.

Voltaremos a este importante invariante de um corpo após desenvolver um pouco mais a teoria.

31. Uma caracterização das álgebras simples.

Seja B uma K-álgebra com unidade satisfazendo a seguinte propriedade: se A é uma K-álgebra contendo B como subálgebra e com a mesma unidade que B, então $A = C_A(B) \otimes_K B$. Vamos mostrar que esta é uma condição necessária e suficiente para que B seja simples central sobre K.

A suficiência é imediata. Com efeito, por meio da representação regular à direita de B podemos supor que B é uma subálgebra de K_n (e as unidades coincidem), onde $n = \dim_K B$; assim, $K_n = C_{K_n}(B) \otimes_K B$. Como K_n é simples central sobre K, segue do Teorema 28.4 que B é simples central sobre K.

Para provar a necessidade precisamos do seguinte

Lema 31.1 - Seja A uma K-álgebra com unidade e seja B uma subálgebra de A com a mesma unidade tal que $B \simeq K_n$ para algum inteiro $n \geq 1$. Então $A = C_A(B) \otimes_K B$.

Demonstração: Como $B \simeq K_n$, existe uma base b_{ij} $(i,j=1,\ldots,n)$ de B sobre K onde os b_{ij} se comportam como as

matrizes unitárias de K_n: $b_{11} + b_{22} + \ldots + b_{nn} = 1$ e $b_{ij}b_{k\ell} = \delta_{jk}b_{i\ell}$ (δ_{jk} = delta de Kronecker).

Sejam $a_{ij} = \sum_{k=1}^{n} b_{ki}a_{jk}b_{jk}$ $(i,j=1,\ldots,n)$.

Então $a_{ij}b_{st} = b_{si}ab_{jt} = b_{st}a_{ij}$; isto é, os a_{ij} centralizam uma base de B. Consequentemente, os a_{ij} estão em $C_A(B)$. Além disso,

$$\sum_{i,j=1}^{n} a_{ij}b_{ij} = \sum_{i,j,k=1}^{n} (b_{ki}ab_{jk})b_{ij} = \sum_{j,k=1}^{n} b_{kk}ab_{jj} = a.$$

Assim, concluimos que o homomorfismo $\varphi: C_A(B) \otimes_K B \to A$, $\varphi(\Sigma\, x_\ell \otimes y_\ell) = \Sigma\, x_\ell y_\ell$, é sobrejetivo. Agora, se $a = \sum_{i,j=1}^{n} a_{ij}b_{ij} = 0$ então

$$0 = \sum_{t=1}^{n} b_{tr}ab_{st} = \sum_{t=1}^{n} a_{rs}b_{tt} = a_{rs} \qquad (r,s = 1,\ldots,n).$$

Logo, o núcleo de φ é zero e portanto φ é um isomorfismo. Com isto o lema está demonstrado.

Podemos agora provar a necessidade.

Teorema 31.2 - Seja A uma K-álgebra com unidade e seja B uma subálgebra de A com a mesma unidade. Se B é simples central sobre K, então $A = C_A(B) \otimes_K B$.

Demonstração: Sejam $A' = A \otimes B^{op}$ e $B' = B \otimes B^{op}$. Então B' é uma subálgebra de A', a unidade de B' coincide com a unidade de A' e, pelo Teorema 27.2, $B' \simeq K_n$ onde $n = \dim_K B$. Logo, aplicando o lema anterior, temos que $A' = C_{A'}(B') \otimes B'$. Mas

$$C_{A'}(B') = C_A(B) \otimes C_{B^{op}}(B^{op}) = C_A(B) \otimes K = C_A(B)$$

e portanto

$$A \otimes B^{op} = A' = C_{A'}(B') \otimes B' = (C_A(B) \otimes B) \otimes B^{op}.$$

Daí, tomando-se o centralizador de B^{op} em ambos os lados, obtemos $A = C_A(B) \otimes B$ como queríamos demonstrar.

32. O teorema do duplo centralizador.

Seja A uma álgebra simples central sobre K. Vamos mostrar que as subálgebras simples de A que contém K ocorrem em pares B_1 e B_2 tais que $C_A(B_1) = B_2$ e $C_A(B_2) = B_1$.

Precisamos do seguinte

Lema 32.1 - Seja A uma álgebra simples central sobre K e seja F um subcorpo de A contendo K. Então $C_A(F)$ é uma álgebra simples central sobre F.

