Hygino H. Domingues

Sobre Alguns Fundamentos Algébricos da Combinatória

unesp

1910000350

À Biblioteca do
IBILCE.
20/6/87
O autor :

HYGINO H. DOMINGUES

SOBRE ALGUNS FUNDAMENTOS ALGÉBRICOS DA COMBINATÓRIA

Tese apresentada ao Instituto de Biociências, Letras e Ciências Exatas de São José do Rio Preto - UNESP - como parte dos requisitos para obtenção do título de Livre-Docente.

São José do Rio Preto
- 1986 -

Inst. de Biociências, Letras e Ciências Exatas - UNESP
BIBLIOTECA
T= 350/87
68

ÍNDICE

página

INTRODUÇÃO I

CAPÍTULO I: Álgebras Umbrais 01

1. Deslocamentos em Espaços Vetoriais 01

2. Operadores 06

3. Álgebras Umbrais 10

4. Funcionais Delta 13

5. O Cálculo Umbral 22

(5.1) Introdução 22

(5.2) Base Associada a um Operador Delta 24

(5.3) Relação entre Funcionais D-delta Recíprocos 26

(5.4) A Derivada de Pincherle e a Fórmula de Rodrigues.. 28

(5.5) Algumas Bases Associadas 29

(5.6) Algumas Sequencias Conjugadas 33

6. Aplicações 35

CAPÍTULO II - As Álgebras de Incidência e a Funçaõ de Möbius... 44

1. Álgebras de Incidência 44

2. A Função de Möbius 45

3. O Princípio de Inclusão-Exclusão 48

(3.1) 48

(3.2) 49

4. A Função de Möbius e o Permanente de uma Matriz 51

(4.1) 51

(4.2) Aplicações 52

5. Conexões de Galois 56

(5.1) 56

(5.2) Aplicações e Exemplos 60

6. A Função de Möbius em Reticulados Finitos e Complementados 65
(6.1) 65
(6.2) A Função de Möbius em Reticulados Modulares Finitos 69
(6.3) Aplicações 72
7. Álgebras de Incidência Reduzidas 75

CAPÍTULO III - Coálgebras em Combinatória 80
1. Coálgebras 80
2. Coeficientes de Secção 81
3. Coálgebras de Incidência 83
(3.1) 83
(3.2) 86
(3.3) 87
4. A Coálgebra de Dirichlet 89
(4.1) Construção 89
(4.2) A Álgebra Dual da Coálgebra de Dirichlet 89
(4.3) A Estrutura de Anel Fatorial Subjacente em V* 90
5. Álgebras e Coálgebras Associadas a Recobrimentos 94
(5.1) 94
(5.2) 96
(5.3) 98

INTRODUÇÃO

Em 1980, após tomar conhecimento do artigo "Co-algebras and Bialgebras in Combinatorics", de S.A. Joni e G.C.Rota (19), resolvemos participar das atividades do Grupo de Estudos de Combinatória (GEPC) que já funcionava há algum tempo no Instituto de Biociências, Letras e Ciências Exatas da UNESP, em São José do Rio Preto, sob a direção do Prof. Dr. Ruy Madsen Barbosa. É que, a par das vantagens inegáveis do trabalho de pesquisa integrado, mormente em centros pequenos, novos e relativamente isolados, como é o caso de Rio Preto, o artigo referido mostrava um caminho, dentro da Combinatória, onde se tornava viável o uso de nossa formação mais específica na área de Álgebra, segundo um direcionamento teórico-prático quanto a estudos e pesquisas, o que era uma preocupação nossa àquela altura. Isto sem falar que o assunto, a nível pessoal, nos agradou sobremodo.

A linha do trabalho citado se inscreve no que poderia ser classificado, acreditamos, como Fundamentos da Combinatória. Diga-se de passagem que no GEPC ninguém, àquela altura, trabalhava nessa linha. Duas frases de Gian Carlo Rota, provavelmente o maior expoente neste campo de pesquisa, podem caracterizar bem a preocupação em vista. Ao enfocar o campo de problemas cuja abordagem algébrica é exposta em (19) afirma: "Com exceção da Teoria dos Números talvez não exista em Matemática um ramo tão rico em problemas e tão pobre em idéias gerais para resolvê-los..." Noutra oportunidade já dissera, a propósito de questões análogas: "A Combinatória precisa de mais teoria e de menos teoremas." O trabalho, sem dúvida brilhante, de matemáticos como Rota, P. Doubilet, M. Henle, S. Roman, R. Stanley, R. Mullin, A.M. Garsia, entre outros, consis

tiu fundamentalmente em construir embasamentos teóricos tão amplos quanto possível, visando a encontrar conexões e raizes comuns para problemas combinatórios muitas vezes aparentemente isolados. E as perspectivas abertas foram muito grandes. Mas como acontece invariavelmente em ciência, por traz dos grandes avanços há sempre a marca importante dos trabalhos pioneiros. Sem nos remontarmos à fase "primitiva" do assunto no século passado, há que registrar na década de 30 os passos importantes nesse sentido dados por M. Ward e L. Weisner. Mas foi em 1964, com os artigos de Rota: "The number of partitions of a set", inserido no texto de (22) e principalmente em (24) que as pesquisas nesse campo ganharam força e autonomia.

O primeiro capítulo do presente trabalho diz respeito à álgebra e ao cálculo umbral. Suas origens estão ligadas à notação umbral, usada já desde o século passado com vistas a um tratamento algorítmico de sequencias indexadas $(a_1,a_2,\ldots)$ como sequencias $(a^1,a^2,\ldots)$ de potências. Mas uma fundamentação teórica rigorosa para o "calculo" que daí resultava só surgiu em 1964, em (22), quando Rota teve a idéia de associar a uma sequencia (a_n) o funcional linear f, sobre o espaço dos polinômios, definido por $a_n = f(x^n)$ $(n = 0,1,2,\ldots)$. As propriedades em consideração da sequencia passam a ser retratadas pelo funcional de maneira mais simples e com abrangência teórica maior. A constatação de que esses funcionais podem ser multiplicados segundo a lei

$$(fg)(x^n) = \sum_{k=o}^{n} \binom{n}{k} f(x^k)\, g(x^{n-k})$$

com grande alcance para a combinatória, deu origem à álgebra umbral, designação devida a Roman e Rota. Eis alguns pontos em que, resumidamente, acreditamos ter dado nossa contribuição pessoal ao assunto: (a)no seu aprofundamento teórico, ao considerar, em vez de $R[x]$, um espaço vetorial qualquer, de dimensão enumerável infinita, sobre um corpo de característica zero, o que exige a genera

lização do conceito de derivada para o de deslocamento; (b) no estabelecimento da conexão entre teoria assim construida e o cálculo umbral, para o que foi preciso introduzir a noção de base admissível, paralelamente à de base deslocamento; (c) na resolução, a partir dessa bagagem teórica e ainda dos conceitos de depósito e particional, recentemente introduzidos (21), de alguns problemas de contagem.

O capítulo II trata da função de Möbius em combinatória, portanto no contexto das álgebras de incidência. A função de Möbius foi introduzida no século passado para resolver o seguinte problema: se duas funções aritméticas f e g, estão relacionadas por $f(n) = \sum_{d|n} g(d)$, é possível expressar g em termos de f ? É bem conhecido que a resposta é afirmativa e se traduz por

$$g(n) = \sum_{d|n} \tilde{\mu}(d) f(\frac{n}{d})$$

onde $\tilde{\mu}$ é a função de Möbius da aritmética, surgida em função desse problema. A questão que se apresenta em princípio é substituir a relação de ordem definida por "x|y", subjacente a esse caso particular, por uma relação de ordem "$\leqslant$" genérica sobre um conjunto P, de sorte que $(P, \leqslant)$ seja localmente finito, e verificar se é possível uma inversão como a citada da teoria dos números. Os primeiros a mostrar que a generalização do problema é válida foram L. Weisner e P. Hall, independentemente, este último um pouco de tempo depois do primeiro. Mas ao que parece nenhum dos dois vislumbrou as implicações combinatórias que seu trabalho comportava. Por exemplo, um dos mais úteis e conhecidos princípios da combinatória, o de inclusão-exclusão, é uma consequencia da fórmula de inversão de Möbius para o caso de uma álgebra booleana finita. Neste capítulo, paralelamente ao desenvolvimento da teoria necessária, fomos procurando colocar e resolver problemas que nela pudessem se inserir, como por exemplo o da contagem do número de permutações com

um primeiro elemento fixo, além de outros, entre os quais destacamos alguns através de uma técnica de "zeros" e "uns" via permanente de uma matriz. (Em certos casos presumivelmente se trata de soluções novas de problemas já conhecidos.) No item 6.2 estabelecemos resultado teórico pelo qual é possível expressar a função de Möbius nos reticulados modulares finitos e complementados em termos do número de complementares dos membros de uma cadeia maximal, o que propicia uma maneira mais uniforme para a resolução de diversos problemas ligados a inversão nesses reticulados, como exemplificamos em várias situações, logo a seguir.

O último capítulo diz respeito ao uso da estrutura de coálgebra em Combinatória. Não foi senão relativamente há pouco tempo que se percebeu que a noção de coálgebra, como de resto a de biálgebra e a de álgebra de Hopf, podem se constituir em estruturas teóricas importantes para a Combinatória, conforme o que foi delineado de início nesta introdução. Basta observar que a diagonalização, um dos elementos constitutivos de uma coálgebra, é uma transformação linear que oferece a possibilidade de traduzir matematicamente o efeito de "decompor" em partes, obedecidas convenientes prescrições, algum "objeto" em estudo, o que interessa à Combinatória. Quanto a esta parte, um resumo de nosso trabalho é o seguinte: (i) focalizamos algumas coálgebras, como aquelas resultantes do conceito de coeficientes de secção (uma generalização dos coeficientes binomiais) e as de incidência, plenas ou reduzidas; (ii) vimos como fazer a conexão deste assunto com os itens pertinentes do capítulo II, através da dualidade, e em especial nos detivemos na dual da coálgebra de Dirichlet, para a qual vimos ser válida a generalização, no que se refere à estrutura de anel fatorial, do que ocorre com as funções aritméticas relativamente à convolução de Dirichlet, mostrando ainda que este dual não é principal; (iii) introduzimos as coálgebras associadas a recobrimentos =

de conjuntos finitos, o que permite tratar com menos hipóteses algébricas certas situações examinadas em (19), com resultados no que se refere à função de Möbius no caso que denominamos de recobrimentos quase-independentes.

CAPÍTULO I

ÁLGEBRAS UMBRAIS

1. Deslocamentos em Espaços Vetoriais.

Indicaremos sempre por V, neste capítulo, um espaço vetorial de dimensão infinita enumerável sobre um corpo K de característica zero.

Definição 1. a) Um operador linear S sobre V é chamado do deslocamento em V se dim $\mathrm{Ker}(S^n) = n$, para todo $n \geq 0$, e se $V = \bigcup_{n\geq 0} \mathrm{Ker}(S^n)$, b) Uma sequencia $B = (e_n)$, $n = 0, 1, 2, \ldots$, onde $e_o \neq 0$, se diz uma base deslocamento de S se $S(e_o) = 0$ e $S(e_n) = n\, e_{n-1}$ para todo $n \geq 1$.

É fácil provar, por indução, que os vetores $e_o, e_1, \ldots, e_n$ são linearmente independentes, para todo $n \geq 0$. Observemos ainda que da definição 1 decorre que $S^k(e_r) = (r)_k\, e_{r-k}$, sempre que $r \geq k$, e $S^k(e_r) = 0$ se $r < k$. Donde $S^{n+1}(e_r) = 0$ para $r = 0, 1, 2, \ldots, n$; então $e_o, e_1, \ldots, e_n \in \mathrm{Ker}(S^{n+1})$. Considerando que dim $\mathrm{Ker}(S^{n+1}) = n+1$, então $(e_o, e_1, \ldots, e_n)$ é base de $\mathrm{Ker}(S^{n+1})$ para todo $n \geq 0$. Assim, levando em conta que $V = \bigcup_{n\geq 0} \mathrm{Ker}(S^n)$, podemos concluir que B é uma base de V pois, sempre que $r \geq 0$, a sequencia $(e_o, e_1, \ldots, e_r)$ é necessariamente livre.

Definição 2. Seja u uma avaliação sobre V, isto é, um funcional linear não nulo sobre V. Dizemos que uma base deslocamento (e_n) de S está normalizada em relação a u se $u(e_o) = 1$ e $u(e_n) = 0$, para todo $n \geq 1$.

Por exemplo, se $V = K[x]$ é considerado espaço vetorial sobre K, o operador $D = \frac{d}{dx}$ é um deslocamento em V e $B = (1, x, x^2, \ldots)$ é uma base deslocamento para esse operador, normalizada em relação ao funcional definido por $p(x) \to p(o)$.

Seja $(H_1, H_2, \ldots)$ uma sequencia de operadores lineares de V. Se existe um operador linear H de V de maneira que, para todo e_r de B, existe um índice n_o de maneira que $H_n(e_r) = H(e_r)$, sempre que $n > n_o$, dizemos que a sequencia (H_n) converge para H. É óbvio então que a sequencia $(I, S, S^2, \ldots)$, onde I é o operador idêntico de V, converge para o operador nulo. Também é fácil ver que uma série $\Sigma a_n S^n$ $(n = 0,1,2,\ldots)$ converge. De fato, considerando e_r em B, para todo $n > r$.

$(a_o + a_1 S + \ldots + a_r S^r + \ldots + a_n S^n)(e_r) = (a_o + a_1 S + \ldots + a_r S^r)(e_r)$ ou seja $\Sigma a_n S^n = H$, onde $H(e_r) = (a_o + a_1 S + \ldots + a_r S^r)(e_r)$ $(r \geq 0)$. Um operador $H = \Sigma a_n S^n$ é chamado série de potências de S, com termo constante a_o.

Proposição 1. Seja S um operador deslocamento em V. Então: (a) Existe uma base deslocamento (e_n) para V; (b) Se (e'_n) também é uma base deslocamento para S, existe uma série formal T em S, com termo constante não nulo, de modo que $T(e_n) = e'_n$ $(n = 0,1,2,..)$; (c) Se u é uma avaliação sobre V que não se anula no núcleo de S, então existe e é única uma base deslocamento normalizada em relação a u.

Demonstração

(a) Se $N_n = \text{Ker}(S^n)$, então é claro que $N_n \subset N_{n+1}$ $(n = 0,1,2,\ldots)$. Além disso, se $y \in S(N_{n+1})$, então $y = S(x)$, $x \in N_{n+1}$, e daí $S^n(y) = S^{n+1}(x) = 0$ o que leva à conclusão que $y \in \text{Ker}(S^n) = N_n$. Assim: $S(N_{n+1}) \subset N_n \subset N_{n+1}$, para todo $n \geq 0$. Donde $S|N_{n+1}$ é um operador linear em N_{n+1}.

Mostremos que $N_1 = \text{Ker}(S|N_r)$, para todo $r \geq 1$. De fato: se $x \in N_1$, então $x \in N_r$ e daí $(S|N_r)(x) = S(x) = 0$, para qualquer $r \geq 1$; é óbvia, por outro lado, a inclusão contrária. Portanto, para todo $n \geq 0$, $\dim \text{Ker}(S|N_{n+1}) = \dim N_1 = 1$. Como

$$\dim N_{n+1} = n+1 = \dim \text{Ker}(S|N_{n+1}) + \dim \text{Im}(S|N_{n+1})$$ en-

tão dim Im $(S|N_{n+1}) = n$. Juntando-se a isso que $S(N_{n+1}) \subset N_n$, então Im $(S|N_{n+1}) = N_n$, isto é, $S|N_{n+1}: N_{n+1} \to N_n$ é sobrejetora.

Tomemos $e_o \in N_1$, $e_o \neq 0$, o que implica $S(e_o) = 0$. Sendo $S|N_2$ sobrejetora, existe $e_1 \in N_2$ de modo que $S(e_1) = e_o$. Analogamente, como $S|N_3 : N_3 \to N_2$ é sobrejetora e $2e_1 \in N_2$, existe $e_2 \in N_3$ de maneira que $S(e_2) = 2e_1$. Com base nesse raciocínio, por indução podemos garantir a existência de uma base deslocamento $(e_o, e_1, \ldots$ $\ldots, e_n, \ldots)$ para S.

(b) Seja (e'_n) também uma base deslocamento para S. Como $S(e'_o) = 0$, então $e'_o \in N_1$ e daí $e'_o = \lambda_o e_o$, com $\lambda_o \neq 0$. Daí $S(e'_1 - \lambda_o e_1) = e'_o - \lambda_o e_o = 0$ e $e'_1 - \lambda_o e_1 \in N_1$ o que significa que $e'_1 - \lambda_o e_1 = \lambda_1 e_o$, para algum $\lambda_1 \in K$. Tomando $n \geq 1$ e supondo que

$$\frac{1}{n!} e'_n - \frac{1}{n!} \lambda_o e_n - \frac{1}{(n-1)!} \lambda_1 e_{n-1} - \cdots - \lambda_{n-1} e_1 = \lambda_n e_o$$

então

$$S\left(\frac{1}{(n+1)!} e'_{n+1} - \frac{1}{(n+1)!} \lambda_o e_{n+1} - \frac{1}{n!} \lambda_1 e_n - \cdots -\right.$$

$$\left. \cdots - \frac{1}{2!} \lambda_{n-1} e_2 - \lambda_n e_1\right) = 0.$$

Donde existe $\lambda_{n+1} \in K$ para o qual

$$\frac{1}{(n+1)!} e'_{n+1} - \frac{1}{(n+1)!} \lambda_o e_{n+1} - \frac{1}{n!} \lambda_1 e_n - \cdots - \lambda_n e_1 = \lambda_{n+1} e_o$$

Assim, para todo $n \geq 0$:

$$e'_n = \lambda_o e_n + n\lambda_1 e_{n-1} + n(n-1)\lambda_2 e_{n-2} + \ldots + n!\lambda_{n-1} e_1 + n!\lambda_n e_o$$

Ou seja

$$e'_n = \sum_{i=o}^{n} (n)_i \lambda_i e_{n-i} = \sum_{i=o}^{n} \lambda_i S^i(e_n) = \left(\sum_{i=o}^{n} \lambda_i S^i\right)(e_n) =$$

$$= \left(\sum_{i=o}^{\infty} \lambda_i S^i\right)(e_n) = T(e_n)$$

onde $T = \sum_{i=o}^{\infty} \lambda_i S^i$.

(c) Seja V_o o núcleo de u e mostremos que $V = V_o + N_1$. Como $u(e_o) \neq 0$, então K é gerado por $u(e_o)$ e portanto existe, para todo índice $n \geq 0$, um escalar λ_n tal que $u(e_n) = \lambda_n u(e_o)$. Daí $u(e_n - \lambda_n e_o) = 0$ e $e_n - \lambda_n e_o \in V_o$ ($\lambda_o = 1$). Donde $e_n \in [e_o] + V_o$, do que segue: $V \subset [e_o] + V_o = N_1 + V_o$. A inclusão contrária é óbvia.

Com isso podemos estabelecer que $N_{n+1} = (N_{n+1} \cap V_o) + N_1$. Que o segundo membro está contido no primeiro é fácil de ver. Se $x \in N_{n+1}$, como $N_{n+1} \subset V = V_o + N_1$, então $x = v_o + n_1$ ($v_o \in V_o$; $n_1 \in N_1$), daí $v_o = x - n_1 \in N_{n+1}$, visto que $n_1 \in N_1 \subset N_{n+1}$. Donde $x = v_o + n_1 \in [(N_{n+1} \cap V_o) + N_1]$. Levando em conta a linearidade de S:

$$N_n = S(N_{n+1}) = S(N_{n+1} \cap V_o) + S(N_1) = S(N_{n+1} \cap V_o)$$ ou seja, a restrição de S a $N_{n+1} \cap V_o$ é linear sobre N_n.

Assim, seja $e_o \in N_1$ tal que $u(e_o) = 1$. Como a restrição de S a $N_2 \cap V_o$ tem por imagem N_1, existe $e_1 \in N_2 \cap V_o$ de modo que $S(e_1) = e_o$. Assim sucessivamente, obtemos a sequencia $(e_o, e_1, e_2, \ldots)$ onde $S(e_{n+1}) = (n+1)e_n \in N_{n+1} \cap V_o$ ($n \geq o$). Trata-se de uma base normalizada em relação a u já que $u(e_o) = 1$ e $e_1, e_2, e_3, \ldots \in V_o = \text{Ker}(u)$.

Vejamos agora a unicidade desta base. De $N_{n+1} = (N_{n+1} \cap V_o) + N_1$ decorre que

$$n+1 = \dim N_{n+1} = \dim (N_{n+1} \cap V_o) + \dim N_1 - \dim (N_{n+1} \cap V_o \cap N_1) = \dim (N_{n+1} \cap V_o) + 1 - \dim (N_1 \cap V_o)$$

Como $V_o = \text{Ker}(u)$ e u não se anula em N_1, salvo no vetor nulo, então $N_1 \cap V_o = \{0\}$. Donde

$$\dim (N_{n+1} \cap V_o) = n = \dim N_n$$

Assim N_n e $N_{n+1} \cap V_o$ são isomorfos através de S (em virtude de $S(N_{n+1} \cap V_o) = N_n$). Consequentemente, para cada $n \geq 1$, é único o elemento $e_n \in N_{n+1} \cap V_o$ tal que $S(e_n) = n.e_{n-1}$. Agora, se $e'_o \in N_1$, então $e'_o = \lambda e_o$ e daí $u(e'_o) = \lambda u(e_o) = \lambda$, o que mostra que também é único o elemento e_o para o qual $u(e_o) = 1$.

Proposição 2. Seja S um operador deslocamento sobre V. (a) Se M é um operador linear inversível em V, então $M S M^{-1}$ = também é um deslocamento em V; (b) Se (e_n) é uma base deslocamento para S, então $(M(e_n))$ é uma base deslocamento de $M S M^{-1}$; (c) Se (e_n) esta normalizada em relação a u, então $(M(e_n))$ está normalizada em relação a $u M^{-1}$.

Demonstração

(a) Se $(g_o, g_1, \ldots, g_{n-1})$ é uma base de $Ker(S^n)$, então $(M(g_o), \ldots, M(g_{n-1}))$ é base de $Y_n = Ker(M S^n M^{-1})$. Como $(M S^n M^{-1})(M(g_i)) = 0$, então $M(g_i) \in Ker(Y_n)$ $(i = 0,1,\ldots, n-1)$. Se $x \in Y_n$, então $(M S^n M^{-1})(x) = 0$ e, como M é inversível, $(S^n M^{-1})(x) = 0$; daí $M^{-1}(x) \in Ker(S^n)$, o que implica

$$M^{-1}(x) = \alpha_o g_o + \ldots + \alpha_{n-1} g_{n-1}$$

para convenientes $\alpha_o, \alpha_1, \ldots, \alpha_{n-1} \in K$. Daí

$$x = \alpha_o M(g_o) + \ldots + \alpha_{n-1} M(g_{n-1})$$

o que mostra que Y_n é gerado por $(M(g_o), \ldots, M(g_{n-1}))$. Como esta sequencia é obviamente livre, fica provada a afirmação feita.

Se $x \in V$, então $M^{-1}(x) \in V$ e, por hipótese, existe $n \geq 0$ de maneira que

$$M^{-1}(x) = \alpha_o g_o + \alpha_1 g_1 + \ldots + \alpha_{n-1} g_{n-1}$$

Daí

$$x = \alpha_o M(g_o) + \alpha_1 M(g_1) + \ldots + \alpha_{n-1} M(g_{n-1})$$

ou seja $x \in Y_n$. Portanto

$$V = \bigcup_{n \geq o} Y_n$$

(b) Como

$$(M\ S\ M^{-1})(M(e_o)) = M(S(e_o)) = 0$$

e, para $n \geq 1$:

$$(M\ S\ M^{-1})(M(e_n)) = M(n\ e_{n-1}) = n\ M(e_{n-1})$$

fica provada esta segunda parte.

(c) Óbvia.

2. Operadores.

Definição 3. A um operador linear $T : V \to V$ para o qual $TS = ST$ damos o nome de S-invariante. Se não houver dúvidas quanto ao deslocamento usado nos referiremos a T, nessas condições, como operador invariante.

Proposição 3. Seja S um operador deslocamento em V. Uma condição necessária e suficiente para que um operador linear $T : V \to V$ seja S-invariante é que T seja uma série formal de potências em S.

Demonstração. É imediato que se T é uma série formal de potencias em S, então $TS = ST$. Para a recíproca consideremos uma base deslocamento (e_n) de S e façamos $T(e_n) = e'_n$ $(n \geq 0)$. Como $S(e'_o) = S(T(e_o)) = T(S(e_o)) = 0$ e, para $n \geq 1$:

$$S(e'_n) = S(T(e_n)) = T(S(e_n)) = T(n\ e_{n-1}) = n\ e'_{n-1}$$

o raciocínio empregado na demonstração da proposição 1-b nos garante a existência de $L = \sum_{n=o}^{\infty} \lambda_n S^n$ de maneira que $L(e_n) = e'_n$ $(n \geq o)$. Donde $L = T$ e a demonstração fica concluida. Notemos que como (e'_n) não é necessariamente uma base de V, não podemos garantir que λ_o seja não nulo.

Proposição 4. Seja S um deslocamento em V e seja (e_n) uma base deslocamento para S. Indiquemos por (g_n) uma base de V e por M o operador linear inversível definido por $M(e_n) = g_n$. Então:

(a) (g_n) é uma base deslocamento para S se, e somente se, M é S-invariante; (b) Se M é S-invariante, então $(g_o, g_1, \ldots, g_n)$ é uma base de Ker (S^{n+1}), para todo $n \geq 1$.

Demonstração

(a) Para n = 0: $(M\ S)(e_o) = M(0) = S(g_o) = (S\ M)(e_o)$.

Se n > 0:

$$(M\ S)(e_n) = M(n\ e_{n-1}) = n\ g_{n-1} = S(g_n) = S(M(e_n)) = (S\ M)(e_n)$$

Por outro lado, se M S = S M:

$$S(g_o) = S(M(e_o)) = M(S(e_o)) = M(0) = 0$$

e, para n > 0:

$$S(g_n) = S(M(e_n)) = M(S(e_n)) = M(n\ e_{n-1}) = n\ g_{n-1}$$

(b) Para todo $n \geq 0$, se $x \in [g_o, g_1, \ldots, g_n]$ então $x = \alpha_o\ g_o + \ldots + \alpha_n\ g_n = M(\alpha_o\ e_o + \ldots + \alpha_n\ e_n)$. Daí

$$S^{n+1}(x) = (S^{n+1}\ M)(\alpha_o\ e_o + \ldots + \alpha_n\ e_n) = (M\ S^{n+1})(\alpha_o\ e_o + \ldots + \alpha_n\ e_n) = 0$$

Donde

$$[g_o, g_1, \ldots, g_n] \subset \text{Ker } (S^{n+1})$$

Como esses dois subespaços têm mesma dimensão, concluimos que Ker $(S^{n+1}) = [g_o, g_1, \ldots, g_n]$.

Corolário. Uma sequência (g_n), n = 0,1,2,..., de vetores de V é uma base deslocamento de S se, e somente se

$$g_n = \sum_{i=o}^{n} \binom{n}{i} \alpha_{n-i}\ e_i$$

para todo $n \geq 0$, onde $\alpha_{n-i} \in K$ e $\alpha_o \neq 0$.

Demonstração

($\leftarrow$) O fato de $\alpha_o \neq 0$ garante que (g_n) é base de V. Por outro lado

$$S(g_n) = \sum_{i=1}^{n} \binom{n}{i} . \alpha_{n-i} . i . e_{i-1} = \sum_{k=o}^{n-1} n \binom{n-1}{k} \alpha_{n-1-k}\ e_k = n\ g_{n-1}$$

para $n \geq 1$ e , obviamente, $S(g_o) = 0$. Donde (g_n) é uma base deslocamento de S.

($\rightarrow$) (Por indução sobre n). Suponhamos $g_o = \alpha_o e_o +$ $+ \alpha_1 e_1 + \ldots + \alpha_t e_t$. Mantidas as notações da proposição:

$$(S\,M)(e_o) = S(g_o) = \alpha_1 e_o + 2\alpha_2 e_1 + \ldots + t\alpha_t e_{t-1}$$

ao passo que

$$(M\,S)(e_o) = 0$$

Considerando que $M\,S = S\,M$, então

$$\alpha_1 = \alpha_2 = \cdots = \alpha_t = 0 \quad \text{e} \quad g_o = \alpha_o e_o$$

do que decorre, inclusive, que $\alpha_o \neq 0$.

Seja $n \geq 0$ e admitamos

$$g_n = \sum_{i=o}^{n} \binom{n}{i} \alpha_{n-i} e_i$$

Supondo ainda

$$g_{n+1} = b_o e_o + b_1 e_1 + \ldots + b_n e_n + b_{n+1} e_{n+1} + \ldots + b_t e_t \quad (b_i \in K)$$

então

$$(S\,M)(e_{n+1}) = S(g_{n+1}) = b_1 e_o + 2b_2 e_1 + \ldots + n\,b_n e_{n-1} + (n+1)b_{n+1} e_n + \ldots$$

$$\ldots + t\,b_t e_{t-1} = (M\,S)(e_{n+1}) = M((n+1)e_n) = (n+1)g_n = (n+1) \sum_{i=o}^{n} \binom{n}{i} \alpha_{n-i} e_i$$

Donde

$$b_r = \frac{1}{r}(n+1)\binom{n}{r-1}\alpha_{n-r+1} = \binom{n+1}{r}\alpha_{n-r+1} \quad (r = 1,2,..,n)$$

e $b_r = 0$ se $r > n$. Assim, fazendo $b_o = \alpha_{n+1}$ (único coeficiente novo em g_{n+1}), o corolário fica demonstrado.

Definição 4. Seja S um deslocamento em V. Um operador linear Q sobre V é chamado operador S-delta se Q é S-invariante, $Q(e_o) = 0$ e $Q(e_1) \neq 0$, para uma base deslocamento (e_n) de S.

Notemos que em virtude do corolário anterior a base deslocamento que figura na definição anterior é qualquer. De fato, se (g_n) é também uma base deslocamento de S, então $g_o = \alpha_o e_o$ = $(\alpha_o \neq 0)$ e $g_1 = \alpha_1 e_o + \alpha_o e_1$. Daí, se $Q(e_o) = 0$ e $Q(e_1) \neq 0$, então

$Q(g_o) = \alpha_o\, Q(e_o) = 0$ e

$Q(g_1) = \alpha_1\, Q(e_o) + \alpha_o\, Q(e_1) = \alpha_o\, Q(e_1) \neq 0$

Proposição 5. Para que um operador linear Q sobre V seja um operador S-delta é necessário e suficiente que $Q = \sum_{k=1}^{\infty} a_k S^k$, $a_1 \neq 0$.

Demonstração

($\rightarrow$) Como Q comuta com S, pela proposição 3: $Q = \sum_{k=o}^{\infty} a_k S^k$ ($a_k \in K$; $k \geq 0$). Como $Q(e_o) = a_o e_o = 0$, então $a_o = 0$ e como $Q(e_1) = a_1 e_o \neq 0$, então $a_1 \neq 0$.

($\leftarrow$) Sendo Q uma série formal de potências em S então Q é S-invariante, devido à proposição citada. Como $Q = a_1 S + a_2 S^2 + \ldots$, é claro que $Q(e_o) = 0$ e $Q(e_1) = a_1 \neq 0$.

Definição 5. Seja S um deslocamento em V. (a) Um operador linear T sobre V é chamado anti-deslocamento de S se = S T - T S = I; (b) Se a imagem de um anti-deslocamento T está contida no núcleo de uma avaliação u sobre V, dizemos que T é um anti-deslocamento definido.

Proposição 6. (a) Se S é um deslocamento em V, então existe um anti-deslocamento de S; (b) Se T e T' são anti-deslocamentos de S, então T - T' é S-invariante; (c) Se S é um deslocamento em V, então para cada avaliação u, se $u(e_n) = 0$ ($n \geq 1$), há um só anti-deslocamento de S, definido em relação a u.

Demonstração.

(a) Se (e_n) é uma base deslocamento de S, então o operador linear T definido por $T(e_n) = e_{n+1}$ ($n \geq 0$) é um anti-deslocamento de S.

(b) $S(T - T') = S T - S T' = I + T S - I - T'S =$

$= (T-T')S$

(c) Considerando T definido em (a), então

$$u(T(e_n)) = u(e_{n+1}) = 0$$

para todo $n \geq 0$ e portanto $Im(T) \subset Ker(u)$, o que mostra que T é definido. Seja T' também um anti-deslocamento definido de S. Devido a (b):

$$T - T' = L = \Sigma a_n S^n \quad (n \geq 0)$$

e daí

$$L(e_n) = (a_o I + a_1 S + \ldots + a_n S^n)(e_n) = a_o e_n + (n)_1 a_1 e_{n-1} + \ldots + (n)_n a_n e_o$$

o que implica

$$u(L(e_n)) = (n)_n a_n$$

Mas

$$u(L(e_n)) = u(T(e_n) - T'(e_n)) = u(T(e_n)) - u(T'(e_n)) = 0$$

e portanto $(n)_n a_n = 0$ o que dá $a_n = 0$, para todo $n \geq 0$. Donde $T = T'$.

Notemos que se T é um anti-deslocamento de S, por indução chega-se a que $S^n T - T S^n = n S^{n-1}$ $(n \geq 1)$. Portanto, se $Q = \Sigma a_n S^n$ $(n \geq 2;\ a_2 \neq 0)$, então

$$QT - TQ = \Sigma\, n\, a_n S^{n-1} \quad (n \geq 2)$$

é um operador S-delta.

3. Álgebras Umbrais.

Fixemos um deslocamento S em V e uma base deslocamento $B = (e_n)$ de S e indiquemos por V* o espaço vetorial dual de V. Se definirmos o "produto" fg de dois funcionais $f, g \in V^*$ por

$$(fg)(e_n) = \sum_{k=o}^{n} \binom{n}{k} f(e_k) g(e_{n-k}) \qquad (n \geq 0)$$

é fácil mostrar que V* adquire uma estrutura de álgebra associativa, comutativa com unidade, esta o funcional u já introduzido ($u(e_o) = 1$; $u(e_n) = 0$, se $n \geq 1$). A álgebra assim construida recebe o nome de álgebra umbral sobre V e será indicada simplesmente por V*.

A ordem de um funcional $f \in V^*$, $f \neq 0$, é o menor número natural r tal que $f(e_r) \neq 0$. Notação: 0(f). Por exemplo,

$0(u) = 0$. Se $0(f) = r$ e $0(g) = s$, através de cálculos fáceis chega-se a que

$$(fg)(e_{r+s}) = \binom{r+s}{r} f(e_r) g(e_s) \neq 0$$

e

$$(fg)(e_{r+s-i}) = 0 \qquad (0 \leqslant i \leqslant r+s)$$

Isto vem mostrar que $0(fg) = 0(f) + 0(g)$. Como consequencia desse fato tiramos que $fg \neq 0$, sempre que $f \neq 0$ e $g \neq 0$.

Proposição 7. Se $f,g \in V^*$ são funcionais não nulos, então: $f|g \iff 0(f) \leqslant 0(g)$.

Demonstração. É imediata a implicação ($\rightarrow$) considerando-se que a ordem do produto é a soma das ordens.

Quanto à recíproca, estamos supondo $s=0(f) \leqslant 0(g)=r$ e devemos encontrar $h \in V^*$ de sorte que $g = fh$. Assim $h(e_{r-s}) \neq 0$ e $h(e_i) = 0$ se $0 \leqslant i \leqslant r-s-1$ o que implica

$$(fh)(e_r) = \binom{r}{s} f(e_s) h(e_{r-s}) = g(e_r)$$

e então

$$h(e_{r-s}) = \frac{g(e_r)}{\binom{r}{s} f(e_s)}$$

Fazendo $r - s = t$, admitindo $h(e_n)$ definido para $n < t+i$ $(i \geqslant 1)$, então

$$g(e_{r+i}) = \binom{r+i}{s} f(e_s) h(e_{t+i}) + \binom{r+i}{s+1} f(e_{s+1}) h(e_{t+i-1}) + \ldots$$

$$\ldots + \binom{r+i}{r+i} f(e_{r+i}) h(e_o) \; .$$ Como $f(e_s) \neq 0$, da igualdade acima pode-se tirar $h(e_{t+i})$.

Da proposição demonstrada decorre que

. $f,g \in V^*$ são associados se, e somente se, $0(f) = 0(g)$.

. $f \in V^*$, $f \neq 0$, é inversível se, e somente se, $0(f) = 0$.

. $p \in V^*$, $p \neq 0$, p não inversível, é irredutí

vel se, e somente se, $0(p) = 1$.

Quanto a esta última observação devemos notar que para todo $r \in N^*$ existem obviamente funcionais $f \in V^*$ para os quais $0(f) = r$.

. todo $q \in V^*$ irredutível é primo.

Isto posto, da maneira habitual pode-se mostrar que o anel subjacente a V^* é fatorial. Mas isto poderia ser mostrado através dos ideais de V^*. Seja I um ideal em V^* e tomemos $f \in I$ de maneira que $0(f)$ seja mínima. Se $g \in I$, então $0(f) \leqslant 0(g)$ o que equivale a $f|g$ e portanto $g \in \langle f \rangle$. Donde $I = \langle f \rangle$.

Para cada $f \in V^*$ seja $T(f)$ o operador linear em V definido por

$$T(f)(e_n) = \sum_{k=0}^{n} \binom{n}{k} f(e_{n-k}) e_k$$

Uma verificação simples nos garante que $T(f)S = ST(f)$, para qualquer $f \in V^*$. Por isso damos o nome de operador S-invariante associado a f ao operador linear $T(f)$. Notemos que se w é o funcional linear definido por $w(e_r) = \delta_{r1}$, então $T(w)(e_o) = 0$ e $T(w)(e_n) = n\, e_{n-1}$ $(n \geqslant 1)$, o que garante que $T(w) = S$.

Por outro lado, se T é um operador S-invariante, o funcional $f(T)$ associado a T é definido por

$$(f(T))(e_n) = u(T(e_n)) \qquad (n \geqslant 0)$$

É imediato verificar que $f(T(g)(e_n)) = (fg)(e_n)$, para todo $n \geqslant 0$ e para quaisquer $f,g \in V^*$. Esta é a chamada fórmula de transferência.

Notemos que

$$(f(T(f)))(e_n) = u\left(\sum_{k=0}^{n} \binom{n}{k} f(e_{n-k}) e_k\right) = \sum_{k=0}^{n} \binom{n}{k} u(e_k) f(e_{n-k}) =$$

$= f(e_n)$ isto é, $f(T(f)) = f$, para todo $f \in V^*$. Por outro lado, como $T = a_o + a_1 S + a_2 S^2 + \ldots$ $(a_i \in K)$, então

$$T(e_{n-k}) = (n-k)_o a_o e_{n-k} + (n-k)_1 a_1 e_{n-k-1} + \ldots + (n-k)! a_{n-k} e_o$$

e portanto

$$u(T(e_{n-k})) = (n-k)! a_{n-k}$$

Donde

$$(T(f(T)))(e_n) = \sum_{k=o}^{n} \binom{n}{k} f(T)(e_{n-k}) e_k = \sum_{k=o}^{n} \binom{n}{k} u(T(e_{n-k})) e_k =$$

$$= \sum_{k=o}^{n} \binom{n}{k} (n-k)! a_{n-k} e_k = \sum_{k=o}^{n} (n)_{n-k} a_{n-k} e_k = T(e_n)$$

o que nos garante que $T(f(T)) = T$, para todo operador S-invariante T.

Assim, denotando por Γ o conjunto dos operadores S-invariantes de V e por ϕ e σ as aplicações

$$\phi : V^* \to \Gamma \; ; \quad \phi(f) = T(f)$$

$$\sigma : \Gamma \to V^* \; ; \quad \sigma(T) = f(T)$$

então $\phi\sigma = id_\Gamma$ e $\sigma\phi = id_{V^*}$, o que implica que ϕ e σ são bijetoras e cada uma é a inversa da outra. Por outro lado é uma questão apenas de cálculos mostrar que $\phi(fg) = \phi(f)\phi(g)$, $\phi(f+g) = \phi(f) + \phi(g)$ e $\phi(kf) = k\,\phi(f)$, para quaisquer $f,g \in V^*$ e todo $k \in K$. Logo Γ é uma álgebra isomorfa à algebra umbral V^*.

4. Funcionais Delta.

Como vimos fazendo já desde o item anterior consideraremos fixados um deslocamento S em V e uma base deslocamento $B = (e_n)$ de S.

Definição 6. Um funcional linear $h \in V^*$ é chamado funcional S-delta se $h(e_o) = 0$ e $h(e_1) \neq 0$.

Proposição 8. Um operador linear $Q : V \to V$ é um operador S-delta se, e somente se, existe um funcional S-delta h de maneira que $Q = T(h)$.

Demonstração

($\to$) Como $Q = \sum_{i=1}^{\infty} a_i S^i \quad (a_i \in K;\ a_1 \neq 0)$

então

$$Q(e_n) = a_1(n)_1\, e_{n-1} + a_2(n)_2\, e_{n-2} + \ldots + a_{n-1}(n)_{n-1}\, e_1 + a_n(n)_n\, e_o$$

Seja h o funcional definido por

$$h(e_o) = 0 \quad \text{e} \quad h(e_{n-k}) = \frac{n!}{(n)_k}\, a_{n-k} \quad (k = 0,1,\ldots,n-1)$$

Como $h(e_1) = a_1 \neq 0$, h é um funcional delta. Por outro lado, $\forall\, n \geq 0$:

$$T(h)(e_n) = \sum_{k=o}^{n} \binom{n}{k} h(e_{n-k}) e_k = \sum_{k=o}^{n-1} \binom{n}{k} \frac{n!}{(n)_k} a_{n-k}\, e_k =$$

$$= \sum_{k=o}^{n-1} (n)_{n-k}\, a_{n-k}\, e_k = Q(e_n)$$

e portanto $Q = T(h)$.

($\leftarrow$) É fácil calcular que $T(h)(e_o) = 0$ e $T(h)(e_1) = h(e_1)\, e_o \neq 0$. Logo $T(h)$ é um operador S-delta.

Com isso ficou provado que no isomorfismo $\phi : V^* \to \Gamma$ aos funcionais S-delta correspondem operadores S-delta.

Definição 7. Uma base (v_n) de V sobre K é dita admissível se $v_n = \sum_{k=o}^{n} a_{nk}\, e_k$ $(n \geqslant 0)$, $a_{nn} \neq 0$

e

$$(fg)(v_n) = \sum_{k=o}^{n} \binom{n}{k} f(v_k) g(v_{n-k})$$

para quaisquer $f, g \in V^*$.

Como $u^2 = u$, então

$$u(v_o) = u^2(v_o) = u(v_o)u(v_o)$$

Mas $u(v_o) = a_{oo}\, u(e_o) = a_{oo} \neq 0$. Logo $u(v_o) = 1 = a_{oo}$. Por outro lado, como

$$u(v_1) = u(v_o)u(v_1) + u(v_1)u(v_o)$$

então $u(v_1) = 2u(v_1)$ e $u(v_1) = 0$. Por indução pode-se mostrar então que $u(v_n) = 0$, para $n \geqslant 1$. Mas $u(v_n) = a_{no}$, o que implica que $a_{no} = 0$ sempre que $n > 0$.

Proposição 9. Seja (v_n) uma base admissível de V. (a) Se $h \in V^*$ é tal que $h(v_o) = 0$, então $h^k(v_n) = 0$, para todo $k > n$; (b) Se h é um funcional S-delta, então $h^n(v_n) = n![h(v_1)]^n \neq 0$.

Demonstração.

(a) Por indução sobre n.

(b) Se $n = 0$, $h^n = u$. Daí $u(v_o) = u(e_o) = 1 = 1![h(v_1)]^o$. Supondo a afirmação verdadeira para $n \geq 0$, então (levando em conta (a)):

$$h^{n+1}(v_{n+1}) = (h\, h^n)(v_{n+1}) = (n+1)h(v_1)h^n(v_n) = (n+1)\, h(v_1)n![h(v_1)]^n = (n+1)![h(v_1)]^{n+1} \neq 0.$$

Definição 8. Seja $h \in V^*$ um funcional S-delta. Uma base (v_n) de V é dita base associada a h se

$$v_n = \sum_{k=o}^{n} a_{nk}\, e_k \quad (a_{nn} \neq 0,\ n \geq 0) \quad \text{e} \quad h^k(v_n) = n!\, \delta_{nk} \quad (n,k \geq 0).$$

Da definição decorre facilmente que $a_{oo} = 1$ e $a_{no} = 0$ $(n > 0)$. Como

$$v_n = a_{no}\, e_o + a_{n1}\, e_1 + \ldots + a_{nn}\, e_n$$

levando em conta a proposição anterior

$$h^n(v_n) = a_{nn}\, h^n(e_n)$$

e

$$a_{nn} = h^n(v_n).\ [h^n(e_n)]^{-1}$$

visto que (e_n) é canonicamente admissível. A partir daí, pela aplicação sucessiva de h^{n-1}, h^{n-2}, ..., h a v_n, verifica-se que os a_{n1}, a_{n2}, ..., a_{nn} existem e estão univocamente determinados, $\forall$ $n \geq 1$. Donde é única a base associada a um funcional S-delta h.

Notemos que se (v_n) é a base associada ao funcional S-delta h, então $h(v_n) = n!\, \delta_{n1} = \delta_{n1}$. Por outro lado, se (v_n)

é uma base admissível de V e h é o funcional definido por $h(v_n) = \delta_{n1}$, então $h^o(v_n) = u(v_n) = \delta_{no} = n!\,\delta_{no}$; isto posto, admitindo que $h^k(v_n) = n!\,\delta_{nk}$ $(k \geq 0)$, então

$$h^{k+1}(v_n) = \sum_{t=o}^{n} \binom{n}{t} h^k(v_t) h(v_{n-t}) = \sum_{t=o}^{n} \binom{n}{t} t!\,\delta_{tk}\,\delta_{n-t,1}$$

Ora, esta última soma só não é nula quando $t = k$ e $n-t = 1$, ou seja $t = k = n-1$. Assim

$$h^{k+1}(v_n) = \binom{n}{n-1}(n-1)!\,\delta_{n-1,k} = n!\,\delta_{n,k+1}$$

Assim provamos a

Proposição 10. Seja (v_n) uma base admissível de V e seja $h \in V^*$ um operador S-delta. Para que (v_n) seja a base associada a h é necessário e suficiente que $h(v_n) = \delta_{n1}$ $(n \geq 0)$. Em particular (v_n) é a base associada ao funcional h, assim definido.

Desta proposição decorre que a base associada ao funcional w é exatamente (e_n). Cabe perguntar também, que bases deslocamento são admissíveis?

Proposição 11. A única base deslocamento admissível é (e_n).

Demonstração. Seja (g_n) uma base deslocamento admissível e indiquemos por M o automorfismo definido por $M(e_n) = g_n$. Como $(w\,M^{-1})(g_n) = w(e_n) = \delta_{n1}$, então (g_n) é a base associada a $w\,M^{-1}$. Como (g_n) é deslocamento:

$$g_o = \alpha_o e_o,\ g_1 = \alpha_1 e_o + \alpha_o e_1,\ g_2 = \binom{2}{0}\alpha_2 e_o + \binom{2}{1}\alpha_1 e_1 + \binom{2}{2}\alpha_o e_2, \ldots$$

Por ser também admissível, as considerações após a definição 7 impõem que: $\alpha_o = 1$, $\alpha_1 = 0$, $\alpha_2 = 0, \ldots$. Logo $g_n = e_n$ $(n \geq 0)$.