Demonstração: Sejam A_R e A_L as representações regulares à direita e à esquerda de A respectivamente. Sabemos que $A \otimes_K A^{op} \simeq A_R A_L = \mathfrak{L}(A)$, a álgebra das transformações lineares em A sobre K (cf. Teorema 27.2). Assim, $F \otimes_K 1 \simeq F_R \subseteq \mathfrak{L}(A)$ onde F_R é a subálgebra de A_R que consiste das multiplicações à direita por elementos de F, $R_\alpha : a \to a\alpha$ $(\alpha \in F)$. O que podemos dizer sobre o centralizador de F_R em $\mathfrak{L}(A)$? Ora, $T \in C_{\mathfrak{L}(A)}(F_R)$ se e somente se para todo $\alpha \in F$

$$(a\alpha)T = a(R_\alpha T) = a(TR_\alpha) = (aT)\alpha \qquad a \in A.$$

Em outras palavras, $C_{\mathfrak{L}(A)}(F_R)$ é precisamente a álgebra das transformações lineares em A sobre F (aqui a ação de F em A é à direita, mas isso não importa). Portanto, $C_{\mathfrak{L}(A)}(F_R) \simeq F_m$ onde $m = \dim_F A$ e temos que

$$F_m \simeq C_{\mathfrak{L}(A)}(F_R) \simeq C_{A \otimes_K A^{op}}(F \otimes_K 1) = C_A(F) \otimes_K A^{op}.$$

Logo, como $F \otimes_K A^{op}$ é uma subálgebra simples central sobre F da F-álgebra $C_A(F) \otimes_K A^{op}$, segue do Teorema 31.2 que

$$F_m \simeq (F \otimes_K A^{op}) \otimes_F C_{C_A(F) \otimes_K A^{op}}(F \otimes_K A^{op})$$

$$= (F \otimes_K A^{op}) \otimes_F (C_{C_A(F)}(F) \otimes_K C_{A^{op}}(A^{op}))$$

$$= (F \otimes_K A^{op}) \otimes_F (C_A(F) \otimes_K K)$$

$$= (F \otimes_K A^{op}) \otimes_F C_A(F).$$

Daí, pelo Teorema 28.4 concluimos que $C_A(F)$ é simples central sobre F, como queriamos demonstrar.

Estamos agora em condições de provar o "teorema do duplo centrlizador".

Teorema 32.2 - Seja A uma álgebra simples central sobre K e seja B uma subálgebra simples de A contendo K. Então $C_A(B)$ é uma subálgebra simples de A e $C_A(C_A(B)) = B$.

Demonstração: Seja F o centro de B. Então F é um corpo contendo K e, pelo lema anterior $C_A(F)$ é uma álgebra simples central sobre F. Como $C_A(F) \supseteq B$ segue do Teorema 31.2 que

(1) $$C_A(F) = C_{C_A(F)}(B) \otimes_F B = C_A(B) \otimes_F B.$$

Logo, pelo Teorema 28.4, C_A B) é simples central sobre F. Considerando $C_A(F) \supseteq C_A(B)$ podemos aplicar novamente o Teorema 31.2; ou seja,

(2) $$C_A(F) = C_{C_A(F)}(C_A(B)) \otimes_F C_A(B) = C_A(C_A(B)) \otimes_F C_A(B).$$

Portanto, de (1) e (2), obtemos

$$C_A(B) \otimes_F B = C_A(C_A(B)) \otimes_F C_A(B).$$

Como $B \subseteq C_A(C_A(B))$, contando as dimensões sobre F concluimos que $B = C_A(C_A(B))$. Isto completa a demonstração.

33. Extensões de isomorfismos.

Sabemos da álgebra linear que todo automorfismo da álgebra das matrizes nxn sobre um corpo K é interno; ou seja, é da forma $X \to MXM^{-1}$ para alguma matriz inversível M.

Lema 33.1 - Se A é uma algebra simples central sobre K então todo automorfismo de A é interno.

Demonstração· Seja φ um automorfismo de A. Sejam A_R e A_L as representações regulares à direita e à esquerda de A em K_n respectivamente ($n = \dim_K A$). Então φ induz um automorfismo $\bar{\varphi}$ de $A_R A_L = K_n$, $\bar{\varphi}(\Sigma R_{a_i} L_{b_i}) = \Sigma R_{\varphi(a_i)} L_{b_i}$. Pelo que observam s acima, existe uma matriz inversível $M \in K_n$

tal que $\bar{\varphi}(X) = MXM^{-1}$ para todo $X \in K_n$. Em particular, $L_b = ML_bM^{-1}$ para todo $b \in A$. Logo, $M \in C_{K_n}(A_L) = A_R$, isto é, $M = R_a$ para algum $a \in A$. O leitor verificará facilmente que $M^{-1} = R_{a^{-1}}$. Portanto $\varphi(x) = axa^{-1}$ para todo $x \in A$, como queríamos demonstrar.

Teorema 33.2 - Seja A uma álgebra simples central sobre K e sejam B e B' subálgebras simples de A cujas unidades coincidem com a unidade de A. Então todo isomorfismo entre B e B' pode ser extendido a um automorfismo interno de A.

Demonstração: Seja $\varphi: B \to B'$ um isomorfismo. Mostraremos que φ pode ser extendido a um automorfismo de A. Pelo lema anterior, este automorfismo será interno. Dividiremos a demonstração em três partes.