De maneira análoga ao que se fez para operadores, uma sequência $(f_1, f_2, \ldots)$ de funcionais de V* é dita convergente

para $f \in V^*$ se, para todo e_r de B, existe n_o de maneira que $f_n(e_r) = f(e_r)$, sempre que $n > n_o$. Se h é S-delta e (v_n) sua base associada, então (propos.9): $h^k(v_n) = 0$, para todo $k > n$. Donde $(u, h, h^2, \ldots)$ converge para o funcional nulo. É imediato, também, que uma série $\Sigma a_r h^r$ $(r \geq 0)$ converge para o funcional s definido por $s(v_r) = r!a_r$.

Mostremos que se h é S-delta então a sequência $(u, h, h^2, \ldots)$ é uma base de V^* sobre K. Como, para $r \geq 0$, se (v_n) é a base associada a h: $(a_o u + a_1 h + \ldots + a_r h^r)(v_r) = (r!)a_r$, então $(u, h, h^2, \ldots)$ é livre. Por outro lado, para todo $f \in V^*$:

$$\left(\Sigma \frac{f(v_r)}{r!} h^r \right)(v_n) = (n!) \frac{f(v_n)}{n!} = f(v_n)$$

e então $(u, h, h^2, \ldots)$ gera V^* sobre K.

Assim, se $f_1, f_2 \in V^*$, então $f_1 = \Sigma a_k h^k$ e $f_2 = \Sigma b_k h^k$, onde

$$a_k = \frac{f_1(v_k)}{k!} \quad \text{e} \quad b_k = \frac{f_2(v_k)}{k!}$$

e (v_n) é a base associada a h. Supondo $f_1 f_2 = \Sigma c_k h^k$, então

$$c_k = \frac{(f_1 f_2)(v_k)}{k!}$$

Mas

$$(f_1 f_2)(v_k) = \sum_{i=o}^{n} \binom{k}{i} f_1(v_i) f_2(v_{k-i}) = \sum_{i=o}^{n} \binom{k}{i} i! a_i (k-i)! b_{k-i} =$$

$$= k! \sum_{i=o}^{n} a_i b_{k-i}$$

Donde

$$c_k = \sum_{i=o}^{k} a_i b_{k-i}$$

o que mostra que a álgebra umbral V^* é isomorfa à álgebra $K[[t]]$ das séries formais sobre K

Logo, para todo funcional linear $f \in V^*$, como

$$f = \Sigma \frac{f(e_n)}{n!} w^n$$

pode-se associar a f a série formal

$$F(t) = \Sigma \frac{f(e_n)}{n!} t^n$$

que será chamada indicadora de f. Obviamente

$$f \longmapsto F(t)$$

é um isomorfismo.

Cálculos simples levam a

$$T(f) = \Sigma \frac{f(e_k)}{k!} S^k$$

para todo $f \in V^*$. Isto sugere que nos refiramos à série F(t) como indicadora também de T(f).

Proposição 12. Toda base associada a um funcional S-delta é admissível.

Demonstração. Se (v_n) é a base associada ao funcional S-delta h, para quaisquer $i,j \geq 0$:

$$(h^i h^j)(v_n) = h^{i+j}(v_n) = n!\ \delta_{n,i+j}$$

Por outro lado:

$$\sum_{k=0}^{n} \binom{n}{k} h^i(v_k) h^j(v_{n-k}) = \sum_{k=0}^{n} \binom{n}{k} k!\delta_{ki}(n-k)!\delta_{n-k,j} =$$

$$= \binom{n}{i} i!(n-i)!\delta_{n-i,j} = n!\delta_{n,i+j}$$

Portanto

$$(h^i h^j)(v_n) = \sum_{k=0}^{n} \binom{n}{k} h^i(v_k) h^j(v_{n-k})$$

Agora, como (h^n) é uma base de V*, para quaisquer $f_1 = \Sigma a_r h^r$ e $f_2 = \Sigma b_s h^s$ em V*, é uma questão apenas de cálculos verificar que

$$(f_1 f_2)(v_n) = \sum_{k=0}^{n} \binom{n}{k} f_1(v_k) f_2(v_{n-k})$$

Proposição 13. Uma base (v_n) de V sobre K, $v_o = e_o$ e $v_n = a_{no}e_o + \ldots + a_{nn}e_n$ $(n > 0;\ a_{nn} \neq 0)$ é admissível se, e somente se

$$\binom{i+j}{i} a_{n,i+j} = \sum_{k=o}^{n} \binom{n}{k} a_{ki}\, a_{n-k,j} \qquad (*)$$

Demonstração.

($\rightarrow$) Para todo $v_s = a_{so}e_o + \ldots + a_{si}e_i + \ldots + a_{ss}e_s$, como (e_n) é a base associada a w, então $w^i(v_s) = a_{si}.i!$. Donde

$$a_{ki} = \frac{w^i(v_k)}{i!} \quad \text{e} \quad a_{n-k,j} = \frac{w^j(v_{n-k})}{j!}$$

Logo

$$\sum_{k=o}^{n} \binom{n}{k} a_{ki}a_{n-k,j} = \sum_{k=o}^{n} \binom{n}{k} \frac{w^i(v_k)}{i!} \cdot \frac{w^j(v_{n-k})}{j!} = \frac{1}{i!j!}\, w^{i+j}(v_n) =$$

$$= \frac{(i+j)!}{i!j!}\, a_{n,i+j} = \binom{i+j}{i} a_{n,i+j}$$

($\leftarrow$) Reciprocamente, de (*) decorre que

$$\binom{i+j}{i} \frac{w^{i+j}(v_n)}{(i+j)!} = \sum_{k=o}^{n} \binom{n}{k} \frac{w^i(v_k)}{i!} \cdot \frac{w^j(v_{n-k})}{j!}$$

e então

$$w^{i+j}(v_n) = \sum_{k=o}^{n} \binom{n}{k} w^i(v_k)w^j(v_{n-k})$$

Como porém $(u, w, w^2, \ldots)$ é uma base de V* sobre K, o raciocínio usado na proposição anterior garante que (v_n) é admissível.

Definição 9. Se $h \in V^*$ é um funcional S-delta, a sequencia (v_n) definida por

$$v_n = \sum_{k=o}^{n} \frac{h^k(e_n)}{k!}\, e_k$$

é chamada sequencia conjugada de h.

Como da definição decorre facilmente que $v_o = e_o$ e como

$$\frac{h^n(e_n)}{n!} = \frac{n!\,[h(e_o)]^n}{n!} = [h(e_o)]^n \neq 0$$

então (v_n) é uma base de V. Como ainda

$$\binom{i+j}{i}\frac{h^{i+j}(e_n)}{(i+j)!} = \frac{1}{i!j!}\,h^{i+j}(e_n) = \sum_{k=o}^{n}\binom{n}{k}\frac{h^i(e_k)}{i!}\;\frac{h^i(e_{n-k})}{j!}$$

então os coeficientes dos vetores v_n satisfazem (*) da proposição anterior e portanto (v_n) é admissível. Assim nos referiremos a (v_n), conforme definição 9, como a base conjugada de h.

Notemos ainda que os coeficientes $c_{n1} = h(e_n)$ determinam todos os demais vetores v_n. Basta notar que, por exemplo

$$h^2(e_n) = \sum_{k=o}^{n}\binom{n}{k}h(e_k)h(e_{n-k}) = \sum_{k=o}^{n}\binom{n}{k}c_{k1}\cdot c_{n-k,1}$$

Proposição 14. Toda base conjugada de um funcional S-delta é admissível e, reciprocamente, toda base admissível é conjugada de um conveniente funcional S-delta.

Demonstração. A primeira dessas afirmações está justificada nas considerações que seguem a última definição.

Seja (v_n), onde $v_o = e_o$ e $v_n = \sum_{k=o}^{n} a_{nk}e_k$ $(a_{nn} \neq 0)$, para $n \geq 1$, uma base admissível. Definamos então, para cada $k \geq 0$, o funcional $h_k \in V^*$ por $h_k(e_n) = k!a_{nk}$. Como $h_1(e_o) = 0$ e $h_1(e_1) = a_{11} \neq 0$, h_1 é S-delta. Levando em conta a condição (*) da proposição 13, para todo $n \geq 0$:

$$h_{i+j}(e_n) = (i+j)!a_{n,i+j} = i!j!\,\frac{(i+j)!}{i!j!}\,a_{n,i+j} =$$

$$= i!j!\binom{i+j}{i}a_{n,i+j} = i!j!\sum_{k=o}^{n}\binom{n}{k}a_{ki}a_{n-k,j} = i!j!\sum_{k=o}^{n}\binom{n}{k}\frac{h_i(e_k)}{i!}\;\frac{h_j(e_{n-k})}{j!} =$$

$$= \sum_{k=o}^{n} \binom{n}{k} h_i(e_k) h_j(e_{n-k}) = (h_i h_j)(e_n)$$

Donde $h_{i+j} = h_i h_j$ para quaisquer $i,j \geq 0$. Como consequencia $h_k = h_1^k$, sempre que $k \geq 0$. Donde

$$a_{nk} = \frac{h_k(e_n)}{k!} = \frac{h_1^k(e_n)}{k!}$$

e portanto (v_n) é a sequencia conjugada do funcional S-delta h_1.

Assim, a cada funcional S-delta h, correspondem duas bases admissíveis: sua base associada e sua base conjugada, que se dizem recíprocas uma da outra. No caso em que coincidem, para um certo funcional, dizemos que se trata de uma base auto-recíproca. Por exemplo, já vimos que a base associada a w é (e_n). Calculemos a base conjugada de w, definida por

$$v_n = \sum_{k=o}^{n} \frac{w^k(e_n)}{k!} e_k$$

Ora, é fácil mostrar, por indução, que $w^k(e_n) = (n)_{k-1} \delta_{n,k}$, para $k \geq 1$. Disto decorre que $v_o = e_o$ e, para $n \geq 1$:

$$v_n = \sum_{k=o}^{n} \frac{(n)_{k-1} \delta_{nk}}{k!} e_k = \frac{(n)_{n-1}}{n!} e_n = e_n$$

e portanto (e_n) é auto-recíproca.

Por outro lado, se (v_n) é uma base admissível, podemos associar a ela dois funcionais S-delta: o funcional h cuja base associada é (v_n) e o funcional $\tilde{h}$ do qual (v_n) é a base conjugada. Diz-se que h e $\tilde{h}$ são recíprocos. Se $h = \tilde{h}$, este funcional se diz auto-recíproco.

Definição 10. Um operador linear $A: V \to V$ que transforma uma base associada em outra base associada, ambas de funcionais S-delta, é chamado operador umbral.

Se A é umbral, o operador adjunto de A, definido por $A^*(h)(z) = h(A(z))$, para todo $h \in V^*$ e todo $z \in V$, é um automorfismo da álgebra V^*. Alem disso, se (p_n) é a base associada a h e (q_n) a associada a g e se $A(p_n) = q_n$ $(n \geq 0)$, então $A^*(g) = h$ pois:

$$A^*(g)(p_n) = g(A(p_n)) = g(q_n) = \delta_{n1} = h(p_n)$$

Notemos também que se uma sequencia $(h_1, h_2, \ldots)$ de funcionais converge para h, então

$$A^*(h_n)(e_r) = h_n(A(e_r)) = h(A(e_r)) = A^*(h)(e_r)$$

a partir de um conveniente índice n_o. Logo $(A^*(h_n))$ converge para $A^*(h)$, ou seja, A^* é contínuo.

5. O Cálculo Umbral.

5.1. Introdução.

Seja K um corpo de característica zero e consideremos a álgebra $U = K[x]$. A base (x^n) de U é uma base deslocamento associada à derivada D em U. Uma sequencia polinomial $p_n(x)$, $n = 0,1,2,\ldots$, é uma sequencia de polinômios em que o grau de $p_n(x)$ é n, para todo $n \geq 0$. Logo toda sequencia polinomial é uma base de $K[x]$ sobre K. Uma sequencia polinomial é dita uma base binomial de U sobre K se a identidade binomial

$$p_n(x+y) = \sum_{k=o}^{n} \binom{n}{k} p_k(x) p_{n-k}(y)$$

se verifica, para quaisquer $x, y \in K$ e todo $n \geq 0$. Da definição decorre que $p_o(x) = 1$ e $p_n(0) = 0$, se $n \geq 1$.

Proposição 15. Uma sequencia polinomial $p_n(x)$, $n = 0,1,\ldots$, é uma base binomial de U se, e somente se $(p_n(x))$ é uma base admissível desta álgebra.

Demonstração.

($\leftarrow$) Para cada $a \in K$ seja ε_a o funcional linear definido por $\varepsilon_a(x^n) = a^n$. Se $a, b \in K$, então $(\varepsilon_a \varepsilon_b)(x^n) =$

$$= \sum_{k=o}^{n} \binom{n}{k} \varepsilon_a(x^k)\varepsilon_b(x^{n-k}) = \sum_{k=o}^{n} \binom{n}{k} a^k b^{n-k} = (a+b)^n = \varepsilon_{a+b}(x^n)$$

Donde $\varepsilon_a \varepsilon_b = \varepsilon_{a+b}$, para quaisquer $a,b \in K$. Como, por hipótese,

$$(\varepsilon_a \varepsilon_b)(p_n(x)) = \sum_{k=o}^{n} \binom{n}{k} \varepsilon_a(p_k(x))\, \varepsilon_b(p_{n-k}(x))$$

então

$$p_n(a+b) = \sum_{k=o}^{n} \binom{n}{k} p_k(a)\, p_{n-k}(b)$$

para quaisquer $a,b \in K$.

($\rightarrow$) Seja $P = K[x,y]$ o espaço vetorial sobre K dos polinomios nas variáveis x e y. Se f é um funcional linear sobre $K[x]$, seja f_x o operador linear em P definido por

$$f_x\, p(x,y) = \Sigma\, a_{ij}\, f(x^i)y^j$$

para todo $p(x,y) = \Sigma\, a_{ij} x^i y^j \in P$. Analogamente o operador f_y é definido por

$$f_y\, p(x,y) = \Sigma\, a_{ij}\, f(y^j)x^i$$

onde $f(y^j) = f(x^j)$, $j = 0,1,\ldots$. Daí

$$(f_x o g_y)(x+y)^n = (f_x o g_y)\left(\sum_{k=o}^{n} \binom{n}{k} x^k y^{n-k}\right) = \sum_{k=o}^{n} \binom{n}{k} f(x^k)\, g(y^{n-k}) = (fg)(x^n)$$

Como (x^n) gera $K[x]$, para todo $p(x) \in K[x]$:

$$(fg)(p(x)) = (f_x o\, g_y)p(x+y)$$

Em particular, se $n \geq 0$:

$$(fg)(p_n(x)) = (f_x o\, g_y)p_n(x+y)$$

Como porem

$$(f_x o\, g_y)p_n(x+y) = (f_x o\, g_y) \sum_{k=o}^{n} \binom{n}{k} p_k(x)\, p_{n-k}(y) = \sum_{k=o}^{n} \binom{n}{k} f(p_k(x))\, g(p_{n-k}(x))$$

então

$$(fg)(p_n(x)) = \sum_{k=o}^{n} \binom{n}{k} f(p_k(x)) g(p_{n-k}(x))$$

e $(p_n(x))$ efetivamente é admissível.

5.2. Base Associada a um Operador D-delta.

Seja Q um operador linear D-delta em U. É imediato que se $p(x) \in U$ tem grau $n \geq 1$, então $Q(p(x))$ é de grau n-1. A partir deste fato pode-se construir uma única base $(p_n(x))$ de U sobre K, de maneira que $gr(p_n(x)) = n$ $(n = 0,1,...)$ e: (i) $p_o(x) = 1$; (ii) $p_n(0) = 0$, se $n \geq 1$; (iii) $Q\, p_n(x) = n\, p_{n-1}(x)$. Para tanto basta notar que, supondo-se $p_o(x)$, $p_1(x)$,..., $p_{n-1}(x)$ já obtidos, um polinomio genérico de grau n pode ser colocado como

$$p(x) = a\, x^n + \sum_{k=o}^{n-1} c_k\, p_k(x)$$

Sendo $Q(x^n)$ de grau n-1, há uma só escolha para as constantes $c_1, c_2, \ldots, c_{n-1}$ de modo que $Q\, p(x) = n\, p_{n-1}(x)$. A escolha de c_o está univocamente determinada pelo fato de que $p_n(0) = 0$, $n \geq 1$. Assim fica justificada a observação feita. Chamaremos $(p_n(x))$, obtida dessa maneira, de base associada a Q.

O fato de Q ser D-delta assegura a existência de um funcional D-delta h para o qual $T(h) = Q$. Observemos que $h^o\, p_o(x) = u(1) = 1$ e $u(p_n(x)) = 0$ se $n > 0$ pois $p_n(x)$ não tem termo constante. Logo $h^o p_n(x) = n!\delta_{no}$ $(n \geq 0)$. Além disso:

$$h(p_n(x)) = (u\, h)p_n(x) = u(T(h)p_n(x)) = u(n\, p_{n-1}(x)) = n!\delta_{n1}$$

Admitindo $h^k p_n(x) = n!\delta_{nk}$, para $n \geq 0$ e $k \geq 1$, então:

$$h^{k+1} p_n(x) = h^k(T(h)p_n(x)) = h^k(n\, p_{n-1}(x)) = n(n-1)!\delta_{n-1,k} = n!\delta_{n,k+1}$$

o que mostra que $(p_n(x))$ é a base associada a h. Logo $(p_n(x))$ é admissível e portanto binomial.

Por exemplo, para cada $a \in k$, seja E^a o operador

linear de translação definido por $E^a(x^n) = (x+a)^n$. É imediato que E^a é D-invariante e que o operador $Q = E^aD$ é D-delta. Achemos a base associada a Q. Como $p_1(x) = cx$, então $(E^aD)(cx) = E^a(c) = c = p_o(x) = 1$. Logo $p_1(x) = x$. Supondo $p_2(x) = cx^2 + c_1x$, então $(E^aD)(p_2(x)) = E^a(2cx + c_1) = 2c(x+a)+c_1 = 2x$. Donde $c=1$ e $c_1 = -2a$ o que dá: $p_2(x) = x(x-2a)$. Por indução chega-se a que $p_n(x) = x(x-na)^{n-1}$ $(n \geq 1)$. Estes polinômios são chamados polinômios de Abel.

Já salientamos anteriormente que, como para um funcional D-delta h vale

$$h = \Sigma \frac{h(x^n)}{n!} w^n$$

então

$$T(h) = \Sigma \frac{h(x^n)}{n!} D^n$$

Mas de $T(h)x^n = \Sigma \binom{n}{k} h(x^{n-k}) x^k$ decorre que $\left[T(h)x^n\right]_{x=o} = h(x^n)$. Donde

$$T(h) = \Sigma \frac{\left[T(h)x^n\right]_{x=o}}{n!} D^n$$

Sejam $(p_n(x))$ e $(q_n(x))$ as bases associadas aos dos operadores D-delta P e Q, respectivamente e consideremos o operador inversível $F: U \to U$ definido por $F(p_n(x)) = q_n(x)$. Se $(r_n(x))$ é a base associada a um operador R, então $(s_n(x))$, definida por $F\, r_n(x) = s_n(x)$ é a base associada a $S = F\, R\, F^{-1}$. De fato. Como $F\, p_o(x) = q_o(x) = 1$, então $F\, r_o(x) = F\, p_o(x) = 1$. Por outro lado, como para $n > 0$, $r_n(x) = \sum_{k=o}^{n} a_k p_k(x)$, então $r_n(0) = 0 = \sum_{k=o}^{n} a_k p_k(0) = a_o$, do que decorre

$$s_n(x) = F\, r_n(x) = \sum_{k=1}^{n} a_k q_k(x)$$

e portanto $s_n(0) = 0$ $(n \geq 1)$. Ademais, é imediato verificar que $S(s_o(x)) = 0$ e $S(s_n(x)) = n\, s_{n-1}(x)$, se $n \geq 1$.

Em particular, se $(p_n(x))$ é uma base associada, considerando a base (x^n) associada a D e o operador umbral definido por F $p_n(x) = x^n$, então a sequencia $(s_n(x))$ definida por F $x^n = s_n(x)$ é a base associada a F D F^{-1}. Esta sequencia $(s_n(x))$ é chamada base inversa de $(p_n(x))$.

É conveniente, a esta altura, introduzir a notação umbral. Se $(a_n(x))$ é uma base associada e se M é o operador linear definido por M $x^n = a_n(x)$, dizemos que M é a representação umbral de $(a_n(x))$. A notação umbral se caracteriza pelo seguinte: se M $x^n = a_n(x)$, faz-se $a_n(x) = [\underline{a}(x)]^n$ e portanto M $x^n = [\underline{a}(x)]^n$. Por exemplo, a identidade binomial que caracteriza uma base binomial $(p_n(x))$, com a notação umbral fica

$$\underline{p}^n(x+y) = [\underline{p}(x) + \underline{p}(y)]^n$$

No caso já considerado da base inversa de uma base associada $(p_n(x))$, supondo $p_n(x) = \sum_{i=o}^{n} a_i x^i$, então

$$x^n = F\ p_n(x) = \Sigma\ a_i\ F(x^i) = \Sigma\ a_i q_i(x) = p_n(\underline{q}(x))$$

5.3. Relação entre Funcionais D-delta Recíprocos.

Sejam $(p_n(x))$ e $(q_n(x))$ as bases associadas aos funcionais D-delta g e f, respectivamente. Indiquemos por A_g e A_f, pela ordem, as representações umbrais de $(p_n(x))$ e $(q_n(x))$. Como a composta $A_f A_g$ é umbral, se $(A_f A_g)(x^n) = r_n(x)$, então $(r_n(x))$ é associada a um certo funcional D-delta que será indicado por f o g. Como ainda: $(A_f A_g)(x^n) = A_f(p_n(x)) = p_n(\underline{q}(x))$, então $(p_n(\underline{q}(x))$ é binomial (associada a f o g).

Apenas registremos que para os adjuntos de A_f e A_g, quaisquer que sejam f e g funcionais D-delta, vale a identidade : $A_g^* A_f^* = A_{f\,o\,g}^*$.

Proposição 16. Para que dois funcionais f e g se

jam recíprocos é necessário e suficiente que $f \circ g = w$.

Demonstração.

($\rightarrow$) Supondo $(p_n(x))$ a base associada a f e $(q_n(x))$ aquela associada a g, então

$$p_n(x) = \sum_{k=o}^{n} \frac{g^k(x^n)}{k!} x^k$$

Daí, supondo $q_n(x) = c_1 x + \ldots + c_n x^n$:

$$q_n(\underline{p}(x)) = c_1 p_1(x) + \ldots + c_n p_n(x) = \sum_{i=1}^{n} \frac{g^i(q_n(x))}{i!} x^i = x^n$$

o que mostra que o funcional associado a (x^n) é $f \circ g$ e portanto $f \circ g = w$.

($\leftarrow$) Mantidas as notações anteriores

$$\sum_{i=1}^{n} c_i p_i(x) = x^n$$

Daí

$$\sum_{i=1}^{n} c_i f^k(p_i(x)) = f^k(x^n)$$

do que decorre: $c_k\, k! = f^k(x^n)$. Donde

$$q_n(x) = \Sigma\, c_k x^k = \Sigma\, \frac{f^k(x^n)}{k!} x^k$$

e portanto $q_n(x)$ é a base conjugada de f.

Consideremos agora f e g funcionais recíprocos. É imediato que $A_w = I$ (operador idêntico). Como $A_f A_g = A_{f \circ g}$, então $A_f A_g = I$. Disto decorre então que

$$A_{\tilde{f}} = A_g = A_f^{-1}$$

Lembremos que se $F(t) = \sum_{k \geq 1} a_k t^k$ e $G(t) = \sum_{k \geq 1} b_k t^k$ são séries formais sobre K, com $a_1 \neq 0$ e $b_1 \neq 0$, definindo-se a composta

$$H(t) = F(G(t)) = (F \circ G)(t) = \Sigma\, a_k (G(t))^k$$

se $H(t) = \sum_{k\geq 1} c_k t^k$, então

$$c_k = \sum_{j=1}^{n} a_j \left(\sum_{k_1+\ldots+k_j=n} b_{k_1} b_{k_2} \ldots b_{k_j} \right)$$

e fica estabelecida sobre o conjunto das séries formais nessas condições uma estrutura de grupo cujo elemento neutro é a série formal $E(t) = t$.

Proposição 17. Se f e g são funcionais D-delta cujas indicadoras são F(t) e G(t) respectivamente, então G(F(t)) é a indicadora de f o g.

Demonstração. É uma questão apenas de cálculos verificar que $A_f^*(F(w)) = w$, $A_g^*(G(w)) = w$ e $A_{f\,o\,g}^*(f\,o\,g) = w$. Daí

$$f\,o\,g = (A_{f\,o\,g}^*)^{-1}(w) = (A_g^* A_f^*)^{-1}(w) = (A_f^*)^{-1}(A_g^*)^{-1}(w) = (A_f^*)^{-1}(G(w)) =$$

$$= G(A_f^*)^{-1}(w) = G(F(w))$$

o que garante que G(F(t)) é a indicadora de f o g.

Corolário. Dois funcionais D-delta são recíprocos se, e somente se, suas indicadoras são elementos inversos, uma da outra, no grupo das séries formais sobre K, com coeficiente inicial nulo e coeficiente de t não nulo.

5.4. A Derivada de Pincherle e a Fórmula de Rodrigues.

Seja f um funcional linear sobre $U = K[x]$. A derivada de f é o funcional linear $f' \in U^*$ definido por $f'(x^n) = f(x^{n+1})$. Se indicarmos por X o operador linear de U definido por $X\,p(x) = x\,p(x)$, para todo $p(x) \in U$, então $f' = f\,X$ (composição). É fácil mostrar que $f \mapsto f'$ é uma derivação em U^*.

Para todo operador linear T em U, damos o nome de derivada de Pincherle de T ao operador linear $T' = TX - X\,T$. Cálculos simples permitem verificar que se $Q = T(f)$, então $Q' = T(f')$ e que se a indicadora de $Q = T(f)$ é F(t), então F'(t) é a indicadora de $Q' = T(f')$.

Notemos que se h é um funcional D-delta, então T(h') é inversível. De fato, para $n \geq 0$:

$$T(h')(x^n) = \sum_{k=0}^{n} \binom{n}{k} h'(x^{n-k}) x^k = \sum_{k=0}^{n} \binom{n}{k} h(x^{n-k+1}) x^k$$

onde o coeficiente de x^n na última soma é $h(x) \neq 0$. Logo T(h') transforma (x^n) numa outra base de U e portanto T(h') é inversível.

Proposição 18. (Fórmula de Rodrigues). Seja h um funcional D-delta e indiquemos por $(p_n(x))$ a base associada a $Q = T(h)$. Então

$$x\, Q'^{-1}(p_n(x)) = p_{n+1}(x) \qquad (n = 0,1,2,\ldots)$$

Demonstração. Em virtude da unicidade da base associada a h basta provar que

$$h^r(x\, Q'^{-1}(p_n(x))) = (n+1)!\ \delta_{n+1,r}$$

Para r = 0 esse resultado é verdadeiro pois $h^0 = u$ e como o termo constante de $x\, Q'^{-1}(p_n(x))$ é nulo, então

$$h^0(x\, Q'^{-1}(p_n(x))) = u(x\, Q'^{-1}(p_n(x))) = 0 = (n+1)!\ \delta_{n+1,0}$$

Admitindo-se o resultado verdadeiro para $r \geq 0$ e considerando que $(h^{r+1})' = (r+1)h^r\, h'$, então

$$h^{r+1}(x\, Q'^{-1} p_n(x)) = (h^{r+1})'\, Q'^{-1} p_n(x) = ((r+1)h^r h') Q'^{-1} p_n(x) =$$

$$= ((r+1)h^r)(T(h')Q'^{-1}) p_n(x) = (r+1)h^r\, p_n(x) = (r+1)r!\ \delta_{nr} =$$

$$= (r+1)!\ \delta_{n+1,r+1}$$

5.5. Algumas Bases Associadas.

(I) A base associada ao funcional D-delta w é, como já vimos, (x^n). Mas, do fato de que $T(w) = D$, segue que (x^n) também é a base associada a D. Obviamente a indicadora de w é a sé

rie t. A expressão de ε_y em termos das potências de w é

$$\varepsilon_y = \Sigma \frac{\varepsilon_y(x^k)}{k!} w^k = \Sigma \frac{y^k}{k!} w^k$$

(II) Se $\varepsilon = \varepsilon_o = u$, então a base associada ao funcional $\varepsilon_1 - \varepsilon$ é $((x)_n)$, onde $(x)_o = 1$ e $(x)_n = x(x-1) \ldots$ $\ldots (x-n+1)$ se $n \geq 1$.

Como

$$T(\varepsilon_a)x^n = \sum_{k=o}^{n} \binom{n}{k} \varepsilon_a(x^{n-k}) x^k = \sum_{k=o}^{n} \binom{n}{k} a^{n-k} x^k = (x+a)^n = E^a x^n$$

então $T(\varepsilon_a) = E^a$. De modo análogo se mostra que $T(\varepsilon) = I$ (identidade no conjunto dos operadores em U). Assim, $T(\varepsilon_a - \varepsilon) = E^a - I$. Em particular $T(\varepsilon_1 - \varepsilon) = E^1 - I = E - I$ em se fazendo, como é praxe, $E^1 = E$.

Observando que

$$(E - I)(1) = 1 - 1 = 0$$

e, para $n > 0$

$$(E - I)(x)_n = E(x)_n - (x)_n =$$

$$= (x+1)x \ldots (x-n+3)(x-n+2) - x(x-1) \ldots (x-n+2)(x-n+1) =$$

$$= x(x-1) \ldots (x-n+2)(x+1 - x+n-1) = n(x)_{n-1}$$

fica provado que $((x)_n)$ é a base associada a $E - I$ e portanto a $\varepsilon_1 - \varepsilon$.

Como $(\varepsilon_1 - \varepsilon)(1) = 0$ e $(\varepsilon_1 - \varepsilon)(x^n) = 1$ se $n \geq 1$, então a indicadora de $\varepsilon_1 - \varepsilon$ é

$$F(t) = \sum_{n=1}^{n} \frac{1}{n!} t^n = e^t - 1$$

A expressão de ε_y em termos de $\varepsilon_1 - \varepsilon$ é

$$\varepsilon_y = \Sigma \frac{(y)_k}{k!} (\varepsilon_1 - \varepsilon)^k$$

Como

$$(\varepsilon_1 - \varepsilon)^k = \sum_{i=o}^{k} \binom{k}{i} \varepsilon_1^i (-1)^{k-i}$$

uma vez que ε é o elemento neutro da multiplicação em U*, então

$$\varepsilon_y = \sum_{k=o}^{\infty} \sum_{i=o}^{k} \frac{(-1)^{k-i}}{k!} \binom{k}{i} (y)_k \, \varepsilon_1^i$$

(III) A base associada ao funcional $\varepsilon - \varepsilon_{-1}$ ou, equivalentemente, ao operador $I - E^{-1}$ é $((x)^n)$, onde $(x)^o = 1$ e $(x)^n = x(x+1)\ldots(x+n-1)$, se $n \geq 1$. A indicadora desse funcional é obviamente $1 - e^{-t}$.

(IV) Para todo inteiro $h \geq 1$ a base associada a $\frac{E^h - I}{h}$ é $((x)_{(n;h)})$, onde $(x)_{(o;h)} = 1$ e

$$(x)_{(n;h)} = x(x-h)(x-2h) \ldots (x-(n-1)h)$$

De fato, a generalização dos cálculos do exemplo (II) leva a

$$(E^h - I)(x)_{(n;h)} = nh(x)_{(n-1;h)}$$

Como a indicadora de $\frac{E^h - I}{h}$ é

$$F(t) = t + \frac{h}{2!} t^2 + \frac{h^2}{3!} t^3 + \ldots$$

a notação para esse operador será, por razões obvias:

$$\frac{e^{hD} - I}{h}$$

Calculemos o operador linear Q cuja base associada é a base inversa de $((x)_{(x;h)})$. Com as notações do item 5.2, se T é o operador inversível definido por $T((x)_{(n;h)}) = x^n$, a sequencia $s_n(x) = T(x^n)$ é a base inversa de $((x)_{(n;h)})$. Considerando que

$$Q = \sum \frac{a_k}{k!} D^k \quad , \quad a_k = [Q\, x^k]_{x=o}$$

calculemos $Q\, x^n$. Procedendo de maneira usual chega-se a que

$$D(x)_{(n;h)} = \sum_{i=o}^{n-1} (-h)^{n-i-1} \cdot \frac{n!}{i!(n-i)} \cdot (x)_{(i;h)}$$

e então

$$Q\ x^n = (T\ D\ T^{-1})x^n = (T\ D)(x)_{(n;h)} = T \sum_{i=o}^{n-1} (-h)^{n-i-1} \cdot \frac{n!}{i!(n-i)} (x)_{(i;h)} =$$

$$= \sum_{i=o}^{n-1} (-h)^{n-i-1} \cdot \frac{n!}{i!(n-i)} \cdot x^i = (-h)^{n-1} \cdot \frac{n!}{o!n} + \ldots$$

Donde:

$$a_n = (-h)^{n-1} \cdot \frac{n!}{n}$$

e portanto

$$Q = D - \frac{1}{2} h\ D^2 + \frac{1}{3} h^2\ D^3 - \ldots$$

cuja notação não poderia ser senão

$$Q = \frac{1}{h} \ln (I + h\ D)$$

Os polinomios $s_n(x)$ da base inversa recebem, neste caso, o nome de polinômios exponenciais passo h. Completaremos este exemplo estabelecendo a seguinte fórmula:

$$s_{n+1}(x) = x(\underline{s}(x) + h)^n$$

Da fórmula obtida para Q decorre que

$$Q' = I - h\ D + h^2\ D^2 - h^3\ D^3 + \ldots = (I + h\ D)^{-1}$$

Pela fórmula de Rodrigues obtem-se então que:

$$s_n(x) = x\ (Q')^{-1} s_{n-1}(x) = x\ (I+h\ D) s_{n-1}(x) = x\ s_{n-1}(x) + h\ x\ \dot{s}'_{n-1}(x)$$

ou seja

$$s_n(x) = x\ s_{n-1}(x) + h\ x\ s'_{n-1}(x)$$

que é uma recorrente para os polinômios exponenciais passo h.

Como

$$T\ x(x-h)_{(n-1;h)} = x \cdot x^{n-1}$$

mudando n-1 por n:

$$T\ x(x-h)_{(n;h)} = x \cdot x^n = x\ T(x)_{(n;h)}$$

que pode ser reescrita assim:

$$T\ x\ E^{-h}(x)_{(n;h)} = x\ T\ (x)_{(n;h)}$$

Por linearidade, substituindo $(x)_{(n;h)}$ por $p(x+h)$, onde $p(x) \varepsilon K[x]$:

$$T \; x \; E^{-h} \; p(x+h) = x \; T \; p(x+h)$$

Ou seja

$$T \; x \; p(x) = x \; T \; p(x+h)$$

Como

$$T(p(x+h)) = p \; (T(x+h)^{i}) = p \; (h + \underline{s}(x))$$

e,por outro lado

$$T(x \; p(x)) = \underline{s}(x) \; p(\underline{s}(x))$$

então

$$\underline{s}(x) \; p(\underline{s}(x)) = x \; p(\underline{s}(x)+h)$$

Se fizermos $p(x) = x^n$, obteremos a fórmula enunciada:

$$s_{n+1}(x) = \left[\underline{s}(x)\right]^{n+1} = x\left[\underline{s}(x)+h\right]^{n}$$

(IV) Já vimos que a base associada ao operador $Q = E^{a}D$ é formada pelos polinômios de Abel $a_n(x)$, onde $a_o(x)=1$ e $a_n(x) = x(x-na)^{n-1}$ $(n \geqslant 1)$. Como $T(\varepsilon_a w) = T(\varepsilon_a)T(w) = E^{a}D$, então $(a_n(x))$ é a base associada a $\varepsilon_a w$. Observando que $(\varepsilon_a w)x^n = n\, a^{n-1}$, podemos garantir que a indicadora de $\varepsilon_a w$ é

$$\Sigma \; \frac{a^{n-1}}{(n-1)!} t^{n}$$

(V) Os polinomios de Gould.

$$G_n(x,a,b) = \frac{x}{x-an} \left(\frac{x-an}{b} \right)_n$$

formam a base associada ao funcional $\varepsilon_a(\varepsilon_b - \varepsilon)$. Como, para todo $y \varepsilon K$, a indicadora de ε_y é e^{yt}, então a indicadora de $\varepsilon_a(\varepsilon_b-\varepsilon)$ é

$$e^{at}(e^{bt} - 1)$$

5.6. Algumas Sequencias Conjugadas.

(I) Como já vimos a base (x^n) é auto-recíproca o que significa que a base conjugada de w é (x^n).

(II) Indicando por $S\left[n,k\right]$ os coeficientes de Stirling de segunda espécie

$$x^n = \sum_{k=o}^{n} S[n,k](x)_k$$

observando que $((x)_k)$ é a base associada a ε_1-ε, então

$$(\varepsilon_1 - \varepsilon)^p x^n = \sum_{k=o}^{n} S[n,k]k!\ \delta_{kp} = S[n,p]p!$$

Logo a sequencia $(q_n(x))$ conjugada de $\varepsilon_1 - \varepsilon$ é dada por

$$q_n(x) = \sum_{k=o}^{n} S[n,k]x^k$$

(III) A sequencia conjugada de $\varepsilon - \varepsilon_{-1}$ é dada por

$$q_n(x) = \sum_{k=o}^{n} (-1)^{n-k} S[n,k]x^k$$

(IV) Vejamos a sequencia conjugada do funcional de Abel $\varepsilon_a w$. Como

$$(\varepsilon_a w)x^n = \left[(E^a D)x^n\right]_{x=o} = \left[n(x+a)^{n-1}\right]_{x=o} = n\ a^{n-1}$$

por indução se obtem que

$$\left[(E^a D)^k\ x^n\right]_{x=o} = (n)_k (k\ a)^{n-k}$$

Indicando por $(q_n(x))$ a sequencia procurada:

$$q_n(x) = \sum_{k=o}^{n} \frac{(n)_k\ (k\ a)^{n-k}}{k!}\ x^k = \sum_{k=o}^{n} \binom{n}{k} (k\ a)^{n-k}\ x^k$$

(V) Determinemos agora a sequencia conjugada do funcional $\varepsilon_a(\varepsilon_b - \varepsilon)$. Notemos para tanto que como E^a e E^b-I comutam entre si, então $\left[E^a(E^b-I)\right]^r = E^{ar}(E^b-I)^r$.

Como já citamos (ex IV - 5.4)

$$(E^b-I)(x)_{(i;b)} = i.b.(x)_{(i-1;b)}$$

e, por indução:

$$(E^b-I)^r(x)_{(i;b)} = (i)_r.b^r.(x)_{(i-r;b)}$$

Como

$$x^n = \sum_{i=o}^{n} S_b[n;i](x)_{(i;b)}$$

onde $S_b[n;i]$ indica os números de Stirling de segunda espécie, passo b, então

$$\left[E^a(E^b-I)\right]^r x^n\Big|_{x=o} = \sum_{i=o}^{n} S_b[n;i].(i)_r.b^r.(r.a)_{(i-r;b)}$$

Logo

$$\frac{\left[E^a(E^b-I)\right]^r x^n\Big|_{x=o}}{r!} = \sum_{i=o}^{n} \binom{i}{r} S_b[n;i].b^r.(ra)_{(i-r;b)}$$

Assim a sequencia conjugada de $\varepsilon_a(\varepsilon_b - \varepsilon)$ é dada por

$$q_n(x) = \sum_{r=o}^{n} \left[\sum_{i=o}^{n} \binom{i}{r} b^r.(ra)_{(i-r;b)} \cdot S_b[n;i] \right] x^r$$

Quanto aos coeficientes de Stirling de segunda ordem, passo h, é válida a seguinte fórmula, generalização de uma bem conhecida no caso h = 1:

$$S_h[n+1;j] = \sum_{k=o}^{n} \binom{n}{k} h^{n-k} S_h[k;j-1]$$

6. Aplicações.

Definimos um depósito σ como sendo um par ordenado $\sigma = (D,d)$, onde D é um conjunto não vazio e $d: D \to N$ uma aplicação tal que, para todo $n \in N$, o conjunto $d^{-1}(\{n\})$ é finito. Para cada $n \in N$, o cardinal de $d^{-1}(\{n\})$ será indicado por a_n. Em geral o conjunto D está dotado de alguma estrutura e o que se pretende é determinar a_n, para cada $n \in N$. Se $x \in D$ a imagem d(x) é chamada grau de x. Chamaremos (a_n) de sequencia contadora de σ e suporemos sempre $a_1 > 0$.

O funcional gerador de σ é, por definição, o funcional D-delta h definido por

$$h(x^n) = a_n$$

Fica subentendido então que $h(1) = 0$.

Vejamos agora o conceito de particional de um depósito σ. Adotando a notação $part(\sigma)$ para esse particional, um elemento $p \in part(\sigma)$ se caracteriza pelo seguinte

(i) $p = \{(B_1,s_1); (B_2,s_2);...; (B_k;s_k)\}$ onde os B_i são os blocos de uma partição de $\{1,2,..., n\}$, para um certo n, e portanto cada $B_i \neq \emptyset$;

(ii) os elementos s_i pertencem a D;

(iii) $d(s_i) = |B_i|$

A cada $p \in part(\sigma)$ associaremos dois inteiros: o grau de p definido por

$$d(p) = d(s_1)+...+ d(s_k)$$

e o número particional de p que é exatamente o número k de blocos de p.

Se indicarmos por $b_{n,k}$ o número de elementos de $part(\sigma)$ de grau n e número particional k, então $(b_{n,k})$ é chamada sequencia contadora de part (σ). Definiremos $b_{o,o} = 1$. Como $a_1>0$, podemos provar que $b_{n,n} > 0$, para todo n. Como $a_1 > 0$, existe um elemento $s \in D$ de grau 1. Portanto

$$\{(\{1\}, s); (\{2\}, s);...; (\{n\}, s)\}$$

é um elemento de $part(\sigma)$ de grau n e número particional n o que garante que $b_{nn} \geq 1$.

Proposição 19. Seja σ um depósito cujo funcional gerador é h. Se $(b_{n,k})$ é a sequencia contadora de $part(\sigma)$, então

$$b_{n,k} = \frac{h^k(x^n)}{k!}$$

Demonstração. Vamos admitir que a sequencia $(b_{n,k})$ satisfaça a identidade

$$\binom{i+j}{i} . b_{n,i+j} = \sum_{k=o}^{n} \binom{n}{k} . b_{k,i} . b_{n-k,j}$$

Então a base $(p_n(x))$ de $K[x]$ sobre K definida por $p_n(x) = \sum_{k=o}^{n} b_{nk} x^k$ $(n>0)$ é admissível (prop. 13) e portanto é a base conjugada de um certo funcional D-delta f para o qual se verifica (prop. 14):

$$b_{nk} = \frac{f^k(x^n)}{k!} \qquad (1)$$

Como porém b_{n1} é o número de elementos $\{B,s)\} \in part(\sigma)$, onde necessariamente $B = \{1,2,\ldots,n\}$, então esse número coincide com o de elementos $s \in D$ tais que $d(s) = n$. Ora, mas este número é a_n e portanto $b_{n1} = a_n = h(x^n)$. Como então h coincide com f na base (x^n), pois de (1) decorre que $b_{n1} = f(x^n)$, então $f = h$.

Seja agora X um k-subconjunto de $X_n (0 \leqslant k \leqslant n)$ e construamos os b_{ki} elementos $\{(B'_1,s'_1);\ldots;(B'_i,s'_i)\}$, onde $\{B'_1,\ldots,B'_i\}$ é uma partição de X e $s'_1,\ldots,s'_i \in D$ são tais que $d(s'_p)=|B'_p|$ $(1 \leqslant p \leqslant i)$. Para o complementar X^c, em X_n, de cada X, construamos igualmente os $b_{n-k,j}$ elementos $\{(B''_1,s''_1);\ldots;(B''_j,s''_j)\}$ em que $\{B''_1,\ldots,B''_j\}$ é uma partição de X^c, os $s''_p \in D$ e $d(s''_p)=|B''_p|$ $(1 \leqslant p \leqslant j)$. Isto posto, o número

$$\sum_{k=o}^{n} \binom{n}{k} . b_{ki} . b_{n-k,j}$$

representa a quantidade de pares ordenados que se podem formar com os elementos assim construidos, fazendo X percorrer a coleção de todos os subconjuntos de X_n. Observemos ainda que cada união

$$\{(B'_1,s'_1);\ldots;(B'_i,s'_i)\} \cup \{(B''_1,s''_1);\ldots;(B''_j,s''_j)\}$$

é um membro de part(σ), de grau n e número particional i+j; vice-versa, cada membro de part(σ) nessas condições, é uma união desse tipo. Como com cada um destes membros de part(σ) podemos formar exatamente $\binom{i+j}{i}$ dos pares considerados, então

$$\binom{i+j}{i} . b_{n,i+j} = \sum_{k=o}^{n} \binom{n}{k} . b_{ki} . b_{n-k,j}$$

Corolário 1. A sequencia conjugada do funcional h, gerador de σ, é

$$\sum_{k=o}^{n} b_{n,k}\, x^k$$

Corolário 2. Se c_n indica o número de elementos de grau n em part(σ), então $c_n = e^h(x^n)$ e a indicadora de e^h é a função geradora exponencial de (c_n).

Demonstração. De fato

$$e^h(x^n) = (u + h + \frac{h^2}{2!} + \frac{h^3}{3!} + \dots)(x^n) =$$

$$= b_{no} + b_{n1} + \dots + b_{nn} = c_n$$

Como a indicadora de e^h é

$$\sum \frac{e^h(x^n)}{n!}\, t^n = \sum \frac{c_n}{n!}\, t^n$$

fica completada a demonstração.

Exemplo 1.

Calculemos o número de partições de {1,2,...,n}, em k blocos, com um elemento etiquetado em cada bloco. Por exemplo, se n = 4 e k = 2, então {{1,2}; {3,4}} e {{1,2}; {3,4}} são partições consideradas diferentes de {1,2,3,4}.

Seja σ o depósito cujos elementos de grau n são exatamente os n-conjuntos {1,2,..., n}, {1,2,..., n},..., {1,2,...,n}. Se (b_{nk}) é a sequencia contadora de part(σ), então obviamente o número procurado é b_{nk}. Indicando por h o funcional gerador de σ, como $h(x^n) = n$, então $h = w\varepsilon_1$. Levando em conta então o exemplo (IV), item 5.6:

$$b_{nk} = \binom{n}{k}\, k^{n-k}$$

Observemos que cada partição $\{B_1, B_2, \dots, B_k\}$ de X_n dá origem a $|B_1||B_2| \dots |B_k|$ partições com um elemento etiquetado em cada bloco. Daí

$$\Sigma\ |B_1||B_2|\ \ldots\ |B_k| = \binom{n}{k}\ k^{n-k}$$

onde a somatória do primeiro membro é estendida a todas as partições $\{B_1, B_2, \ldots, B_r\}$, com k blocos, de um n-conjunto.

É fácil ver que $\binom{n}{k}k^{n-k}$ conta também o número de florestas etiquetadas, com raiz, de n vértices, onde cada vértice, exceto a raiz, é de grau 1, com k árvores.