1) Suponhamos que B, e consequentemente B', são simples centrais sobre K. Neste caso, o Teorema 31.2 nos diz que

$$A = C_A(B) \otimes B = C_A(B') \otimes B'.$$

Como A é simples central sobre K, pelo Teorema 28.3, $C_A(B)$ e $C_A(B')$ são simples centrais sobre K. Logo, $C_A(B) \simeq D_r$ e $C_A(B') \simeq \Delta_s$ onde D e Δ são álgebras com divisão de centro K. Além disso, como por hipótese $B \simeq B'$, temos que $B^{op} \simeq B'^{op}$; portanto

$$B \otimes B^{op} \simeq K_m \simeq B' \otimes B^{op}$$

onde $m = \dim_K B = \dim_K B'$. De tudo isso, segue-se que

$$D_{rm} \simeq (C_A(B)\otimes B)\otimes B^{op} = (C_A(B') \otimes B') \otimes B^{op} \simeq \Delta_{sm}.$$

Pela unicidade no teorema de Wedderburn, concluimos que $r = s$ e $D \simeq \Delta$. Assim, existe um isomorfismo $\psi: C_A(B) \to C_A(B')$, e

$$\psi \otimes \varphi: A = C_A(B) \otimes B \to A = C_A(B') \otimes B'$$

e um automorfismo de A que extende φ.

2) Suponhamos agora que $B = K(z)$, o corpo obtido a partir de K pela adjunção de um elemento $z \in A$. Deste modo, $B' = K(z')$ onde $z' = \varphi(z)$. Seja $n = \dim_K A$ e sejam A_R e A_L as representações regulares de A em K_n. Vamos trabalhar com as cópias de B e B' em A_R, que indicaremos pelos mesmos símbolos respectivamente. Mostraremos que φ pode ser extendido a um automorfismo de A_R.

Como $\varphi(R_z) = R_{z'}$ e R_z são raizes dos mesmos polinômios sobre K, existe $U \in K_n = A_R A_L$ tal que $U R_z U^{-1} = R_{z'}$. Consideremos o automorfismo interno ψ de K_n, $\psi: X \to UXU^{-1}$. Então ψ é uma extensão de φ e portanto $\psi(A_L) \subseteq C_{K_n}(B')$, pois A_L centraliza B. Assim,

(i) $C_{K_n}(B')$ é simples central sobre B' (cf. Lema 32.1).

(ii) $B'\psi(A_L)$ e $B'A_L$ são subálgebras simples centrais sobre B' de $C_{K_n}(B')$.

(iii) $B'\psi(A_L)$ e $B'A_L$ são equivalentes sobre B':

$$R_{b'}\psi(L_a) \to R_{b'}L_a.$$

Logo, pelo caso que tratamos acima, existe $T \in C_{K_n}(B')$ tal que

$$(TU)L_a(TU)^{-1} = T\psi(L_a)T^{-1} = L_a \qquad (a \in A).$$

Seja $S = TU$. Então $S \in C_{K_n}(A_L) = A_R$ e $R_a \to SR_aS^{-1}$ é um automorfismo de A_R que estende φ.

3) Terminaremos a demonstraçao por indução na dimensão de B sobre K. Se $\dim_K B = 1$, então $B = B' = K$ e o resultado é óbvio. Suponhamos que $\dim_K B = m > 1$ e que o resultado é verdadeiro para subálgebras simples de menor dimensão. Já provamos o teorema quando B é central sobre K; assim, podemos supor que K está contido pr·priamente no centro de B.

Se B é um corpo e a extensão $B \supset K$ não contém corpos intermediários, então $B = K(z)$ qualquer que seja $z \in B$, $z \notin K$. Já vimos que nesta circunstância o teorema é verdadeiro.

Se B é um corpo e a extensão $B \supset K$ contém corpos intermediários ou se B não é um corpo, então existe um subcorpo F do centro de B com $B \supsetneq F \supsetneq K$. Seja F' a imagem de F pelo isomorfismo $\varphi\colon B \to B'$. Então $F \simeq F'$ e pela hipótese de indução existe um automorfismo $\bar{\varphi}$ de A tal que $\bar{\varphi}(\alpha) = \varphi(\alpha)$ para todo $\alpha \in F$. Agora, a aplicação $\bar{\varphi}(b) \to \varphi(b)$ $(b \in B)$ é um isomorfismo de $\bar{\varphi}(B)$ em B', considerados como álgebras sobre F'. Pelo Lema 32.1, $C_A(F')$ é uma álgebra simples central sobre F'. Por indução, existe um automorfismo ψ de $C_A(F')$ tal que $\psi\bar{\varphi}(b) = \varphi(b)$ para todo $b \in B$. Pelo Lema 33.1, ψ é interno e portanto podemos considerá-lo como um automorfismo de A. Deste modo $\psi\bar{\varphi}$ é a extensão desejada. Com isto o teorema esta demonstrado.