E a função geradora exponencial do número c_n de partições, com um elemento etiquetado em cada bloco, de um n-conjunto, é $\exp(w\varepsilon_1)$. Deve-se observar a propósito que a indicadora de w é t e a de ε_1 é $\exp(t)$.

Exemplo 2.

Determinemos agora o número de partições com blocos k-etiquetados de um n-conjunto. Este problema já foi resolvido por Barbosa, R.M., através de um enfoque mais específico. Em (1) está tratado o caso k = 2.

Seja σ o depósito cujos elementos de grau n são $\{1,2,\ldots,n\}_1$, $\{1,2,\ldots,n\}_2$, ... , $\{1,2,\ldots,n\}_k$, onde os índices representam as etiquetas possíveis. Se h é o funcional gerador de σ, então $h(x^n) = k$ e portanto $h = k(\varepsilon_1 - u)$.

Examinemos um elemento $p = \{(B_1,s_1);\ldots;(B_r,s_r)\}$ de part(σ) . Se $|B_i| = n_i$, então $d(s_i) = n_i$ e portanto s_i é um dos k conjuntos etiquetados: $\{1,2,\ldots, n_i\}_1$, ... , $\{1,2,\ldots, n_i\}_k$. Como $\{B_1,\ldots, B_r\}$ é uma partição genérica de X_n, se (b_{nr}) é a sequencia contadora de σ, então o número de partições com r blocos, k-etiquetados, de um n-conjunto, é dado por b_{nr}.

Como

$$x^n = \sum_{r=1}^{n} S[n,r](x)_r$$

e $((x)_r)$ é associada a $\varepsilon_1 - \varepsilon$, então

$$(k(\varepsilon_1-\varepsilon))^p\, x^n = \sum_{r=1}^{n} S[n,r]k^p\, r!\delta_{rp} = k^p\, S[n,p]p!$$

Logo a sequencia conjugada de $k(\varepsilon_1-\varepsilon)$ é:

$$q_n(x) = \sum_{r=o}^{n} k^r\, S[n,r]x^r$$

Donde

$$b_{nr} = k^r\, S[n,r]$$

e o número de partições de um n-conjunto, com blocos k-etiquetados, é

$$\sum_{r=1}^{n} k^r\, S[n,r]$$

Em particular se $k = 1$ a somatória $\sum_{r=1}^{n} S[n,r]$ é o número de partições de um n-conjunto e $S[n,r]$ o número de partições, em r blocos, de um n conjunto. Ainda neste último caso, a função geradora exponencial do número de partições de um n-conjunto é $\exp(\varepsilon_1-\varepsilon)$. Como a indicadora de u é 1 e a de ε_1 é $\exp(t)$, então é obvia a notação

$$e^{e^t-1}$$

para $\exp(\varepsilon_1-\varepsilon)$. Os números $B_n = e^h(x^n)$ são conhecidos na literatura como números de Bell ($h = \varepsilon_1-\varepsilon$).

Exemplo 3.

Uma partição de um n-conjunto com subconjuntos selecionados e um elemento permanente é um conjunto

$$\{(B_1;(B_1,C_1));\ldots;\ (B_r;\ (B_r,C_r))\}$$

onde $\{B_1,\ldots,\ B_r\}$ é uma partição desse n-conjunto, cada C_i é subconjunto de B_i e cada C_i contem um determinado e fixado elemento. Vejamos como determinar o número dessas partições com um certo número r de blocos.

Seja σ o depósito cujos elementos de grau n são

os pares ({1,2,..., n}; C}, onde C é subconjunto de X_n e C contem um determinado elemento deste conjunto. Ou seja, todos os C nessas condições contêm o mesmo elemento de {1,2,..., n}. Se p ε part(σ), um elemento genérico de p é um par $(B_i; (\{1,2,..., n_i\}; C_i))$, onde $|B_i| = n_i$ e $C_i \subset \{1,2,..., n_i\}$ deve conter um fixado elemento t, $1 \leq t \leq n_i$. É claro então que se (b_{nr}) é a sequencia contadora de part(σ), então b_{nr} expressa exatamente o número de partições procuradas.

Como o número de elementos de grau n em D é 2^{n-1} (σ = (D,d)), então o funcional gerador deste depósito é

$$h = \frac{\varepsilon_2 - \varepsilon}{2}$$

Consequentemente, considerando que

$$x^n = \sum_{r=1}^{n} S_2[n,r](x)_{(r;2)}$$

então, levando em conta o exemplo (IV), 5.5:

$$h^p(x^n) = S_2[n,p].p!$$

Logo a sequencia conjugada de h é

$$q_n(x) = \sum_{p=o}^{n} S_2[n,p]x^p$$

e

$$b_{nr} = S_2[n,r].$$

Exemplo 4.

Vejamos agora que coeficientes c_{nk} de uma base conjugada expressa como combinação linear da base canônica (x^n), dá o número de elementos do grupo simétrico S_n formado exatamente de k ciclos.

Seja σ o depósito cujos elementos de grau n são os elementos de S_n formados de um único ciclo. Então o funcional gerador de σ é dado por $h(x^n) = (n-1)!$ e obviamente os coeficien

tes c_{nk} desejados são precisamente os termos da sequencia contadora de part(σ).

Se $(q_n(x))$ é a base conjugada de h, então $q_n(x) = \sum_{k=1}^{n} c_{nk}\, x^k$ $(n \geq 1)$, onde $c_{n1} = h(x^n) = (n-1)!$. Observemos porem que como $((x)^n)$ é binomial, então é a base conjugada de algum funcional g. Assim

$$(x)^n = \sum_{k=1}^{n} d_{nk}\, x^k \quad (n \geq 1)$$

onde, por identidade de polinômios se tem $d_{n1} = (n-1)!$, ou seja $g(x^n) = (n-1)! = h(x^n)$. Mas, conforme já observamos ao definir base conjugada, podemos concluir então que $d_{nk} = c_{nk}$ e portanto os coeficientes procurados são dados por

$$(x)^n = \Sigma\, c_{nk}\, x^k$$

Exemplo 5.

Contemos agora o número de florestas etiquetadas, com raiz, de n vértices. (Cayley)

Seja σ o depósito cujos elementos de grau n são as árvores etiquetadas, com raiz, de n vértices. Então part(σ) é o conjunto das florestas com as especificações exigidas. Se (b_{nk}) é a sequencia contadora de part(σ), então b_{nk} indica o número de florestas de n vértices e k árvores, do tipo que estamos contando. Em particular cada b_{n1} é o número de árvores de grau n. E se de cada uma destas árvores retiramos a raiz obtemos n vezes o número de florestas, do mesmo tipo, porém de grau n-1, em virtude de cada n "desenraizamentos" produzirem a mesma floresta. Assim

$$b_{n1} = n\, \Sigma\, b_{n-1,k}$$

Se h é o funcional gerador de σ, a igualdade acima se converte em

$$h(x^n) = n \sum \frac{h^k(x^{n-1})}{k!}$$

Mas pela fórmula da transferência

$$nh^k(x^{n-1}) = h^k(T(w)x^n) = (h^k\ w)(x^n)$$

Logo

$$h(x^n) = \sum \frac{(wh^k)(x^n)}{k!} = (w\ e^h)(x^n)$$

e portanto $h = w\ e^h$. Disto segue que $w = h\ e^{-h} = F(h)$ e então $h = F^{-1}(w)$. Pelo corolário da proposição 17 concluimos que $\tilde{h} = F(w) = w\ e^{-w} = w\ \varepsilon_{-1}$ cuja base associada é $(a_n(x))$, onde $a_n(x) = x(x+n)^{n-1}$ são os polinomios de Abel no caso a = -1. Como a base associada de $\tilde{h}$ é a conjugada de h, então

$$x(x+n)^{n-1} = \sum_{k=1}^{n} b_{nk}\ x^k \quad (n \geq 1)$$

Por identidade de polinomios

$$x(x+n)^{n-1} = x \sum_{k=o}^{n-1} \binom{n-1}{k} n^{n-1-k}.\ x^k = \sum_{k=o}^{n-1} \binom{n-1}{k}.\ n^{n-1-k}.\ x^{k+1} =$$

$$= \sum_{k=1}^{n} \binom{n-1}{k-1}.\ n^{n-k}.\ x^k = \sum_{k=1}^{n} b_{nk}\ x^k$$

obtemos

$$b_{nk} = \binom{n-1}{k-1} n^{n-k}$$

Daí segue em particular que o número de árvores etiquetadas com raiz, de grau n, é $b_{n1} = n^{n-1}$.

CAPÍTULO II.

AS ÁLGEBRAS DE INCIDÊNCIA E A FUNÇÃO DE MÖBIUS.

1. Álgebras de Incidência.

Seja P um conjunto parcialmente ordenado pela relação $\leq$. Para cada par de elementos $a, b \in P$, $a \leq b$, admitiremos que o intervalo $[a,b] = \{x \in P \mid a \leq x \leq b\}$ seja finito, isto é, admitiremos que P, no que diz respeito à relação considerada, seja localmente finito.

Seja

$$A(P) = \{f: P \times P \to C \mid f(x,y) = 0 \text{ se } x \not\leq y\}$$

Definindo-se a adição em A(P) e a multiplicação de elementos de A(P) por elementos de C da maneira usual e, ainda, o produto $f * g$ de duas funções quaisquer $f,g \in A(P)$, através da convolução:

$$(f*g)(x,y) = \sum_{x \leq z \leq y} f(x,z)g(z,y)$$

obtem-se sobre A(P) uma estrutura de álgebra associativa, com unidade e não comutativa, em geral. A unidade é a função $\delta: P \times P \to C$ definida por $\delta(x,y) = 1$ se $x = y$ e $\delta(x,y) = 0$ se $x \neq y$. Esta álgebra é chamada álgebra de incidência sobre P.

Proposição 1. Um elemento $f \in A(P)$ é inversível (simetrizável em relação a *) se, e somente se, $f(x,x) \neq 0$, para todo $x \in P$.

Demonstração. Seja $f \in A(P)$ tal que $f(x,x) \neq 0$, $\forall x \in P$. A inversa g de f, cuja existência pretendemos mostrar, deve estar definida de maneira que

$$g(x,y) = 0 \text{ se } x \not\leq y \text{ e } g(x,x) = [f(x,x)]^{-1}, \forall x \in P$$

Admitindo-se g definida para todo par (x,z), $x \leq z < y$, mostremos que

$$g(x,y) = - \sum_{x \leq z < y} g(x,z)f(z,y)[f(y,y)]^{-1}$$

De fato

$$(g*f)(x,y) = \sum_{x\leq z<y} g(x,z)f(z,y) + g(x,y)f(y,y) =$$

$$= \sum_{x\leq z<y} g(x,z)f(z,y) - \sum_{x\leq z<y} g(x,z)f(z,y) = 0$$

Donde $g*f = \delta$. Analogamente se prova que $f*g = \delta$.

A recíproca é imediata.

2. A Função de Möbius.

Definição 1. A função $\zeta: P \times P \to C$ definida por $\zeta(x,y) = 1$ se $x \leq y$ e $\zeta(x,y) = 0$ se $x \not\leq y$ certamente está em $= A(P)$ e, pela proposição 1, é inversível. A esta função chamamos função zeta; sua inversa, denotada por μ, recebe o nome de função de Möbius.

Da proposição citada

$$\mu(x,x) = 1 \quad e \quad \mu(x,y) = - \sum_{x\leq z<y} \mu(x,z)$$

Portanto, se y cobre x: $\mu(x,y) = - \mu(x,x) = -1$.

A função $n = \zeta - \delta$ é chamada função de incidência de A(P). É claro que $n(x,y) = 1$ se $x < y$ e $n(x,y) = 0$ se $x \not< y$.

Proposição 2. (Lema de Hall). Seja P um conjunto parcialmente ordenado com 0 e 1. Para todo k, seja c_k o número de cadeias de k elementos, entre 0 e 1. Então, se P é loc. finito:

$$\mu(0,1) = \sum_{k\geq 1} (-1)^k c_{k+1}$$

Demonstração. A definição de produto em A(P) garante que

$$n^k(0,1) = \sum_{0<y_1<\ldots<y_{k-1}<1} n(0,y_1)n(y_1,y_2)\ldots n(y_{k-1},1)$$

onde cada fator, em cada parcela, é igual a 1. Como o número de parcelas é igual ao número de cadeias de comprimento k, de 0 a 1, então $n^k(0,1) = c_{k+1}$. Por raciocínio parecido obtem-se a conclusão

seguinte: se a cadeia de maior comprimento, ligando 0 a 1, tem r elementos, então $n^s(0,1) = 0$, sempre que $s \geq r$. Como consequencia se $x,y \in P$ e $x < y$, então $n^r(x,y) = 0$ e portanto $n^r = 0$. Donde

$$\mu = \zeta^{-1} = (\delta+n)^{-1} = \delta - n + n^2 - \ldots + (-1)^{r-1} n^{r-1}$$

e daí

$$\mu(0,1) = \delta(0,1) - n(0,1) + \ldots + (-1)^{r-1} n^{r-1}(0,1) = \sum_{k \geq 1} (-1)^k c_{k+1}$$

Corolário. Seja P um conjunto parcialmente ordenado e localmente finito. Se $x, y, z, t \in P$, $x \leq y$ e $z \leq t$ e $[x,y] \simeq [z,t]$ (isomorfos), então $\mu(x,y) = \mu(z,t)$.

Demonstração. Basta notar que o número de cadeias de x a y é o mesmo que aquele de z a t e que as funções de Möbius de $[x,y]$ e $[z,t]$ são as restrições respectivas da função de Möbius de P.

Proposição 3. (Fórmula de Inversão de Möbius). Seja P um conjunto parcialmente ordenado e localmente finito. Se $f: P \to C$ é tal que $f(x) = 0$ se $p \not\leq x$, para algum $p \in P$, e se

$$g(x) = \sum_{y \leq x} f(y)$$

então

$$f(x) = \sum_{y \leq x} g(y)\mu(y,x)$$

Demonstração. A função $g: P \to C$ está bem definida visto que P é localmente finito. Isto posto:

$$\sum_{y \leq x} g(y)\mu(y,x) = \sum_{y \leq x} \Big(\sum_{z \leq y} f(z) \Big) \mu(y,x) = \sum_{y \leq x} \sum_{z} f(z)\zeta(z,y)\mu(y,x) =$$

$$= \sum_{z} f(z) \sum_{z \leq y \leq x} \zeta(z,y)\mu(y,x) = \sum_{z} f(z)\delta(z,x) = f(x)$$

Corolário 1. Seja $r: P \to C$ uma função tal que $r(x) = 0$ se $x \not\leq q$, para um certo $q \in P$. Se

$$s(x) = \sum_{x \leq y} r(y)$$

então

$$r(x) = \sum_{x \leq y} \mu(x,y)s(y)$$

Corolário 2. Se μ^* é a função de Möbius do conjunto parcialmente ordenado $(P,\geq)$, dual de $(P,\leq)$, então $\mu^*(y,x) = \mu(x,y)$, para quaisquer $x, y \in P$.

Demonstração. Mostremos primeiro que

$$\sum_{y \geq x \geq z} \mu^*(y,x) = \delta(x,z)$$

Para cada z fixado, definindo $r(y) = \delta(y,z)$, então $r(y) = 0$ se $y \not\geq z$. Considerando $s: P \to C$ dada por

$$s(t) = \sum_{y \geq t} r(y) = \sum_{z \geq y \geq t} r(y)$$

o corolário 1, usado para $(P,\geq)$, garante que

$$r(t) = \sum_{y \geq t} \mu^*(y,t)s(y)$$

Mas

$$s(y) = \sum_{t \geq y} r(t) = \sum_{t \geq y} \delta(t,z) = \delta(z,z) = 1$$

Logo

$$\delta(x,z) = r(x) = \sum_{y \geq x} \mu^*(y,x)s(y) = \sum_{y \geq x} \mu^*(y,x)$$

Agora, fazendo $\mu^*(x,y) = q(y,x)$, obtemos na álgebra de incidência sobre $(P,\leq)$:

$$\sum_{x \leq y} q(x,y) = \sum_{x \leq y \leq z} \zeta(y,z)q(x,y) = (q*\zeta)(x,z)$$

Como

$$\delta(x,z) = \sum_{y \geq x} \mu^*(y,x) = \sum_{x \leq y} q(x,y)$$

então $q*\zeta = \delta$ e $q = \mu$. Daí $\mu(x,y) = \mu^*(y,x)$, para quaisquer $x, y \in P$.

Proposição 4. Sejam P e Q conjuntos parcialmente ordenados e localmente finitos. Sobre P x Q consideremos a re

lação de ordem parcial definida por

$$(x,y) \leq (u,v) \iff x \leq u \quad e \quad y \leq v$$

em relação à qual, como é óbvio, P x Q é localmente finito. Se μ_P, μ_Q e μ_{PxQ} indicam as funções de Möbius sobre P, Q e P x Q, respectivamente, então

$$\mu_{PxQ}((x,y);\ (u,v)) = \mu_P(x,u)\mu_Q(y,v)$$

para quaisquer (x,y), (u,v) ε P x Q.

Demonstração. É claro que $\mu_{PxQ}((x,y);(x,y)) = 1 = \mu_P(x,x)\mu_Q(y,y)$. Suponhamos $(x,y) < (u,v)$ e $\mu_{PxQ}((x,y);(a,b)) = \mu_P(x,a)\mu_Q(y,b)$, sempre que $(x,y) \leq (a,b) < (u,v)$. Então

$$\mu_{PxQ}((x,y);\ (u,v)) = -\sum_{(x,y)\leq(a,b)<(u,v)} \mu_{PxQ}((x,y);(a,b)) =$$

$$= -\sum_{(x,y)\leq(a,b)<(u,v)} \mu_P(x,a)\mu_Q(y,b) = -\sum_{x\leq a<u}\ \sum_{y\leq b<v} \mu_P(x,a)\mu_Q(y,b) +$$

$$- \mu_P(x,u)\sum_{y\leq b<v} \mu_Q(y,b) - \mu_Q(y,v)\sum_{x\leq a<u} \mu_P(x,a) = -\mu_P(x,u)\mu_Q(y,v) +$$

$$+ 2\,\mu_P(x,u)\mu_Q(y,v) = \mu_P(x,u)\mu_Q(y,v).$$

A seguinte generalização é óbvia para um produto $P = P_1 \times P_2 \times \ldots \times P_n$ de conjuntos parcialmente ordenados e localmente finitos:

$$\mu_P((x_1,\ldots,x_n);\ (y_1,\ldots,y_n)) = \mu_{P_1}(x_1,y_1)\ldots\mu_{P_n}(x_n,y_n)$$

3. O Princípio de Inclusão - Exclusão.

(3.1) Seja B a coleção de todos os subconjuntos de um conjunto finito $S = \{a_1, a_2, \ldots, a_n\}$ ordenada por inclusão. Considerando em J = {0,1} a ordem usual e em J x J x...x J (n cópias) a relação de ordem focalizada no item anterior, a função que a cada $T \subset S$ associa a n-upla $(\delta_1, \delta_2, \ldots, \delta_n)$, onde $\delta_i = 1$ se $a_i \in T$ e $\delta_i = 0$ se $a_i \notin T$ é um isomorfismo de conjuntos parcialmente ordenados. Assim, se T_1 e T_2 são subconjuntos de S asso

ciados respectivamente às n-uplas $(\delta_1,\delta_2,\ldots,\delta_n)$ e $(\delta'_1,\delta'_2,\ldots,\delta'_n)$, então

$$T_1 \subset T_2 \iff \delta_i \leq \delta'_i \quad (i=1,2,\ldots,n)$$

Logo

$$\mu(T_1,T_2) = \mu((\delta_1,\ldots,\delta_n);\ (\delta'_1,\ldots,\delta'_n)) = \mu(\delta_1,\delta'_1)\ldots\mu(\delta_n,\delta'_n)$$

Mas $\mu(\delta_i,\delta'_i) = 1$ ou -1, sendo que o valor -1 ocorre quando $\delta_i = 0$ e $\delta'_i = 1$, ou seja, quando há um elemento em T_2 que não está em T_1.

Logo

$$\mu(T_1,\ T_2) = (-1)^{|T_2|-|T_1|}$$

(3.2) Mantidas as notações de (3.1) seja $f:B \to C$ uma função qualquer. Se $g: B \to C$ é definida por

$$g(X) = \sum_{Y \subset X} f(Y)$$

pela fórmula de inversão de Möbius:

$$f(X) = \sum_{Y \subset X} \mu(Y,X)\,g(Y)$$

Daí segue, levando em conta o resultado obtido no subitem anterior, que

$$f(X) = g(X) - \sum_{Y \subset X;\,|Y|=|X|-1} g(Y) + \sum_{Y \subset X;\,|Y|=|X|-2} g(Y) + \ldots$$

$$\ldots + (-1)^{|X|}\, g(\emptyset)$$

que é a fórmula que traduz genéricamente o chamado princípio de inclusão-exclusão numa de suas versões. A outra, óbvia a esta altura, corresponde ao caso

$$g(X) = \sum_{X \subset Y} f(Y)$$

Exemplo. Seja n um número natural não nulo. Se $m \in N$, $1 \leq m \leq n$, indiquemos por $P_n(m)$ o número de permutações de $X_n = \{1,2,\ldots,n\}$, em que m é o primeiro elemento cuja posição se mantém inalterada.

Para cada $A \subsetneq X_n$ seja $f(n,m,A)$ o número de per

mutações de X_n que deixam m e A fixos.(*) Seja também g(n,m,A) o número de permutações de X_n que mantém m e pelo menos os elementos de A fixos. Obviamente, então, fazendo $X_n - \{m\} = X_{m-}$:

$$g(n,m,A) = \sum_{X_{m-} \supset B \supset A} f(n,m,B)$$

Pelo princípio de inclusão-exclusão

$$P_n(m) = f(n,m,\emptyset) = g(n,m,\emptyset) - \sum_{B \subset X_{m-}\,;\,|B|=1} g(n,m,B) +$$

$$+ \sum_{B \subset X_{m-}\,;\,|B|=2} g(n,m,B) - \ldots + (-1)^{m-1} \cdot g(n,m,X_{m-})$$

Mas, se $|B| = i$, $B \subset X_{m-}$, o número de permutações que deixam m e pelo menos os elementos de B fixos é $(n-1-i)!$ Como existem $\binom{m-1}{i}$ i-subconjuntos de X_{m-}, então

$$\sum_{B \subset X_{m-}\,;\,|B|=i} g(n,m,B) = \binom{m-1}{i}(n-1-i)!$$

Donde

$$P_n(m) = \sum_{i=0}^{m-1} (-1)^i \binom{m-1}{i}(n-1-i)!$$

Daí, através da identidade $\binom{m}{i} = \binom{m-1}{i} + \binom{m-1}{i-1}$ chega-se à fórmula recorrente

$$P_n(m+1) = P_n(m) - P_{n-1}(m)$$

Exemplo. Vejamos ainda a chamada fórmula geral do crivo. Se A é um conjunto não vazio, seja $\alpha: A \to R$ uma função que possa ser estendida a $\mathcal{P}(A)$ por

$$\alpha(B) = \sum_{x \in B} \alpha(x), \quad B \subset A$$

Suporemos $\alpha(x) = 1$, para todo $x \in A$, e portanto $\alpha(B) = |B|, B \subset A$. Para cada $i \in X_r$ admitamos associada uma propriedade P_i e seja $A_i = \{x \in A \mid P_i(x)\}$. Para cada $J \subset X_r$ façamos $E_J = \bigcap_{j \in J} A_j - \bigcup_{j \notin J} A_j$ e $F_J = \bigcap_{j \in J} A_j$. Quer dizer, E_J é formado pelos elementos de A que gozam apenas das propriedades P_j, com $j \in J$, ao passo que F_J cons-

((*) apenas)

ta daqueles elementos de A para os quais pelo menos as propriedades P_j, $j \in J$, se verificam. Fazendo então $f(J) = \alpha(E_J)$ e $g(J) = \alpha(F_J)$ é claro que $g(J) = \sum_{I \supset J} f(I)$ e portanto

$$f(J) = \sum_{I \supset J} (-1)^{|I-J|} \cdot g(I)$$

A fórmula citada se obtém fazendo a soma para todos os $J \subset X_r, |J|=k$:

$$\sum_{|J|=k} \alpha(E_J) = \sum_{i=k}^{r} (-1)^{i-k} \binom{i}{k} \sum_{|I|=i} \alpha(F_I)$$

É claro que o exemplo anterior pode ser considerado neste contexto.

4.4. Função de Möbius e o Permanente de uma Matriz.

(4.1) Seja $A = (a_{ij})$ uma matriz $m \times n$ complexa, $m \leq n$. O permanente de A, indicado per(A), é a soma

$$\text{per}(A) = \sum_{j_i} \left(\prod_{i=1}^{m} a_{ij_i} \right)$$

estendida a todas as aplicações injetoras $i \to j_i$ $(i=1,2,\ldots,m)$ de X_m em X_n. Logo o número de parcelas da somatória é $(n)_m$.

Registremos as seguintes propriedades:

(a) Permutando-se numa matriz A, $m \times n$, $m \leq n$, duas de suas linhas ou colunas, seu permanente não se altera.

(b) Multiplicar uma linha de A por um escalar λ equivale a multiplicar per(A) por λ, para toda matriz A, $m \times n$, $m \leq n$. Se S é quadrada, isto vale inclusive para uma coluna de A.

(c) Para toda matriz quadrada A: $\text{per}(A) = \text{per}(A^t)$

(d) Se A_{ij} indica a matriz obtida de A pela supressão da linha i-ésima e da coluna j-ésima, então

$$\text{per}(A) = \sum_{j=1}^{n} a_{ij} \, \text{per}(A_{ij})$$

para todo i, $1 \leq i \leq m$.

Proposição 5. Seja A uma matriz quadrada de ordem n. Para todo $E \subset X_n$ seja $A|E$ a submatriz de A formada pelas colunas correspondentes aos índices que estão em E e seja $\phi(A|E)$ o produto das somas dos elementos das linhas de $A|E$. Então

$$per(A) = \sum_{E \subset X_n} (-1)^{|X_n - E|} \cdot \phi(A|E)$$

Demonstração. Suponhamos inicialmente A de tipo m x n qualquer. Para cada $D \subset X_n$ pode-se definir $\phi(A|D)$ de maneira análoga ao caso das matrizes quadradas e é claro que

$$\phi(A|D) = \sum_{f} \left(\prod_{i=1}^{m} a_{if(i)} \right)$$

onde f percorre o conjunto das aplicações de X_m em D. Fazendo

$$\sigma(A|D) = \sum_{f} \left(\prod_{i=1}^{m} a_{if(i)} \right)$$

onde f percorre apenas o conjunto das sobrejeções de X_m em D, é óbvio então que

$$\phi(A|D) = \sum_{E \subset D} \sigma(A|E)$$

Considerando o resultado obtido em (3.1):

$$\sigma(A|D) = \sum_{E \subset D} \mu(E,D)\phi(A|E) = \sum_{E \subset D} (-1)^{|D|-|E|} \cdot \phi(A|E) =$$

$$= \sum_{E \subset D} (-1)^{|D-E|} \cdot \phi(A|E)$$

Observando que no caso de uma matriz quadrada n x n $\sigma(A|X_n) = per(A)$, visto que as sobrejeções de X_n são também as injeções, então

$$per(A) = \sum_{E \subset X_n} (-1)^{|X_n - E|} \cdot \phi(A|E)$$

(4.2) Aplicações.

(a) O problema do desencontro. É bem conhecido

este problema cujo enunciado é o seguinte: "Quantas permutações do conjunto X_n não deixam fixo nenhum elemento?"

Seja D_n esse número. A solução do problema poderia ser obtida diretamente do princípio de inclusão-exclusão. De fato, se para cada $X \subset X_n$, $f(X)$ indica o número de permutações que deixam X fixo então $D_n = f(\emptyset)$. Se $g(X)$ indica o número de permutações que deixam fixos ao menos os elementos de X, então

$$g(X) = \sum_{Y \supset X} f(Y)$$

a partir do que tiramos, através do referido princípio, que

$$D_n = n! \sum_{k=o}^{n} \frac{(-1)^k}{k!}$$

Seja $A = (a_{ij})$ a matriz n x n definida por $a_{ii} = 0$ $(i = 1,2,\ldots,n)$ e $a_{ij} = 1$ sempre que $i \neq j$. Como

$$per(A) = \sigma(A|X_n) = \sum_{f} \left(\prod_{i=1}^{n} a_{if(i)} \right)$$

onde f percorre as bijeções de X_n, as parcelas onde existem encontros $i = f(i)$ são nulas e as demais são iguais a 1, então $per(A) = D_n$ neste caso.

Portanto

$$D_n = \sum_{E \subset X_n} (-1)^{|X_n - E|} \cdot \phi(A|E) =$$

$$= (-1)^{n-1}.\binom{n}{1}.0 + (-1)^{n-2}.\binom{n}{2}.1^2.2^{n-2} + \ldots + (-1)\binom{n}{n-1}.(n-2)^{n-1}.(n-1) +$$

$$+ (-1)^0.\binom{n}{n}.(n-1)^n.n^0 = \sum_{k=2}^{n} (-1)^{n-k}.\binom{n}{k}.(k-1)^k.k^{n-k}$$

Considerando o resultado já citado temos a identidade:

$$n! \sum_{k=o}^{n} \frac{(-1)^k}{k!} = \sum_{k=2}^{n} (-1)^{n-k}.\binom{n}{k}.(k-1)^k.k^{n-k}$$

(b) O problema das aplicações sobrejetoras de X_m em X_n $(m \geq n)$.

Consideremos a matriz $A = (a_{ij})$, m x n, onde $a_{ij} = 1$ para quaisquer índices i e j. Como $\sigma(A|X_n)$ indica a soma dos produtos $\sum_{i=1}^{m} a_{if(i)}$ correspondentes às funções sobrejetoras $f: X_m \to X_n$ e como cada um desses produtos é igual a 1, então existe uma correspondência biunívoca entre o conjunto das sobrejeções de X_m em X_n e o conjunto desses produtos. Logo

$$\sigma(A|X_n) = \sum_{E \subset X_n} (-1)^{|X_n - E|} \cdot \phi(A|E)$$

dá o número dessas sobrejeções. Um cálculo simples sobre

$$A = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 1 & 1 & \dots & 1 \end{bmatrix}$$

fornece

$$\sigma(A|X_n) = (-1)^{n-1}\binom{n}{1}1^m + (-1)^{n-2}\binom{n}{2}2^m + \dots + (-1)^{n-n}\binom{n}{n}n^n =$$

$$= \sum_{k=1}^{n} (-1)^{n-k}\binom{n}{k}k^m$$

(c) O número de permutações de X_n que levam r em s ou s em r $(1 \leq r < s \leq n)$.

Se $A = (a_{ij})$ é a matriz n x n definida por $a_{rs} = a_{sr} = 0$ e $a_{ij} = 1$ sempre que $i \neq r$ ou $j \neq s$, então o número procurado é $n! - \sigma(A|X_n)$. De fato, se todos os termos de A fossem iguais a 1 valeria a igualdade $\sigma(A|X_n) = n!$; como aqueles termos de $\sigma(A|X_n)$ em que aparecem a_{rs} ou a_{sr} são nulos, então $\sigma(A|X_n)$ expressa, para a matriz A em consideração, o número de permutações que não transformam r em s e nem, tampouco, s em r.

Do exame da matriz

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & 1 & \dots & 1 \\ . & . & . & . & \dots & . \\ 1 & 1 & 1 & 1 & \dots & 1 \end{bmatrix}$$

decorre que

$$\sigma(A|X_n) = (-1)^{n-1}.(n-2) + (-1)^{n-2}\left[\binom{n-2}{0}.1^2.2^{n-2} + 2\binom{n-2}{1}.1.2^{n-1} + \right.$$

$$\left. + \binom{n-2}{2}2^n\right] + (-1)^{n-3}\left[\binom{n-2}{1}2^2.3^{n-2} + 2\binom{n-2}{2}2 \cdot 3^{n-1} + \binom{n-2}{3}3^n\right] + \dots$$

$$\dots + (-1)^0\left[(n-1)^2.n^{n-2}\right] = (-1)^{n-1}.(n-2) + \sum_{k=o}^{n-3}(-1)^{n-k-2}.\left[\binom{n-2}{k}(k+1)^2(k+2)^{n-2} + \right.$$

$$\left. + 2\binom{n-2}{k+1}(k+1)(k+2)^{n-1} + \binom{n-2}{k+2}(k+2)^n\right] + (n-1)^2 \cdot n^{n-2}$$

Por exemplo, se $n = 4$:

$$\sigma(A|X_4) = -2 + (-1)^2.\left[\binom{2}{0}1^2.2^2 + 2\binom{2}{1}.1 \cdot 2^3 + \binom{2}{2}2^4\right] +$$

$$+ (-1)\left[\binom{2}{1}2^2.3^2 + 2\binom{2}{2}.2.3^3\right] + 3^2.4^2 = -2 + 52 - 180 + 144 = 14$$

Donde $4! - 14 = 10$ é o número de permutações de X_4 que levam r em s ou s em r, $1 \leqslant r < s \leqslant 4$

(d) O número de aplicações de X_m em X_n $(m \leqslant n)$, com o conjunto imagem de maneira que cada elemento de X_m não seja maior que sua imagem , e cada elemento do conjunto imagem $\geqslant m$.

Em virtude da proposição 5 este número é dado por $\phi(A|D)$ e

$$\sigma(A|D) = \sum_{E \subset D} (-1)^{|D-E|} \cdot \phi(A|E)$$

onde

$$A = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 & \dots & 1 \\ 0 & 1 & 1 & \dots & 1 & \dots & 1 \\ 0 & 0 & 1 & \dots & 1 & \dots & 1 \\ . & . & . & \dots & 1 & \dots & . \\ 0 & 0 & 0 & \dots & 1 & \dots & 1 \end{bmatrix}$$

é $m \times n$ e $D \subset X_n$ é o conjunto de índices correspondente às últimas n-m+1 colunas (aquelas onde não figuram zeros), ou seja, o conjunto imagem das funções procuradas.

Por exemplo, se $m = 3$ e $n = 5$, então $D = \{3,4,5\}$

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

e

$$\sigma(A|D) = (-1)^2(1+1+1) + (-1)^1(2^3+2^3+2^3) + (-1)^0.3^3 = 6$$

Sejam r e s naturais e suponhamos $r \geq s \geq 1$. Logo o número de aplicações de X_s em X_{r+s} cuja imagem é $D = \{s, s+1, \ldots, s+r\}$ é zero visto que $|D| = r+1 > s$. Assim, considerando a matriz A, tipo $s \times (r+s)$:

$$A = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 & 1 & \ldots & 1 \\ 0 & 1 & \ldots & 1 & 1 & 1 & \ldots & 1 \\ . & . & \ldots & . & . & . & \ldots & . \\ 0 & 0 & \ldots & 0 & 1 & 1 & \ldots & 1 \end{bmatrix}$$

obtem-se

$$0 = \sigma(A|D) = (-1)^r\binom{r+1}{1}1^s + (-1)^{r-1}.\binom{r+1}{2}2^s + \ldots + (-1)\binom{r+1}{r}r^s +$$

$$+ (-1)^0\binom{r+1}{r+1}(r+1)^s$$

ou seja, é válida a seguinte identidade combinatória

$$\sum_{i=1}^{r+1} (-1)^{r+1-i} \cdot \binom{r+1}{i} \cdot i^s = 0$$

sempre que $r \geq s \geq 1$ $(r,s \in N)$.

5. Conexões de Galois.

(5.1) Uma conexão de Galois entre dois conjuntos parcialmente ordenados P e Q é uma par de funções $\pi: Q \to P$ e $\rho: P \to Q$ para as quais: (i) $p_1 \leq p_2 \Longrightarrow \rho(p_2) \leq \rho(p_1)$ e $q_1 \leq q_2 \Longrightarrow \pi(q_2) \leq \pi(q_1)$; (ii) $\pi(\rho(p)) \geq p$, $\forall\, p \in P$ e $\rho(\pi(q)) \geq q$,

$\forall\ q \in Q$.

É fácil mostrar que nessas condições as aplicações $p \mapsto \pi(\rho(p))$ e $q \mapsto \rho(\pi(q))$ são operadores fêcho.

Proposição 6. Sejam P e Q conjuntos parcialmente ordenados e localmente finitos tais que P possui 0 e Q possui 0 e 1. Seja $\pi: Q \to P$, $\rho: P \to Q$ conexão de Galois de maneira que: $\pi(x) = 0 \iff x = 1$ e $\rho(0) = 1$. Então

$$\mu(0,1) = \sum_{a>o} \mu_P(0,a)\zeta(\rho(a),0) = \sum_{a:\rho(a)=o} \mu_P(0,a)$$

onde μ_P e μ são as funções de Möbius de P e Q, respectivamente, e ζ é a função zeta de Q.

Demonstração. Notemos primeiro que da definição de conexão de Galois decorre direto que: $\pi(x) \geqslant b \iff x \leqslant \rho(b)$. Daí então, fixando $b \in P$:

$$\sum_{a \geqslant b} \delta(\pi(x),a) = \zeta(x,\rho(b)) \qquad (*)$$

para todo $x \in Q$. De fato, seja $x \in Q$. Se $x \leqslant \rho(b)$, então $\zeta(x,\rho(b)) = 1$. Mas neste caso $\pi(x) \geqslant b$ e $\delta(\pi(x), \pi(x)) = 1$ é umas das parcelas do primeiro membro de (*), sendo as outras obviamente nulas, o que garante a igualdade neste caso. Se $x \not\leqslant \rho(b)$, então $\zeta(x,\rho(b)) = 0$. Mas então $\pi(x) \not\geqslant b$ e portanto no primeiro membro de (*) todas as parcelas são nulas. Assim (*) é efetivamente válida e aplicando a ela a fórmula de inversão de Möbius:

$$\delta(\pi(x),b) = \sum_{a \geqslant b} \mu_P(b,a)\zeta(x,\rho(a))$$

e daí

$$\delta(\pi(x),0) = \sum_{a \geqslant o} \mu_P(0,a)\zeta(x,\rho(a))$$

Mas, das hipóteses decorre que: $\delta(\pi(1),0) = 1$ e $\delta(\pi(x),0) = 0$, $\forall\ x \neq 1$. Logo $\delta(\pi(x),0) = 1 - n(x,1)$.

Assim

$$1 - n(x,1) = \zeta(x,\rho(0)) + \sum_{a>o} \mu_p(0,a)\zeta(x,\rho(a)) \qquad (**)$$

Ainda pelas hipóteses, $\zeta(x,\rho(0)) = \zeta(x,1) = 1$ posto que $x \leq 1$.

Então (**) se transforma em:

$$- n(x,1) = \sum_{a>o} \mu_p(0,a)\zeta(x,\rho(a)) \qquad (***)$$

Levando em conta que $n(1,1) = 0$ e $n(x,1) = 1$, se $x \neq 1$, então

$$\mu(0,1) = - \sum_{o\leq x<1} \mu(0,x) = - \sum_{o\leq x<1} \mu(0,x)n(x,1) + \mu(0,1)n(1,1) = - \sum_{o\leq x\leq 1} \mu(0,x)n(x,1)$$

De (***) e desta última conclusão resulta que:

$$\mu(0,1) = \sum_{a>o} \mu_p(0,a) \cdot \sum_{o\leq x\leq 1} \mu(0,x)\zeta(x,\rho(a)) \qquad (****)$$

Por outro lado, uma verificação parecida à que foi feita para se chegar a (*) fornece:

$$\zeta(y,\rho(a)) = \sum_{x\geq y} \delta(x,\rho(a))$$

para todo $y \in Q$. Pela fórmula de inversão de Möbius:

$$\delta(y,\rho(a)) = \sum_{x\geq y} \mu(y,x)\zeta(x,\rho(a))$$

Em particular

$$\delta(0,\rho(a)) = \sum_{x\geq o} \mu(0,x)\zeta(x,\rho(a))$$

o que substituido em (****) leva a:

$$\mu(0,1) = \sum_{a>o} \mu_p(0,a)\delta(0,\rho(a))$$

Como porem $\delta(0,\rho(a)) = \zeta(\rho(a),0)$, então

$$\mu(0,1) = \sum_{a>o} \mu_p(0,a)\zeta(\rho(a),0)$$

Observando ainda que $\zeta(\rho(a),0) = 0$, sempre que $\rho(a) \neq 0$, então

$$\mu(0,1) = \sum_{a:\,\rho(a)=0} \mu_p(0,a)$$

Corolário. Sejam P e Q conjuntos parcialmente ordenados e localmente finitos tais que P possui unidade e Q pos

sui zero e unidade. Se $p: Q \to P$ e $q: P \to Q$ são funções que preservam a ordem e para as quais: (1) $p(x) = 1 \iff x = 1$; (2) $p(q(x)) \leq x$ e $q(p(y)) \geq y$, $\forall x \in P$ e $\forall y \in Q$; (3) $q(1) = 1$, então

$$\mu(0,1) = \sum_{a<1} \mu_p(a,1)\zeta(q(a),0) = \sum_{a:q(a)=o} \mu_p(a,1)$$

mantidas as notações do teorema.

Demonstração. Consideremos sobre P a relação de ordem oposta à do enunciado. A unidade de P passa a funcionar como zero e a hipótese (2) garante que p e q são conexões de Galois. Daí é só adaptar a notação, lembrando inclusive que $\mu_p^*(1,a) = \mu_p(a,1)$.

Proposição 7. Seja P um conjunto parcialmente ordenado e localmente finito e seja Q um conjunto finito, também parcialmente ordenado com zero. Suponhamos $p: Q \to P$ crescente e sobrejetora de maneira que para todo $a \in P$, $p^{-1}([0,a]) = [0,x]$, e que $p^{-1}(0)$ contenha pelo menos dois elementos de Q. Então, para todo $a \in P$:

$$\sum_{x:p(x)=a} \mu(0,x) = 0$$

Demonstração (por indução). Considerando inicialmente o intervalo $[0,0] = \{0\}$, como $p^{-1}(0)$ contem pelo menos dois elementos, então $p^{-1}(0) = [0,q]$, $q > 0$. Daí:

$$\sum_{x:p(x)=0} \mu(0,x) = \sum_{x\in p^{-1}(0)} \mu(0,x) = \sum_{0\leq x\leq q} \mu(0,x) = \mu(0,q) + \sum_{0\leq x<q} \mu(0,x) = 0$$

Seja $a \in P$, $a > 0$, e suponhamos o teorema verdadeiro para todo $b \in P$, $b < a$. Então

$$\sum_{b<a} \left(\sum_{x:p(x)=b} \mu(0,x) \right) = 0$$

e portanto

$$\sum_{x:p(x)=a} \mu(0,x) = \sum_{b\leq a} \left(\sum_{x:p(x)=b} \mu(0,x) \right)$$

Observando que

$$p^{-1}([0,a]) = \{x \in Q \mid 0 \leq p(x) \leq a\} = [0,r]$$

para algum $r \in Q$, então

$$\sum_{b \leq a} \Big(\sum_{x:p(x)=b} \mu(0,x) \Big) = \sum_{0 \leq x \leq r} \mu(0,x) = \delta(0,r)$$

Mas $r > 0$ porque $a > 0$ obriga a que $[0,a]$ tenha pelo menos dois elementos e consequentemente o mesmo ocorre com $[0,r]$. Daí $\delta(0,r)=0$ e

$$\sum_{x:p(x)=a} \mu(0,x) = \sum_{b \leq a} \Big(\sum_{x:p(x)=b} \mu(0,x) \Big) = 0$$

(5.2) Aplicações e Exemplos.

Proposição 8. (Teorema do Corte Transversal). Seja R um subconjunto de um reticulado finito L, com as seguintes propriedades: (a) $1 \notin R$; (b) para todo $x \in L$, $x \neq 1$, existe $y \in R$ de modo que $y \geq x$. Se, para $k \geq 2$, q_k indica o número de subconjuntos de R de cardinal k cujo ínfimo é 0, então

$$\mu(0,1) = q_2 - q_3 + q_4 - \ldots$$

Demonstração. Seja $P = B(R)$ a álgebra dos subconjuntos de R e estabeleçamos entre P e $Q = L$ a seguinte conexão de Galois: para cada $x \in L$, seja $\pi(x) = \{r \in R \mid r \geq x\}$ (em particular $\pi(1) = \emptyset$); para cada $A \in P$, seja $\rho(A) = \bigwedge A$, isto é, o ínfimo de A (como é usual faz-se $\rho(\emptyset) = 1$). Mostremos que as funções assim definidas formam efetivamente uma conexão de Galois, entre P e Q e que satisfazem as condições da proposição 6.

. Se $x_1 \leq x_2$ em L, então $r \geq x_2$ implica $r \geq x_1$ e portanto $\pi(x_2) \leq \pi(x_1)$

. Sejam $A_1, A_2 \in P$, $A_1 \subset A_2$. Se $A_1 = \emptyset$, então $\rho(A_2) = \bigwedge A_2 \leq 1 = \rho(\emptyset) = \rho(A_1)$; se $A_2 = \emptyset$, então $A_1 = \emptyset$ e $\rho(A_1) = \rho(A_2) = 1$. Excluidos estes casos a definição de ínfimo implica $\bigwedge A_2 \subset \bigwedge A_1$, isto é, $\rho(A_2) \subset \rho(A_1)$:

. Seja $x \in L$. Se $x = 1$ é imediato que $\rho(\pi(x)) = x$. Se $x \neq 1$, então $\pi(x)$ é formado dos elementos de R maiores que ou iguais a x e portanto para $\rho(\pi(x))$, o ínfimo do con

junto desses elementos, o mesmo se verifica: $\rho(\pi(x)) \geq x$.

. Seja $A \in P$. Se $A = \emptyset$, vale $\rho(A) = 1$ e daí $\pi(\rho(A)) = \pi(1) = \emptyset = A$. Se $A \neq \emptyset$, como para cada $r \in A$ vale $r \geq \bigwedge A = \rho(A)$, então $r \in \pi(\rho(A))$ e portanto $A \subset \pi(\rho(A))$.

. Mostremos que: $\pi(x) = \emptyset \iff x = 1$

Supor $\pi(x) = \emptyset$ e $x < 1$ leva a uma contradição visto que esta desigualdade acarreta $1 \in \pi(x)$. A recíproca é óbvia.

Assim, devido à proposição 6

$$\mu(0,1) = \sum_{A:\rho(A)=0} \mu_P(\emptyset,A)$$

Como P é a álgebra dos subconjuntos de R:

$$\mu_P(\emptyset,A) = (-1)^{|A|}$$

Donde

$$\mu(0,1) = \sum_{A:\rho(A)=0} (-1)^{|A|} = \sum_{A:\bigwedge A=0} (-1)^{|A|} = q_2 - q_3 + q_4 - \ldots$$

Proposição 9. Seja $x \to \overline{x}$ um operador fêcho sobre um conjunto parcialmente ordenado Q, com unidade 1, de maneira que $\overline{x} = 1$ se, e somente se, $x = 1$. Se P é o conjunto parcialmente ordenado formado pelos subconjuntos fechados de Q, então: (a) $\overline{x} > x \Longrightarrow \mu(x,1) = 0$; (b) $\overline{x} = x \Longrightarrow \mu(x,1) = \mu_P(x,1)$, onde μ e μ_P são as funções de Möbius de Q e P, respectivamente.

Demonstração. Para cada $x \in Q$, se $Q_x = [x,1]$, então Q_x tem um zero que é x, alem de, obviamente, ser parcialmente ordenado. Definindo $p: Q \to P$ por $p(y) = \overline{y}$ e $q: P \to Q$ por $q(y) = y$ temos:

. $p(q(y)) = p(y) = \overline{y} = y$, para todo $y \in P$, e $q(p(y)) = q(\overline{y}) = \overline{y} \geq y$, para todo $y \in Q$.