34. Corpos de decomposição.

Seja A uma álgebra simples central sobre K e seja F um corpo contendo K. Então $A \otimes_K F$ é uma álgebra simples central sobre F. Dizemos que F é um corpo de decomposição para A se $A \otimes_K F$ é a álgebra das transformações lineares em um espaço vetorial sobre F.

Note que, como $\dim_F A \otimes_K F = \dim_K A$, F é um corpo de decomposição para A se e somente $A \otimes_K F \simeq F_n$ onde $n^2 = \dim_K A$. Por sua vez, esta última condição é equivalente a dizer que a classe de equivalência $[A]$ no grupo de Brauer $B(K)$ é um elemento do núcleo do homomorfismo de grupos $[A] \to [A \otimes_K F]$ de $B(K)$ em $B(F)$. Assim, se $A \simeq D_n$ onde D é a álgebra com divisão dada pelo teorema de Wedderburn, concluimos que F é um corpo de decomposição para A se e somente se F é um corpo de decomposição para D, pois $[A] = [D]$ em $B(K)$.

Vamos provar a existência de corpos de decomposição que são extensões normais e separáveis sobre K (com isto em mãos poderemos exibir representantes especiais para as classes de equivalência no grupo de Brauer $B(K)$). Pelo que observamos acima, basta considerar o problema da existência destes corpos de decomposição para álgebras com divisão.

35. Subcorpos maximais.

Seja D uma álgebra com divisão de centro K. Dizemos que um subcorpo F de D é um subcorpo maximal se não está contido em nenhum subcorpo maior de D. Nesta circunstância necessariamente F contém K, pois caso contrário F estaria contido propriamente em $K(F)$, o corpo obtido pela adjunção dos elementos de F a K. Mostraremos que todo subcorpo maximal de D é um corpo de decomposição para D.

Lema 35.1 - Seja D uma álgebra com divisão e seja F um subcorpo de D. Então F é um subcorpo maximal de D se e somente se $C_D(F) = F$.

Demonstração: Suponhamos que F é um subcorpo maximal de D. Se $u \in C_D(F)$ então $F \subseteq F(u)$, o corpo obtido pela adjunção de u a F. Daí resulta que $F = F(u)$ e $u \in F$. Logo, $C_D(F) \subseteq F$. Como a inclusão reversa é imediata, concluimos que vale a igualdade.

Reciprocamente suponhamos que $C_D(F) = F$. Se L é um subcorpo de D contendo F, então $L \subseteq C_D(F) = F$ e portanto F é um subcorpo maximal.

Temos as ferramentas necessárias para provar o

Teorema 35.2 - Seja D uma álgebra com divisão de centro K e seja F um subcorpo maximal de D. Então $D \otimes_K F \simeq F_n$ onde $n = \dim_F D$.

Demonstração: Seja D^{op} a álgebra oposta de D. Claramente, F

é também um subcorpo maximal de D^{op}. Pelo lema anterior, $C_{D^{op}}(F) = F$. Agora, sabemos que $D \otimes_K D^{op} \simeq \mathfrak{L}(D)$, a álgebra das transformações lineares em D sobre K. Por este isomorfismo, $1 \otimes_K F$ é levado em $F_L = \{L_\alpha \mid \alpha \in F, \ L_\alpha : x \to \alpha x, \ x \in D\}$. Assim,

$$D \otimes_K F = D \otimes_K C_{D^{op}}(F) = C_{D \otimes_K D^{op}}(1 \otimes_K F) \simeq C_{\mathfrak{L}(D)}(F_L).$$

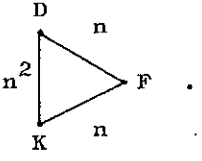
Mas $C_{\mathfrak{L}(D)}(F_L)$ é precisamente a álgebra das transformações lineares em D sobre F (verifique!). Deste modo, $D \otimes_K F \simeq F_n$ onde $n = \dim_F D$, e o teorema está demonstrado.

Como

$$\dim_F D \otimes_K F = \dim_K D = \dim_F D \cdot \dim_K F$$

uma consequência interessante é o seguinte

Corolário - Se D é uma álgebra com divisão de centro K então para todo subcorpo maximal F de D, $\dim_F D = \dim_K F = \sqrt{\dim_K D}$:



36. Subcorpos maximais separáveis.

Para provar a existência de subcorpos maximais separáveis precisamos do seguinte

Lema 36.1 - Seja D uma álgebra com divisão não comutativa de

centro K. Então existe um elemento $a \in D$, $a \notin K$ tal que a é separável sobre K.

Demonstração: Se K é um corpo finito ou a característica de K é zero, então K não possui extensões inseparáveis e todo elemento em D é separável sobre K. Assim, podemos supor que K é um corpo infinito de característica $p \neq 0$.