. $p(y) = \overline{y} = 1$ se, e somente se, $y = 1$, por hipótese

. $q(1) = 1$, por definição de q.

Logo p e q satisfazem as condições do corolário da proposição 6, fato que também ocorre se p for restrita a Q_x e q ao conjunto dos fechados de Q_x. Logo

$$\mu(x,1) = \sum_{a:q(a)=x} \mu_P(a,1)$$

Se $\overline{x} > x$, então $x \notin P$. Mas como $q(a) = x$ ocorre se, e somente se, $a = x$, então não existe $a \in P$ de maneira que $q(a) = x$. Daí

$$\mu(x,1) = 0$$

Suponhamos $\overline{x} = x$. Se $a \in P$ e $q(a) = x$, então $p(q(a)) = p(x) = \overline{x} = x$ e como $p(q(a)) = a$, então $x = a$. Se x é o único elemento de P tal que $q(x) = x$, então

$$\mu(x,1) = \mu_P(x,1).$$

Corolário (Hall). Seja L um reticulado finito. Se $0 \in L$ não é o ínfimo do conjunto dos coátomos de L ou se $1 \in L$ não é o supremo do conjunto dos átomos de L, então $\mu(0,1) = 0$.

Demonstração. (Apenas para o caso em que 0 não é o ínfimo do conjunto dos coátomos de L.)

Para cada $x \in L$ seja

$$A(x) = \{q \in L \mid q \text{ é coátomo e } q \geq x\}$$

Para cada $x \in L$ façamos $\overline{x} = \bigwedge A(x)$. É rotineiro mostrar que $x \mapsto \overline{x}$ é um operador fêcho.

Mostremos que: $\overline{x} = 1 \iff x = 1$. Se $x = 1$, então $A(x) = \emptyset$ e portanto $\overline{x} = \bigwedge A(x) = 1$. Admitamos $\overline{x} = 1$ e $x < 1$. Daí $1 = \overline{x} = \bigwedge A(x)$ do que segue, considerando um coátomo $q \in A(x)$, que $1 \leq q < 1$. Absurdo.

Logo, as hipóteses gerais da proposição 9 se verificam neste caso com relação a L. Como $\overline{0} = \bigwedge A(0) > 0$ por hipótese, então, devido à parte (a) da proposição citada: $\mu(0,1) = 0$.

Proposição 10. Seja $a \to \overline{a}$ um operador fêcho num

reticulado finito Q para o qual $\overline{a \vee b} = \bar{a} \vee \bar{b}$, $\forall\, a,b \in Q$, e $\bar{0} > 0$. Então, para todo $a \in Q$:

$$\sum_{x:\bar{x}=a} \mu(0,x) = 0$$

Demonstração. Seja $P = \{x \in Q \mid x \text{ é fechado}\}$. Então P é um conjunto parcialmente ordenado finito e para $p: Q \to P$ definida por $p(x) = \bar{x}$ vale o seguinte:

. é crescente.

. é sobrejetora pois se $z \in P$, então $z = \bar{z}$ e daí $p(z) = \bar{z} = z$.

. $\bar{0}$ é o zero de P; com efeito, como $0 \leq x, \forall\, x \in P$, então $\bar{0} \leq \bar{x} = x$.

. $0, \bar{0} \in p^{-1}(\bar{0})$ uma vez que $p(0) = \bar{0}$ e $p(\bar{0}) = \bar{\bar{0}} = \bar{0}$; logo $p^{-1}(\bar{0})$ contem pelo menos dois pontos.

. $p^{-1}([0,a]) = [0,a]$; de fato, se $x \in p^{-1}([0,a])$, então $0 \leq p(x) \leq a$, isto é, $0 \leq \bar{x} \leq a$ e como $0 \leq x \leq \bar{x}$ concluimos que $0 \leq x \leq a$ o que garante que $x \in [0,a]$; por outro lado, se $x \in [0,a]$, então $0 \leq x \leq a$ e daí $0 \leq \bar{x} = p(x) \leq \bar{a} = a$, vale dizer, $x \in p^{-1}([0,a])$.

Considerando a proposição 7 podemos concluir então que

$$\sum_{x:\bar{x}=a} \mu(0,x) = 0$$

Corolário (Weisner). Seja L um reticulado finito. (a) Se $a \in L$ e $a > 0$, então, $\forall\, b \in L$:

$$\sum_{x \vee a = b} \mu(0,x) = 0$$

(b) Se $a \in L$ e $a < 1$, para qualquer $b \in L$ vale

$$\sum_{x \wedge a = b} \mu(x,1) = 0$$

Demonstração. Quanto à afirmação (a) basta considerar sobre L o operador fêcho definido por $x \to \bar{x} = x \vee a$. Para (b) considere-se a relação de ordem parcial inversa daquela de L

e o operador fêcho: $x \to x \wedge a$.

Exemplo.

Seja G_n um reticulado geométrico finito de dimensão n. Mostremos que se $a,b \in G_n$ têm mesma dimensão, então $\mu(0,a)$ e $\mu(0,b)$ têm mesmo sinal. Se a e b têm dimensão zero, então a e b são pontos e daí $\mu(0,a) = \mu(0,b) = -1$. Seja $r > 0$ e admitamos a afirmação válida para quaisquer elementos de G_n de dimensão $r - 1$. Seja $a \in G_n$ de dimensão r e tomemos um ponto $p < a$. Do corolário anterior segue então que

$$\mu(0,a) = - \sum_{x \vee p = a;\, x \neq a} \mu(0,x)$$

Mas $d(x \wedge p) + d(x \vee p) \leq d(x) + d(p)$, onde $d(x \vee p) = r$, $d(p) = 0$ e $d(x \wedge p) = d(0) = -1$, para cada x da somatoria anterior. Daí, para estes elementos: $d(x) \geq r-1$. Como porém $x < a$, então $d(x) < d(a)$, e portanto $d(x) = r-1$ para todo x tal que $x \neq a$ e $x \vee p = a$. Como os $\mu(0,x)$ com $d(x) = r-1$ têm todos mesmo sinal pela hipótese de indução, então todos os $\mu(0,a)$, com $d(a) = r$, também têm mesmo sinal o qual é contrário ao sinal dos $\mu(0,x)$, sempre que $d(x)=r-1$.

Como consequencia, se y cobre z, então $\mu(x,y)$ e $\mu(x,z)$ tem sinais contrários. Como $[x,y]$ é geométrico, supondo $y = z \vee p$ (p ponto), observando que em

$$\mu(x,y) = - \sum_{t \vee p = y;\, t \neq y} \mu(x,t)$$

as parcelas do segundo membro têm todas o mesmo sinal, já que $d(t) = d(y) - 1$, sempre que $t \neq y$, e que $\mu(x,z)$ é uma das parcelas, fica justificada a afirmação.

Dos argumentos expostos decorre também que:

$$x \leq y \implies \mu(x,y) \neq 0$$

6. A Função de Mobius em Reticulados Finitos e a Complementação.

(6.1) Seja P um conjunto parcialmente ordenado e localmente finito com 0 e 1 e seja Q um conjunto parcialmente ordenado. Indiquemos por $f: P \to Q$ uma função que preserva as relações de ordem e para a qual $f(0) < f(1)$. Para todo $z \in [0,1]$, se $f(z) > f(0)$, seja

$$[0,z]_f = \{z\} \cup \{y \in [0,z] \mid f(y) < f(z)\}$$

Os elementos 0 e z são, respectivamente, o mínimo e máximo de $[0,z]_f$. Indicaremos por $\mu_f(0,z)$ o valor, no ponto (0,z), da restrição de $\mu \in A(P)$ ao conjunto $[0,z]_f \times [0,z]_f$.

Proposição 11. Sejam P, Q e f conforme as considerações anteriores. Então, para todo t tal que $0 < t \leq 1$ e $f(t) > f(0)$:

$$\mu(0,t) = \sum_{z: z \leq t \text{ e } f(z)=f(t)} \mu_f(0,z).\mu(z,t)$$

Demonstração. Pelo lema de Hall $\mu(0,t) = c_o - c_1 + c_2 - c_3 + \ldots$ onde c_k é o número de cadeias $0 = z_o < z_1 < \ldots < z_k = t$, de comprimento k, de 0 a t (é claro que $c_o = 0$).

Para cada uma dessas cadeias existe um primeiro elemento $z_i = z$ para o qual $f(z) = f(t)$. Mostremos que os membros da subcadeia $0 = z_o < z_1 < \ldots < z_i = z$ estão em $[0,z]_f$. De fato, se $0 \leq n \leq i-1$, como $f(z_n) \leq f(z) = f(t)$ podemos concluir, dada a escolha de z, que $f(z_n) < f(t)$. Por outro lado, se z é algum elemento de P para o qual $0 < z \leq t$ e $f(z) = f(t)$, considerando uma cadeia $z < \ldots < t$ qualquer, então $0 < z < \ldots < t$ é uma cadeia de 0 a t onde z é o primeiro elemento que verifica $f(z) = f(t)$ e cujos elementos 0,z, que formam uma cadeia de 0 a z, estão em $[0,z]_f$.

Para cada x, $0 \leq x \leq t$, indiquemos por $c_k(x,t)$ o número de cadeias de x a t de comprimento k e por $c(x,t,\lambda)$ o poli-

nômio em λ:

$$c(x,t,\lambda) = \sum_k c_k(x,t)\lambda^k$$

Por $c_f(0,z,\lambda)$ denotemos o polinômio cujo coeficiente de λ^k conta as cadeias de 0 a z, $(z \in P, f(0)<f(z))$ no conjunto $[0,z]_f$, de comprimento k.

Observando que o coeficiente de λ^k no produto $c_f(0,z,\lambda).c(z,t,\lambda)$, onde $0 < z \leq t$, é o número de cadeias de comprimento k, de 0 a t, de maneira que z é o primeiro elemento para o qual $f(z) = f(t)$, então

$$c(0,t,\lambda) = \sum_{z:f(z)=f(t)} c_f(0,z,\lambda).c(z,t,\lambda)$$

A tese decorre do lema de Hall fazendo $\lambda = -1$ na igualdade anterior.

Corolário. Mantidas as notações da proposição 11 vale a seguinte igualdade:

$$\mu_f(0,t) = \sum_{z:z\leq t \text{ e } f(z)=f(t)} \mu(0,z)$$

Demonstração.

$$\mu_f(0,t) = \sum_{o\leq z\leq t} \mu_f(0,z)\delta(z,t) =$$

$$= \sum_{o\leq z\leq t} \mu_f(0,z) \sum_{z\leq y\leq t} \mu(z,y)\zeta(y,t) = \sum_{y\leq t} \left(\sum_{z\leq y} \mu_f(0,z)\mu(z,y)\right)\zeta(y,t) =$$

$$= \sum_{y\leq t} \left(\sum_{z\leq y} \mu_f(0,z)\mu(z,y)\right) = \sum_{y\leq t} \mu(0,y)$$

Como a somatória inicial da demonstração é estendida a todos os z, $0 \leq z \leq t$, tais que $f(z) = f(t)$ e como $z \leq y \leq t$, então $f(y) = f(t)$ na última somatória.

Proposição 12. (O efeito da complementação). Seja L um reticulado finito com função de Möbius μ e função zeta ζ. Se $x \in L$ e $x \neq 1$, então

$$\mu(0,1) = \sum_{\substack{\text{complementos} \\ y \text{ e } z \text{ de } x}} \mu(0,y)\zeta(y,z)\mu(z,1)$$

Demonstração. Seja $f: L \to [x,1]$ definida por $f(y) = y \vee x$. É imediato que f está bem definida e que preserva as ordens. Como, ademais, $f(0) = x$ e $f(1) = 1$, então $f(0) < f(1)$. Assim, estamos em condições de aplicar a proposição 11 e seu corolário:

$$\mu(0,1) = \sum_{z:x\vee z=1} \mu_f(0,z)\mu(z,1) \qquad (1)$$

e

$$\mu_f(0,z) = \sum_{y:y\leq z \text{ e } y\vee x=1} \mu(0,y) \qquad (2)$$

Os elementos $z \in L$ tais que $x \vee z = 1$ se dizem sup-semi-complementares de x. Notemos que, para cada um desses elementos, o conjunto parcialmente ordenado $Q = [0,z]_f$ é um subreticulado de L, uma vez que é fechado para $\wedge$ e que, para quaisquer $y_1, y_2 \in Q$ valem as relações $y_1 \leq z$ e $y_2 \leq z$. Em Q consideremos $R = \{y \in Q - \{z\} \mid y \text{ é maximal}\}$. Como $z \notin R$ e, para todo $y \in Q$, $y \neq z$, existe $u \in R$ de modo que $u \geq y$ (pois Q é finito), estamos em condições de aplicar a proposição 8:

$$\mu_f(0,z) = q_2 - q_3 + q_4 - \ldots$$

onde q_k $(k = 2,3,\ldots)$ é o número de subconjuntos de R, de cardinal k, cuja intersecção é 0.

Mostremos agora que, para todo $y \in R$, vale $x \wedge z \leq y$. Para tanto consideremos o elemento $v = y \vee (x \wedge z)$. Então

. $0 \leq y < z$

$0 \leq x \wedge z \leq z$

e portanto $0 \leq y \vee (x \wedge z) \leq z$, ou seja, $v \leq z$.

. se $y \vee (x \wedge z) = z$, então $[y \vee (x \wedge z)] \vee x = z \vee x = 1$; mas $[y \vee (x \wedge z)] \vee x = y \vee [(x \wedge z) \vee x] = y \vee x < 1$. Logo a hipótese $v = z$ deve ser descartada.

. $f(v) = [y \vee (x \wedge z)] \vee x = y \vee x = f(y) < 1$ o que garante, juntamente com o que acabamos de mostrar, que $v \in Q-\{z\}$.

. Como $0 \leq y \leq y \vee (x \wedge z) = v < z$, onde $v \in Q-\{z\}$ e y é maximal em $Q-\{z\}$, então $y = y \vee (x \wedge z)$ e portanto $x \wedge z \leq y$.

Assim, para cada sup-semi-complementar z de x há duas possibilidades:

(I) z não é complementar de x, isto é, $0 < x \wedge z$. Como para cada $y \in R$ vale a relação $x \wedge z \leq y$ e daí, para quaisquer $y_1, \ldots, y_k \in R$:

$$0 < y_1 \wedge y_2 \wedge \cdots \wedge y_k$$

então $q_2 = q_3 = \ldots = 0$ e portanto $\mu_f(0,z) = 0$.

(II) z é complementar de x, isto é, $x \wedge z = 0$, hipótese em que nem todos os q_k são nulos necessariamente.

Considerando (I) e (II) a fórmula (1) fica

$$\mu(0,1) = \sum_{z: x \vee z = 1 \text{ e } x \wedge z = 0} \mu_f(0,z)\mu(z,1) \qquad (3)$$

Mas se $x \wedge z = 0$, então, para cada $y \leq z$, vale $x \wedge y \leq x \wedge z = 0$ e daí $x \wedge y = 0$. Donde (2) fica:

$$\mu_f(0,z) = \sum_{y: y \leq z, x \vee y = 1, x \wedge y = 0} \mu(0,y) \qquad (4)$$

De (3) e (4) resulta

$$\mu(0,1) = \sum_{\substack{z: x \vee z = 1, x \wedge z = 0 \\ y: y \leq z, x \vee y = 1, x \wedge y = 0}} \mu(0,y)\mu(z,1) \qquad (5)$$

Como $\zeta(y,z) = 1$ se $y \leq z$ e $\zeta(y,z) = 0$ se $y \not\leq z$, podemos concluir que

$$\mu(0,1) = \sum_{\substack{\text{complementos} \\ y \text{ e } z \text{ de } x}} \mu(0,y)\zeta(y,z)\mu(z,1)$$

Exemplo.

Seja L_n o reticulado das partições de um conjunto de n elementos, digamos $X_n = \{1,2,\ldots, n\}$, onde a ordenação é feita por refinamento: $\pi \leq \sigma$ se, e somente se, cada bloco de π está contido em um único bloco de σ. O zero de L_n é a partição for

mada por n blocos (todos naturalmente unitários) e a unidade é a partição formada de um único bloco.

É sabido que L_n é geométrico e que um elemento $\pi \in L_n$ é um hiperplano se, e somente se, π é o complementar de um ponto. Outro fato é que todo intervalo $[\pi,\sigma]$ em L_n é também geométrico. Isto posto mostremos que $\mu(0,1) = (-1)^{n-1}(n-1)!$

Ora, se para a fórmula (5) da demonstração anterior escolhemos $x = \{\{1,2,\ldots, n-1\}; \{n\}\}$, então x é um hiperplano de L_n cujos complementares são os n-1 elementos (pontos).

$$y_i = \{\{1\};\ldots;\{i-1\};\{n,i\};\{i+1\};\ldots;\{n-1\}\}$$

$i = 1,2,\ldots, n-1$. Mas na fórmula referida tanto os y como os z são pontos de L_n e, com a escolha feita para x, são os elementos do conjunto $\{y_i\}$. Daí

$$\mu(0,1) = -(n-1)\mu(z,1)$$

visto que para dois pontos quaisquer z_1 e z_2 se tem $[z_1,1] \simeq [z_2,1] \simeq L_{n-1}$. Por indução: $\mu(z,1) = (-1)^{n-2}(n-2)!$ Donde

$$\mu(0,1) = (-1)^{n-1}(n-1)!$$

(6.2) A Função de Möbius em Reticulados Modulares Finitos.

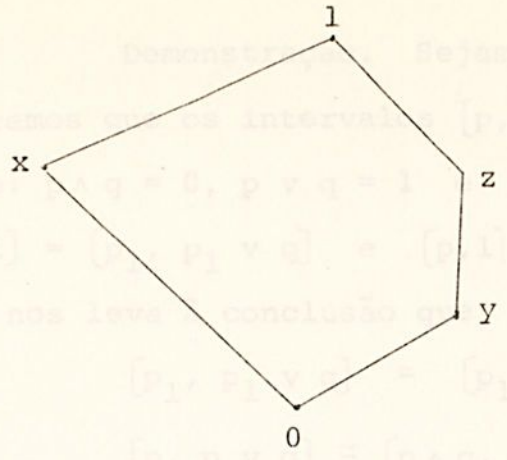
Proposição 13. Seja L um reticulado modular finito. Então, para todo $x \in L$:

$$\mu(0,1) = \sum_{\substack{\text{complementos} \\ z \text{ de } x}} \mu(0,z)\mu(z,1)$$

Demonstração. O teorema anterior (proposição 12), através de sua fórmula (5) nos diz que

$$\mu(0,1) = \sum_{\substack{z: x \vee z = 1 \text{ e } x \wedge z = o \\ y \leq z: x \vee y = 1 \text{ e } x \wedge y = o}} \mu(0,y)\mu(z,1)$$

Suponhamos que fosse possível a desigualdade $y < z$, para um certo $y \in L$, com as hipóteses feitas. Com isso $\{0,x,y,z,1\}$ seria um subreticulado de L, com cinco elementos, com diagrama



Considerando que z e y são complementares de x e que $y < z$, é fácil provar essa afirmação. Como porém:

$$y = y \vee (x \wedge z) \neq (y \vee x) \wedge z = z$$

embora $y < z$, esta hipótese leva a uma contradição com a modularidade de L. Donde $y = z$ e a fórmula (5) citada se converte em

$$\mu(0,1) = \sum_{\substack{\text{complementos} \\ z \text{ de } x}} \mu(0,z)\mu(z,1)$$

A partir de agora passaremos a considerar apenas reticulados modulares finitos complementados. Lembremos que uma condição necessária e suficiente para que um reticulado modular finito seja complementado é que a união dos átomos de L seja igual a 1. Mais ainda: com essas hipóteses L é relativamente complementado, ou seja, para quaisquer $a, b \in L$, $a < b$, o subreticulado modular $[a, b]$ é complementado. Para todo $x \in [a,b]$, se x' é um complementar de x em L, então $(a \vee x') \wedge b = a \vee (x' \wedge b)$ é um complementar de x em $[a,b]$.

Outro fato relativo aos reticulados modulares é o seguinte: se L é modular finito e se q é um coátomo de L, então todos os complementares de q são átomos; dualmente, todos os complementares de um átomo são coátomos.

Proposição 14. Seja L um reticulado modular finito e complementado. Se p é um complementar de um coátomo q e se o número de complementares de q é r, então $\mu(0,1) = - r\, \mu(p,1)$

Demonstração. Sejam p e p_1 átomos complementares de q e mostremos que os intervalos $[p,1]$ e $[p_1,1]$ são isomorfos. Por hipótese: $p \wedge q = 0$, $p \vee q = 1$ e $p_1 \wedge q = 0$, $p_1 \vee q = 1$. Portanto: $[p_1,1] = [p_1, p_1 \vee q]$ e $[p,1] = [p, p \vee q]$. Mas a modularidade de L nos leva à conclusão que

$$[p_1, p_1 \vee q] \simeq [p_1 \wedge q, q] = [0,q]$$

e

$$[p, p \vee q] \simeq [p \wedge q, q] = [0, q]$$

onde $\simeq$ indica a relação de isomorfismos. Donde

$$[p_1,1] \simeq [p,1]$$

De acordo com a proposição anterior

$$\mu(0,1) = \sum_{\substack{\text{complementar} \\ p \text{ de } q}} \mu(0,p)\mu(p,1)$$

Como p cobre 0, então $\mu(0,p) = -1$, para todo complementar p de q. Como ainda $\mu(p,1) = \mu(p_1,1)$ para quaisquer complementares p e p_1 de q, devido ao isomorfismo $[p,1] \simeq [p_1,1]$, então

$$\mu(0,1) = - r \mu(p,1)$$

Corolário. Seja $v \neq 0$ um elemento de um reticulado modular finito e complementado e seja $v_o = 0 < v_1 < v_2 < \ldots < v_k = v$ uma cadeia maximal de 0 a v. Se n_t é o número de complementares de v_t em $[0, v_{t+1}]$ $(t = 1,2,\ldots., k-1)$, então

$$\mu(0,v) = (-1)^k n_1 n_2 \ldots n_{k-1}$$

Demonstração. Como v_1 é um átomo, então $\mu(0,v_1) = -1$. Seja v_1' um complementar de v_1 em $[0,v_2]$. Como $[0,v_2]$ também é modular complementado, alem de finito, a proposição anterios garante que

$$\mu(0,v_2) = - n_1 \mu(v_1', v_2)$$

Mas: $[v_1', v_2] = [v_1', v_1 \vee v_1'] \simeq [v_1' \wedge v_1, v_1] = [0, v_1]$

Logo $\mu(0, v_2) = - n_1 \mu(0, v_1)$. Considerando que $\mu(0,v_1) = - 1$, então

$$\mu(0, v_2) = (-1)^2 n_1$$

Suponhamos

$$\mu(0, v_t) = (-1)^t n_1 n_2 \ldots n_{t-1}$$

onde $0 < t < k$. Se v_t' é um complementar de v_t em $[0, v_{t+1}]$, então

$$\mu(0, v_{t+1}) = -n_t \mu(v_t', v_{t+1})$$

Como $[v_t', v_{t+1}] \simeq [0, v_t]$, então $\mu(v_t', v_{t+1}) = \mu(0, v_t)$ e portanto

$$\mu(0, v_{t+1}) = - n_t \mu(v_t', v_{t+1}) = - n_t(-1)^t n_1 n_2 \ldots n_{t-1} =$$

$$= (-1)^{t+1} n_1 n_2 \ldots n_t$$

(6.3) Aplicações.

(a) Acharemos agora, usando o resultado anterior, a função de Möbius para o reticulado $L(V_n)$ dos subespaços vetoriais de um espaço vetorial V_n de dimensão n sobre G L(q).