Suponhamos por absurdo que o resultado é falso. Então todo elemento em D é puramente inseparável sobre K: dado $a \in D$, $a^{p^r} \in K$ para algum $r = r(a) \geq 0$ (cf. [ ] pp. 138-143). Como o grau do polinômio minimal de qualquer elemento em D é majorado pela dimensão de D sobre K, existe um inteiro positivo s tal que $a^{p^s} \in K$ para todo $a \in D$. Seja $a_1,\ldots,a_n$ uma base de D sobre K, com $a_1 = 1$. Seja F um corpo contendo K. Um "elemento genérico" de $D \otimes_K F$ é da forma

$$u = x_1(a_1 \otimes 1) + \ldots + x_n(a_n \otimes 1),$$

onde $x_1,\ldots,x_n$ são variáveis tomando valores em F. Calculando u^{p^s} e grupando de maneira apropriada, podemos escrever

$$u^{p^s} = f_1(x_1,\ldots,x_n)(a_1\otimes 1) + \ldots + f_n(x_1,\ldots,x_n)(a_n\otimes 1)$$

onde $f_1,\ldots,f_n$ são polinômios com coeficientes em K. Se especificamos valores em K para $x_1,\ldots,x_n$, digamos $x_j \to \alpha_j \in K$, obtemos

$$u^{p^s} = \Big(\sum_{i=1}^{n} f_i(\alpha_1,\ldots,\alpha_n)a_i\Big)^{p^s} \otimes 1 = \alpha \otimes 1$$

onde $\alpha \in K$. Como $a_1 = 1$, a independência linear dos a_i força $f_i(\alpha_1,\ldots,\alpha_n) = 0$, $i = 2,\ldots,n$. Como K é um corpo infinito, se-

gue-se que os polinômios $f_2,\ldots,f_n$ são identicamente nulos. Portanto,

$$u^{p^s} = f_1(x_1,\ldots,x_n)(1 \otimes 1).$$

Especificando agora valores em F para $x_1,\ldots,x_n$, concluímos que $u^{p^s} \in F$ para todo $u \in D \otimes_K F$. Ora, se tomamos para F um subcorpo maximal de D, então $D \otimes_K F \simeq F_m$ onde $m = \dim_F D > 1$. Entretanto, em F_m nenhuma potência da matriz unitária e_{11} é central. Com esta contradição o lema está demonstrado.

Teorema 36.2 - Seja D uma álgebra com divisão de centro K. Então D possui um subcorpo maximal separável sobre K.

Demonstração: Se D é uma álgebra comutativa o resultado é óbvio. Assim, podemos supor que D não é comutativa. Pelo lema acima, a extensão $D \supset K$ admite corpos intermediários separáveis sobre K. Seja F um subcorpo de D contendo K, separável sobre K e maximal com respeito a esta propriedade. Vamos mostrar que F é um subcorpo maximal de D. Pelo Lema 35.1, basta verificar que $C_D(F) = F$. Ora, pelo Lema 32.1, $C_D(F)$ é uma álgebra com divisão de centro F. Se $C_D(F) \neq F$ o lema que acabamos de provar nos diz que existe um elemento $a \in C_D(F)$, $a \notin F$ separável sobre F. Deste modo, $F(a)$ é separável sobre K e $F(a) \neq F$, contradizendo a escolha de F. Logo, $C_D(F) = F$ e a demonstração está completa.

37. Corpos de decomposição galoisianos.

Seja $L \supseteq K$ uma extensão de corpos e seja G o grupo dos automorfismos de L sobre K. Diremos que L é uma extensão galoisiana de K se e somente se L é uma extensão finita de K e o corpo fixo de G é K. Assim, L é uma extensão galoisiana de K se e somente se L é uma extensão normal e separável de K.

Vamos provar agora o resultado mencionado no §34.

Teorema 37.1 - Se D é uma álgebra com divisão de centro K, então D admite um corpo de decomposição que é uma extensão galoisiana de K.

Demonstração: Seja F um subcorpo maximal separável de D (§36). Então F é um corpo de decomposição para D (§35): $D \otimes_K F \simeq F_n$. Como F é uma extensão separável e finita de K, existe uma extensão galoisiana L de K que contém F. O leitor deverá verificar que

$$D \otimes_K L \simeq (D \otimes_K F) \otimes_F L \simeq F_n \otimes_F L \simeq L_n.$$

Portanto, L é um corpo de decomposição para D e o teorema está demonstrado.

Corolário - Se A é uma álgebra simples central sobre K, então A admite um corpo de decomposição que é uma extensão galoisiana de K.

38. Subcorpos maximais galoisianos.

Neste ponto podemos perguntar se toda álgebra com divisão central sobre K contém um subcorpo maximal que é uma extensão galoisiana de K. Veremos mais adiante que a resposta é não. Entretanto, módulo a relação de similaridade temos uma resposta diferente.

Precisamos do seguinte

Lema 38.1 - Seja A uma álgebra simples central sobre K e seja F um subcorpo de A contendo K. As seguinte condições são equivalentes:

(i) F é um subcorpo maximal de A.

(ii) $C_A(F) = F$.

(iii) $\dim_K A = (\dim_K F)^2$.

Demonstração: A equivalência de (i) e (ii) segue como no Lema 35.1. Vamos mostrar a equivalência de (ii) e (iii). Seja $A' = A \otimes K_n$ onde $n = \dim_K F$. Então A' é simples central sobre K e $F \otimes 1$, $1 \otimes F$ são subálgebras simples de A' cujas unidades coincidem com a unidade de A' (aqui estamos considerando $F \subseteq K_n$ por meio da representação regular). Pelo Teorema 33.2, o isomorfismo natural de $F \otimes 1$ em $1 \otimes F$ pode ser extendido a um automorfismo de A'. Logo,

$$C_A(F) \otimes K_n = C_{A'}(F \otimes 1) \simeq C_{A'}(1 \otimes F) = A \otimes C_{K_n}(F).$$

Contando as dimensões sobre K e usando o fato de que $C_{K_n}(F) \simeq F^{op}$, obtemos

$$\dim_K A = (\dim_K C_A(F))(\dim_K F).$$

Como $F \subseteq C_A(F)$, é agora imediata a equivalência de (ii) e (iii).

Teorema 38.2 - Se A é uma álgebra simples central sobre K então, no grupo de Brauer $B(K)$, $[A] = [B]$ onde B contém um subcorpo maximal que é uma extensão galoisiana de K.

Demonstração: Pelo teorema de Wedderburn, $A \simeq D \otimes K_r$ onde D é uma álgebra com divisão de centro K. Seja F um subcorpo maximal separável de D. Sabemos que $\dim_K F = n$ onde $\dim_K D = n^2$. Seja L uma extensão galoisiana de K que contém F. Vimos que nestas condições L é um corpo de decomposição para D, e portanto também para A. Seja $B = D \otimes K_m$ onde $m = \dim_F L$. Então B é simples central sobre K e no grupo de Brauer $B(K)$, $[A] = [B]$. Além disso, como $F \otimes K_m = F_m$ está contido em B, e L está contido em F_m por meio da representação regular, podemos considerar $L \subseteq B$. Agora,

$$\begin{aligned}\dim_K B &= (\dim_K D)(\dim_K K_m) \\ &= n^2 m^2 \\ &= (\dim_K F)^2 \ (\dim_F L)^2 \\ &= (\dim_K L)^2\end{aligned}$$

e portanto, pelo lema anterior, L é um subcorpo maximal de B. Isto completa a demonstração.

Assim, concluímos que a menos de similaridade (i.e., igualdade no grupo de Brauer) podemos restringir o estudo das álgebras

simples centrais sobre K àquelas que contém um subcorpo maximal galoisiano sobre K.

39. Produtos cruzados.

Seja A uma álgebra simples central sobre K, contendo como subcorpo maximal uma extensão galoisiana L de K. Seja G o grupo de Galois de L sobre K. Vamos fixar $\dim_K L = n$, de modo que $\dim_K A = n^2$ e a ordem de G é n. Se $\sigma \in G$ e $\alpha \in L$, indicaremos $\sigma(\alpha)$ por α^σ. Pelo Teorema 33.2, existe um elemento inversível $x_\sigma \in A$ tal que $x_\sigma^{-1} \alpha x_\sigma = \alpha^\sigma$ para todo $\alpha \in L$.

Afirmamos que os elementos x_σ $(\sigma \in G)$ formam uma base de A sobre L. Para provar isto basta mostrar que os x_σ são linearmente independentes sobre L, pois $n = \dim_L A$ é a ordem de G. Suponhamos por absurdo que este não é o caso. Então existe uma relação

$$x_{\sigma_1} \alpha_{\sigma_1} + \ldots + x_{\sigma_r} \alpha_{\sigma_r} = 0 \qquad \alpha_{\sigma_i} \in L$$

onde nenhum coeficiente é nulo e de menor comprimento (r) com esta propriedade. Claramente $r \geq 2$. Como o corpo fixo de G é K, existe $\beta \in L$ tal que $\beta^{\sigma_1} \neq \beta^{\sigma_2}$. Logo, a relação

$$0 = \beta\left(\sum_{i=1}^{r} x_{\sigma_i} \alpha_{\sigma_i}\right) - \left(\sum_{i=1}^{r} x_{\sigma_i} \alpha_{\sigma_i}\right)\beta^{\sigma_1}$$

$$= \sum_{i=2}^{r} x_{\sigma_i}(\beta^{\sigma_i} - \beta^{\sigma_1})\alpha_{\sigma_i}$$

contradiz a minimalidade de r pois $(\beta^{\sigma_2} - \beta^{\sigma_1})\alpha_{\sigma_2} \neq 0$.

Assim, concluimos que todo elemento de A pode ser escrito de maneira única na forma

$$\sum_{\sigma \in G} x_\sigma a_\sigma, \quad a_\sigma \in L.$$

Sejam σ, τ dois elementos arbitrários de G. Então, para todo $a \in L$,

$$x_\tau^{-1} x_\sigma^{-1} a x_\sigma x_\tau = x_\tau^{-1} a^\sigma x_\tau = a^{\sigma\tau} = x_{\sigma\tau}^{-1} a x_{\sigma\tau}$$

e portanto $(x_\sigma x_\tau)x_{\sigma\tau}^{-1} = h(\sigma,\tau) \in C_A(L) = L$. Deste modo, $x_\sigma x_\tau = h(\sigma,\tau)x_{\sigma\tau} = x_{\sigma\tau} f(\sigma,\tau)$ onde $f(\sigma,\tau) = h(\sigma,\tau)^{\sigma\tau} \neq 0$ está em L. Seja L^* o conjunto dos elementos não nuls de L. Segue das relações de associatividade $x_\sigma(x_\tau x_\nu) = (x_\sigma x_\tau)x_\nu$ que a função $f: G \times G \to L^*$ satisfaz

$$f(\sigma,\tau\nu)f(\tau,\nu) = f(\sigma\tau,\nu)f(\sigma,\tau)^\nu.$$

Um conjunto de constantes com esta propriedade é chamado um <u>conjunto de fatores</u> de L sobre K.

Sabemos agora como multiplicar dois elementos arbitrários de A. Basta usar a distributividade e as relações $a x_\sigma = x_\sigma a^\sigma$, $x_\sigma x_\tau = x_{\sigma\tau} f(\sigma,\tau)$ para $a \in L$ e $\sigma,\tau \in G$. Em outras palavras, a estrutura de A fica completamente determinada por L, K, e o conjunto de fatores $f(\sigma,\tau)$.

Reciprocamente, seja L uma extensão galoisiana de K com grupo de Galois G e seja $f: G \times G \to L^*$ um conjunto de fatores. Podemos definir uma álgebra $A = (L,G,f)$, chamada o <u>produto cruzado</u> de L e G com respeito a f, introduzindo formal-

mente um conjunto de elementos x_σ $(\sigma \in G)$ e considerando as combinações lineares

$$\sum_{\sigma \in G} x_\sigma a_\sigma, \qquad a_\sigma \in L.$$

Igualdade, adição e multiplicação por escalares são definidas de maneira usual. Multiplicação é definida distributivamente de acordo com

$$a\, x_\sigma = x_\sigma a^\sigma$$

$$x_\sigma x_\tau = x_{\sigma\tau}\, f(\sigma,\tau).$$

O produto cruzado (L,G,f) é uma álgebra com unidade, $x_1\, f(1,1)^{-1}$, de centro $K \simeq K\, x_1\, f(1,1)^{-1}$, e de dimensão n^2 sobre K onde $n = \dim_K L = \circ(G)$. Além disso, o leitor deverá verificar que (L,G,f) é uma álgebra simples.

Podemos enunciar o

Teorema 39.1 - Seja L uma extensão galoisiana de K com grupo de Galois G e seja f um conjunto de fatores. Então o produto cruzado (L,G,f) é uma álgebra simples central sobre K. Além disso, se A é uma álgebra simples central sobre K então existem L, G e f tais que, em $B(K)$, $[A] = [(L,G,f)]$.

40. Álgebras com divisão centrais que não são produtos cruzados.

Como o leitor já deve ter percebido, as álgebras cíclicas são um caso especial de produtos cruzados. Brauer, Hasse e

Noether [2, p.149] mostraram que toda álgebra simples sobre os racionais é uma álgebra cíclica sobre o centro. As suspeitas de que toda álgebra com divisão é uma álgebra cíclica sobre o centro terminaram quando Albert [1] construiu um produto cruzado não cíclico. Permaneceu a questão se toda álgebra com divisão central é um produto cruzado (este é o caso quando a dimensão sobre o centro é n^2 com $n = 2,3,4,6,12$). Recentemente, Amitsur [3] provou que para todo inteiro n que é divisível pelo quadrado de um primo ímpar ou por 8, existe uma álgebra com divisão de dimensão n^2 sobre o centro que não é um produto cruzado. Mais explicitamente, Amitsur considerou a álgebra com divisão genérica de dimensão n^2, $\mathbb{Q}(X_1,\ldots,X_m)$, gerada por $m \geq 2$ matrizes genéricas de ordem $n \times n$ (isto é, matrizes cujos coeficientes são indeterminadas comutativas sobre os racionais $\mathbb{Q}$).

APÊNDICE

O TEOREMA DE WEDDERBURN SOBRE ÁLGEBRAS COM DIVISÃO FINITAS

Teorema - Toda álgebra com divisão finita é comutativa.

Demonstração: Seja D uma álgebra com divisão finita de centro K e seja $n^2 = \dim_K D$. Sabemos que todo subcorpo maximal de D é n-dimensional sobre K (§35). Portanto, todo subcorpo maximal de D possui q^n elementos, onde q é o número de elementos em D. Pela teoria dos corpos finitos, segue-se que dois quaisquer subcorpos maximais de D são K-isomorfos. Seja F um subcorpo maximal de D. Pelo que acabamos de deduzir, se F' é um outro subcorpo maximal de D, então $F' = aFa^{-1}$ para algum $a \neq 0$ em D (cf. §33). Como todo elemento pode ser imerso num subcorpo maximal, temos que $D = \bigcup_{a \neq 0} aFa^{-1}$. Logo, $D^* = \bigcup_{a \neq 0} aF^*a^{-1}$ onde D^* é o grupo multiplicativo dos elementos não nulos de D e F^* é o subgrupo $D^* \cap F$. Mas um grupo finito não pode ser a união dos conjugados de um subgrupo próprio. Assim, concluimos que $D = F = K$ e o teorema está demonstrado.

BIBLIOGRAFIA

[1] A.A. Albert, A construction of non-cyclic normal division rings, Bull. Amer. Math. Soc., 38 (1938) 449-456.

[2] A.A. Albert, Structure of Algebras, Amer. Math. Soc. Colloquium Publications, Vol. 24, 1939.

[3] S.A. Amitsur, On central division algebras, Israel J. Math. 12 (1972) 408-420.

[4] E. Artin, The influence of J.H.M. Wedderburn on the development of modern algebra, Bull. Amer. Math. Soc., 56 (1950) 65-72.

[5] E. Artin, C.J. Nesbitt, R.M. Thrall, Rings with Minimum Condition, The University of Michigan Press.

[6] R. Bott, J. Milnor, On the parallelizability of the spheres, Bull. Amer. Math. Soc., 64 (1958) 87-89.

[7] A. Cayley, The Philosophical Maganize, (3), 26 (1845) 210-213 e 30 (1847) 257-258 = Coll. Math. Papers, 1, 127 e 301.

[8] C.W. Curtis, The Four and Eight Square Problem and Division Algebras, Studies in Modern Algebra, MAA Studies in Mathematics, Vol. 2, Prentice Hall, pp. 100-125.

[9] L.E. Dickson, Definitions of a linear associative algebra by independent postulates, Trans. Amer. Math. Soc., 4 (1903) 21-26.

[10] L.E. Dickson, On quaternions and their generalization and the history of the eight square theorem, Annals of Math., 20 (1919) 155-171.

[11] L.E. Dickson, Algebras and their Arithmetics, University of Chicago Press, 1923.

[12] F.G. Frobenius, Über lineare Substitutionen und bilineare Formen, J. Reine Angew. Math., 84 (1878) 1-63.

[13] C.F. Gauss, Werke II.

[14] W.H. Greub, Multilinear Algebra, Springer-Verlag, 1967.

[15] W.R. Hamilton, Conjugate functions and on algebra as the science of pure time, Trans. Royal Irish Academy, 17, (1837), 293-422 = Math. Papers, 3, 3-96.

[16] W.R. Hamilton, Lectures on Quaternions, Dublin, 1853.

[17] H. Hankel, Theorie der complexen Zahlensysteme, Leipzig, 1867.

[18] G.H. Hardy and E.M. Wright, An Introduction to the Theory of Numbers, Oxford, 1954.

[19] I.N. Herstein, Noncommutative Rings, The Carus Mathematical Monographs, Nº 15, Amer. Math. Ass.

[20] H. Hopf, Ein topologischer Beitrag zur reelen Algebra, Comment. Math. Helv., 13 (1941) 219-239.

[21] N. Jacobson, Structure of Rings, Amer. Math. Soc. Colloq. Publ. Vol. 37, 1968.

[22] I. Kaplansky, Introdução à Teoria de Galois, Notas de Matemática, nº 13, IMPA, 1958.

[23] M. Kervaire, Non-parallelizability of the n-sphere for n=7, Proc. Nat. Acad. Sci. USA, 44 (1958) 280-283.

[24] M. Kline, Mathematical Thought from Ancient to Modern Times, Oxford University Press, 1972.

[25] C.C. MacDuffe, An Introduction to Abstract Algebra, Dover Publ., 1940.

[26] C.P. Milies, Anéis e Módulos, IME-USP, 1972.

[27] B. Peirce, Linear associative algebras, Amer. J. Math., 4 (1870).

[28] J.H.M. Wedderburn, A theorem on finite algebras, Trans. Amer. Math. Soc., 6 (1905).

[29] J.H.M. Wedderburn, On hypercomplex numbers, Proc. Lond. Math. Soc. (2), 6 (1908) 77-117.