Seja $V = V_k$ um subespaço vetorial de V_n, de dimensão k, e consideremos uma cadeia maximal

$$0 = V_o \subset V_1 \subset \ldots \subset V_k = V$$

onde, obviamente, dim $V_i = i$ $(i = 0,1,\ldots, k)$. Os coátomos de $[0, V_k]$ são os subespaços vetoriais de V_k de dimensão $k - 1$ e os seus complementares em $[0, V_k]$, subespaços vetoriais de V_k de dimensão 1. Logo, para todo k $(1 \leq k < n)$, os complementares de V_{k-1} em $[0, V_k]$ podem ser gerados por um único vetor não nulo. Além disso, indicando por $[u]$ o subespaço gerado por $u \in V_k$: $[u]$ é complementar de V_{k-1} se, e somente se, $u \notin V_{k-1}$. Ora, como V_k e V_{k-1} têm, respectivamente, q^k e q^{k-1} elementos, considerando-se que para cada $u \in V_k - V_{k-1}$ existem q-1 geradores de $[u]$, o número de complementares de V_{k-1} em $[0, V_k]$ é dado por

$$\frac{q^k - q^{k-1}}{q-1} = q^{k-1}$$

Considerando o corolário anterior:

$$\mu(0, V_k) = (-1)^k . q^1 . q^2 \ldots q^{k-1} = (-1)^k . q^{\frac{k(k-1)}{2}} = (-1)^k . q^{\binom{k}{2}}$$

Em particular

$$\mu(0, V_n) = (-1)^n \, q^{\binom{n}{2}}$$

(b) Seja X um subespaço vetorial de V_n de dimensão m. Se Z é um complementar de X, então dim Z = n - m e $[Z, V_n] \simeq [0,X]$. Considerando estes isomorfismos e a proposição 13:

$$\mu(0, V_n) = \sum_{\substack{\text{complementares} \\ Z \text{ de } X}} \mu(0,Z)\mu(0,X)$$

Se indicamos por k o número de subespaços de V_n de dimensão m, então

$$\mu(0, V_n) = k \, \mu(0,Z)\mu(0,X) =$$

$$= k(-1)^{n-m} \, q^{\binom{n-m}{2}} . (-1)^m . q^{\binom{m}{2}} = k(-1)^n . q^{\binom{n-m}{2} + \binom{m}{2}}$$

Como porém

$$\mu(0, V_n) = (-1)^n . q^{\binom{n}{2}}$$

então

$$k = q^{\binom{n}{2} - \binom{n-m}{2} - \binom{m}{2}} = q^{m(n-m)}$$

(c) Consideremos agora um reticulado distributivo L com mínimo 0. Seja a um elemento desse reticulado de maneira que $[0,a]$ é um subreticulado finito e complementado de L. Como $[0,a]$ é distributivo, então cada elemento deste intervalo tem um único complementar que pertence também ao intervalo. Se

$$0 = v_o < v_1 < v_2 < \ldots < v_k = a$$

é maximal, como cada v_t tem complementar único em $[0, v_{t+1}]$, visto que $[0,a]$ é relativamente complementado e os complementos relativos são únicos, o corolário da última proposição nos assegura que

$$\mu(0,a) = \mu(v_o, v_k) = (-1)^k$$

Em particular, se L é finito e possui exatamente

n elementos v-irredutíveis $p_1, p_2, \ldots, p_n$, então arranjando esses elementos de modo que p_1 é minimal, p_2 é minimal entre os demais p_i e assim por diante, então

$$0 < p_1 < p_1 \vee p_2 < \ldots < p_1 \vee p_2 \ldots \vee p_n = 1$$

é maximal e portanto

$$\mu(0,1) = (-1)^n$$

onde $n = \ell(L)$ é o comprimento de L, posto que a condição de cadeia de Jordan-Holder se verifica neste caso.

(d) Mostremos que a função de Möbius no reticulado localmente finito e distributivo $(N^*, |)$, está relacionada com a função de Möbius $\tilde{\mu}$ da teoria dos números do seguinte modo: $\tilde{\mu}(b) = \mu(1,b)$, para todo $b \in N^*$.

Neste reticulado $a \wedge b = mdc(a,b)$ e $a \vee b = mmc(a,b)$. Assim, $a \in N^*$ é v-irredutível se, e somente se, $a = p^{\alpha}$, p primo, $\alpha \geq 1$. De fato. Na decomposição de a em fatores primos, se $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r} = p_1^{\alpha_1} \vee \ldots \vee p_r^{\alpha_r}$ se $r > 1$ e $p_i \neq p_j$ sempre que $i \neq j$, então a não é v-irredutível. Por outro lado, se $a = p^{\alpha} = b \vee c = mmc(b,c)$, então $b = p^{\alpha_1}$ e $c = p^{\alpha_2}$, do que decorre $\alpha = \max\{\alpha_1, \alpha_2\}$ e portanto $\alpha = \alpha_1$ (daí $b = a$) ou $\alpha = \alpha_2$ (daí $c = a$).

Seja $b = p_1 p_2 \ldots p_r$ onde os p_i são primos distintos entre si. Então $[1,b]$ é finito e para cada $a = p_{i_1} p_{i_2} \ldots p_{i_k} \in [1,b]$ existe o complementar relativo de a neste intervalo: é $c = p_{j_1} p_{j_2} \ldots p_{j_t}$, onde os fatores primos são aqueles de b que não estão em a. Além disso os elementos v-irredutíveis de $[1,b]$ são $p_1, p_2, \ldots, p_r$. Donde

$$\mu(1,b) = (-1)^r = \tilde{\mu}(b)$$

Se $b = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, onde algum $\alpha_i > 0$, en

tão embora $[1,b]$ seja finito, o elemento $p_i \in [1,b]$ não admite complementar em $[1,b]$. De fato, se $mmc(p_i,x) = b = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, então $p_i^{\alpha_i}$ é fator de x e daí $mdc(p_i,x) = p_i \neq 1$. Portanto

$$\mu(1,b) = 0 = \tilde{\mu}(b)$$

7. Álgebras de Incidência Reduzidas.

Seja A(P) a álgebra de incidência sobre o conjunto parcialmente ordenado e localmente finito P e consideremos

$$B(P) = \{f \in A(P) \mid f(m,n) = f(r,s), \text{ sempre que } [m,n] \simeq [r,s]\}$$

Nessas condições pode-se provar sem dificuldades que B(P) é uma subálgebra de A(P). À subálgebra B(P) damos o nome de subálgebra de incidência reduzida de A(P). É claro que B(P) é unitária.

Seja $f \in B(P)$ e suponhamos $f(x,x) \neq 0$ para algum $x \in P$. Como $[y,y] \simeq [x,x]$, para todo $y \in P$, então $f(y,y) \neq 0$ para qualquer $y \in P$, e portanto f é inversível em A(P). Seja g a inversa de f. Para todo par $[x,x], [y,y]$ de intervalos unitários:

$$g(x,x) = \frac{1}{f(x,x)} = \frac{1}{f(y,y)} = g(y,y)$$

Sejam $[r,s]$ e $[x,y]$ intervalos isomorfos e suponhamos $g(x,u) = g(r,v)$ sempre que $x \leq u < y$, $r \leq v < s$ e $[x,u] \simeq [r,v]$. Então

$$g(r,s) = -\sum_{r \leq v < s} g(r,v) f(v,s) \frac{1}{f(s,s)} = -\sum_{x \leq u < y} g(x,u) f(u,y) \frac{1}{f(y,y)} = g(x,y)$$

Assim concluimos que $f \in B(P)$ é inversível se, e somente se, $f(x,x) \neq 0$, para algum $x \in P$.

Proposição 15. Os elementos não inversíveis de B(P) formam um ideal bilateral I (logo B(P) é local) e $B(P)/_I \simeq C$.

Demonstração. Se $f,g \in I$ é claro que $f-g \in I$. Se $f \in I$ e $g \in B(P)$, então $f(x,x) = 0$ para todo $x \in P$ e daí $(f*g)(x,x) = f(x,x)g(x,x) = 0$, sempre que $x \in P$, vale dizer, $f*g \in I$. Obviamente $g*f \in I$.

Notemos que: $f+I = g+I \iff f-g \in I \iff \forall\, x \in P : (f-g)(x,x) = 0 \iff \forall\, x \in P: f(x,x) = g(x,x)$. Isto mostra que $f+I \overset{\phi}{\longmapsto} f(x,x)$ é uma função injetora. Mas também é sobrejetora posto que, para todo $k \in C$, considerando $f: P \times P \to C$ definida por $f(x,y) = k$, sempre que $x \leq y$ e $f(x,y) = 0$ caso contrário, então é claro que $f \in B(P)$ e que $\phi(f+I) = f(x,x) = k$.

É imediato, além disso, verificar que ϕ é um homomorfismo de álgebras, o que vem concluir a demonstração.

Exemplos.

(I) Em N consideremos a relação de ordem usual $\leq$ para a qual $[m,n] \simeq [r,s]$ equivale a $n-m = s-r$. Para cada $f \in B(N)$ façamos $f(0,k) = a_k$, $\forall\, k \in N$. Obviamente, então, se $m \leq n$

$$f(m,n) = f(0,n-m) = a_{n-m}$$

Assim, a cada $f \in B(N)$ está associada uma única sequência (a_k) de elementos de C, onde $a_k = f(0,k)$. Se ϕ indica a aplicação definida por $\phi(f) = (a_k)$, então além de ϕ ser obviamente um homomorfismo de espaços vetoriais, supondo $f,g \in B(N)$, $\phi(f) = (a_k)$, $\phi(g) = (b_k)$ e $\phi(f*g) = (c_k)$, então $c_k = (f*g)(0,k) = \sum_{0 \leq r \leq k} f(0,r)g(r,k) =$

$$= \sum_{0 \leq r \leq k} f(0,r)g(0,k-r) = \sum_{0 \leq r \leq k} a_r\, b_{k-r} = \sum_{r+s=k} a_r\, b_s$$

Por outro lado, se $\phi(f) = (a_k) = 0$ (sequência nula), então sempre que $m \leq n$

$$f(m,n) = f(0,n-m) = a_{n-m} = 0$$

e portanto $f = 0$. Como ϕ é óbviamente sobrejetora, podemos a esta altura garantir que ϕ é um isomorfismo de álgebras, isto é

$$B(N) \simeq C[[t]]$$

Notemos que neste isomorfismo a função zeta está representada pela série formal

$$1 + t + t^2 + \ldots$$

visto que $\zeta(0,0) = \zeta(0,1) = \zeta(0,2) = \ldots = 1$. Consequentemente a função de Möbius pode no caso ser expressa por

$$(1 + t + t^2 + \ldots)^{-1} = 1 - t$$

(II) Em N^* consideremos a relação de ordem parcial definida por $x|y$. Neste caso $B(N^*)$ é isomorfa à álgebra de Dirichlet sobre C, ou seja, à álgebra das sequencias

$$(a_1, \frac{a_2}{2^s}, \frac{a_3}{3^s}, \ldots)$$

com a adição de sequencias e a multiplicação de sequencias por escalares definidas de maneira usual e o produto

$$(\frac{a_k}{k^s}).(\frac{b_k}{k^s}) = (\frac{c_s}{k^s})$$

onde $c_k = \sum_{u|k} a_u\, b_{k:u}$

Neste caso $[m,n] \simeq [r,s]$ equivale a $n:m = s:r$. Em vista disso, se para cada $f \in B(N^*)$ fizermos $f(m,n) = a_k$, sempre que $n:m = k$, então

$$\phi(f) = (a_k), \text{ onde } a_k = f(1,k), \quad k \geq 1$$

define uma função bijetora que preserva as estruturas de espaço vetorial subjacentes em seu domínio e contradomínio. Ademais, para quaisquer $f,g \in B(N^*)$, se $\phi(f) = (a_k)$, $\phi(g) = (b_k)$ e $\phi(f*g) = (c_k)$, então

$$c_k = (f*g)(1,k) = \sum_{1|u|k} f(1,u)g(u,k) = \sum_{u|k} f(1,u)g(1,k:u) = \sum_{u|k} a_u\, b_{k:u}$$

Calculemos agora $\phi(f)\phi(g)$. Fazendo

$$(a_k) = (\frac{a'_k}{k^s}) \quad \text{e} \quad (b_k) = (\frac{b'_k}{k^s})$$

temos:

$$\phi(f)\phi(g) = (\frac{a'_k}{k^s})(\frac{b'_k}{k^s}) = (\frac{\sum_{u|k} a'_u\, b'_{k:u}}{k^s})$$

Como porém $a'_u = u^s\, a_u$ e $b'_{k:u} = (k:u)^s\, b_{k:u}$, então

$$\frac{\sum_{u|k} a'_u\, b'_{k:u}}{k^s} = \frac{\sum_{u|k} a_u\, b_{k:u}\, u^s (k:u)^s}{k^s} = \sum_{u|k} a_u\, b_{k:u} = c_k$$

Assim, efetivamente: $\phi(f*g) = \phi(f)\phi(g)$.

Segundo os procedimentos usuais é possível escrever

$$\left(\frac{a_k}{k^s}\right) = a_1 + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \ldots$$

para cada elemento da álgebra de Dirichlet. Isto posto, a função zeta pode ser representada no caso por

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots = \sum_{n=1}^{\infty} n^{-s}$$

visto que $\zeta(1,1) = \zeta(1,2) = \zeta(1,3) = \ldots = 1$. Quanto à função de Möbius, sua expressão será

$$\sum_{n=1}^{\infty} u(1,n)\, n^{-s}$$

Estes resultados eram de esperar, obviamente, considerando a teoria dos números.

(III) Seja β a álgebra booleana de todos os subconjuntos finitos de um dado conjunto infinito enumerável S. Mostremos que neste caso a álgebra de incidência reduzida é isomorfa à álgebra exponencial das sequências (a_k), $k \geq 0$, $a_k \in C$, onde a adição e o produto por escalares são definidos da maneira usual e o produto

$$(a_o, a_1, \ldots)(b_o, b_1, \ldots) = (c_o, c_1, \ldots)$$

por

$$c_k = \sum_{u=o}^{k} \binom{k}{u} a_u\, b_{k-u}$$

Para cada elemento (a_k) desta álgebra é possível, de maneira única, a representação

$$(a_o, a_1, a_2, \ldots) = a_o + \frac{a_1}{1!}\, t + \frac{a_2}{2!}\, t^2 + \ldots$$

De fato, se fizermos $(0,1,0,0,\ldots) = t$, então $t^2 = (0,0,2!,0,\ldots)$, $t^3 = (0,0,0,3!,0,\ldots)$, ... Daí

$$\frac{t^2}{2!} = (0,0,1,0,\ldots); \quad \frac{t^3}{3!} = (0,0,0,1,0,\ldots), \ \ldots$$

o que acarreta

$$(a_o, a_1, a_2,\ldots) = a_o(1,0,0,\ldots) + a_1(0,1,0,0,\ldots) + a_2(0,0,1,0,\ldots) + \ldots$$

$$= a_o + \frac{a_1}{1!}\, t + \frac{a_2}{2!}\, t^2 + \ldots$$

Neste caso, $[A,B] \simeq [C,D]$ equivale a $|B-A| = |D-C|$. Assim, se para cada par $A \subset B$ de subconjuntos de S fizermos

$$f(A,B) = a_k \ , \quad \text{se} \quad |B-A| = k$$

então $f \mapsto (a_k)$ define um isomorfismo conforme o que afirmamos inicialmente. Verifiquemos apenas que os produtos se conservam nessa correspondência. De fato, se $f \mapsto (a_k)$, $g \mapsto (b_k)$ e $f*g \mapsto (c_k)$ e se $A_k \subset S$ tem cardinal k, então

$$c_k = (f*g)(\emptyset, A_k) = \sum_{X \subset A_k} f(\emptyset,X)\, g(X, A_k) = \sum_{X \subset A_k} f(\emptyset,X)\, g(\emptyset, A_k - X)$$

Ora, nesta última somatória, cada subconjunto $X \subset A_k$ pode ter cardinalidade de 0 a k e o número de subconjuntos de A_k com uma dada cardinalidade u $(0 \leq u \leq k)$ é $\binom{k}{u}$. Daí

$$c_k = \sum_{u=o}^{k} \binom{k}{u} a_u\, b_{k-u}$$

Neste caso é imediato que a função zeta pode ser expressa como

$$1 + \frac{t}{1!} + \frac{t^2}{2!} + \ldots = e^t$$

e consequentemente a função de Möbius por

$$e^{-t} = 1 - \frac{t}{1!} + \frac{t^2}{2!} - \frac{t^3}{3!} + \ldots$$

CAPÍTULO III

COÁLGEBRAS EM COMBINATÓRIA

1. Coálgebras.

Uma coálgebra é uma terna (C,Δ,ε), onde C é um espaço vetorial sobre um corpo K de característica zero, $\Delta: C \to C \otimes C$ e $\varepsilon: C \to K$ são K-homomorfismos de espaços vetoriais, e são comutativos os diagramas

$$\begin{array}{ccc} C \otimes C \otimes C & \xleftarrow{I \otimes \Delta} & C \otimes C \\ \uparrow{\scriptstyle \Delta \otimes I} & & \uparrow{\scriptstyle \Delta} \\ C \otimes C & \xleftarrow{\Delta} & C \end{array} \qquad \begin{array}{ccccc} C \otimes K & \xleftarrow{I \otimes \varepsilon} & C \otimes C & & \\ & \nwarrow^{\simeq} \quad \nearrow & & & \\ & C & & & \\ & \swarrow_{\simeq} \quad \searrow & & & \\ K \otimes C & & \xleftarrow{\varepsilon \otimes I} & & C \otimes C \end{array}$$

onde I indica, óbviamente, a aplicação idêntica de C. Os homomorfismos Δ e ε são designados, respectivamente, comultiplicação e counidade da coálgebra. Os diagramas anteriores traduzem, respectivamente, as propriedades coassociativa e counitária.

Exemplo.

Seja P um conjunto parcialmente ordenado e localmente finito para a relação indicada por $\leqslant$. Seja $T = \{(x,y) \in P \times P \mid x \leqslant y\}$ e indiquemos por V um espaço vetorial que admite T como base. Se definimos Δ e ε por

$$\Delta(x,z) = \sum_{x \leqslant y \leqslant z} (x,y) \otimes (y,z)$$

e

$$\varepsilon(x,y) = \begin{cases} 0 & \text{se } x \neq y \\ 1 & \text{se } x = y \end{cases}$$

então (V,Δ,ε) é uma coálgebra.

Um subespaço vetorial W de C se diz uma subcoálgebra de C se $\Delta(W) \subset W \otimes W$. Se J é um subespaço vetorial de C e se

$$\Delta(J) < J \otimes C + C \otimes J \quad \text{e} \quad \varepsilon(J) = 0$$

dizemos que J é um coideal em C.

Seja (C,Δ,ε) uma coálgebra e consideremos o dual de C: $C^* = \mathrm{Hom}_k(C,K)$. Se $M: C^* \times C^* \to C^*$ e $\lambda: K \to C^*$ são respectivamente, as compostas

$C^* \otimes C^* \xrightarrow{\rho} (C \otimes C)^* \xrightarrow{\Delta^t} C^*$ e $K \longrightarrow K^* \xrightarrow{\varepsilon^t} C^*$ onde $\rho(f \underset{K}{\otimes} g) = f \otimes g$, $K \to K^*$ é o isomorfismo natural, Δ^t a transposta de Δ e ε^t a de ε, pode-se mostrar que (C^*,M,λ) é uma álgebra, à qual damos o nome de álgebra dual da coálgebra dada.

Sejam $(C,\Delta_C,\varepsilon_C)$ e $(D,\Delta_D,\varepsilon_D)$ coálgebras e $g: C \to D$ uma transformação linear. Dizemos que g é um homomorfismo de coálgebras se são comutativos os seguintes diagramas

$$\begin{array}{ccc} C & \xrightarrow{g} & D \\ {\scriptstyle\Delta_C}\downarrow & & \downarrow{\scriptstyle\Delta_D} \\ C \otimes C & \xrightarrow[g \otimes g]{} & D \otimes D \end{array} \qquad \begin{array}{ccc} C & \xrightarrow{g} & D \\ & {\scriptstyle\varepsilon_C}\searrow \quad \swarrow{\scriptstyle\varepsilon_D} & \\ & K & \end{array}$$

Pode-se mostrar que se $g: C \to D$ é um homomorfismo de coálgebras, então $g^t: D^* \to C^*$ é um homomorfismo de álgebras.

Seja V um espaço vetorial sobre um corpo K. Se V é simultâneamente, uma álgebra e uma coálgebra (com comultiplicação Δ e counidade ε) e se Δ e ε são homomorfismos de álgebras, dizemos que V é uma biálgebra.

2. Coeficientes de Secção.

Seja A um conjunto não vazio e seja

$$(i,j,k) \longmapsto (i|j,k) \in Z$$

uma aplicação definida em $A \times A \times A$ e satisfazendo às condições:

(s_1) para todo $i \in A$ é finito o conjunto dos pares j,k para os quais $(i|j,k) \neq 0$;

(s_2) $\sum_k (i|j,k)(k|p,q) = \sum_s (i|s,q)(s|j,p)$;

(s_3) existe uma aplicação $\xi: A \to R$ tal que

$\sum_j (i|j,k)\xi(j) = \delta_{ik}$ e $\sum_k (i|j,k)\xi(k) = \delta_{ij}$

Nessas condições damos o nome de coeficientes de de secção aos elementos $(i|j,k)$ do conjunto das imagens, através da aplicação considerada.

Se, ademais, vale a condição

(s_4) $(i+j|p,q) = \sum_{p_1+p_2=p;\, q_1+q_2=q} (i|p_1,q_1)(j|p_2,q_2)$

o que pressupõe em A uma certa adição, então esses coeficientes são chamados coeficientes de bissecção.

Por exemplo, os coeficientes binomiais definidos sobre N por

$$(n|j,k) = \begin{cases} \frac{n!}{j!k!} & \text{se } j+k = n \\ 0, & \text{caso contrário} \end{cases}$$

formam uma coleção de coeficientes de bissecção, bastando definir $\xi: N \to R$ assim: $\xi(0) = 1$ e $\xi(n) = 0$, sempre que $n > 0$. Notemos que neste exemplo a condição (s_4) é consequência da convolução de Vandermonde

$$\binom{i+j}{p} = \sum_{p_1+p_2=p} \binom{i}{p_1}\binom{j}{p_2}$$

Cada coleção de coeficientes de secção sobre A dá origem a uma coálgebra da maneira que mostraremos a seguir. Seja $C = R^{(A)}$, cuja base canônica indicaremos por $(x_i)_{i\in A}$, e consideremos as transformações lineares $\Delta: C \to C \otimes C$ e $\varepsilon: C \to R$ definidas por

$$\Delta(x_i) = \sum_{j,k} (i|j,k)x_j \otimes x_k$$

e $\varepsilon(x_j) = \xi(j)$, onde ξ é a função cuja existência é assegurada por (s_3). A verificação das propriedades coassociativa e counitária se baseia, de maneira natural, nas condições (s_1), (s_2) e (s_3).

Se consideramos sobre um conjunto A, munido de alguma adição, uma coleção de coeficientes de bissecção e definimos o produto em C através de $x_i x_j = x_{i+j}$, para quaisquer $i,j \in A$, com as hipóteses do parágrafo anterior a respeito de $(x_i)_{i\in A}$, então C apresenta uma estrutura de biálgebra.

3. Coálgebras de Incidência.

(3.1) Seja P um conjunto parcialmente ordenado e localmente finito mediante a relação indicada por $\leqslant$. Sobre o conjunto dos intervalos $[x,y]$ podemos definir uma coleção de coeficientes de secção do seguinte modo:

$$([x_1,x_2]\,|\,[y_1,y_2],[z_1,z_2]) = \begin{cases} 1 & \text{se } x_1=y_1,\ x_2=z_2 \text{ e } y_2=z_1 \\ 0, & \text{caso contrário} \end{cases}$$

$$\text{e } \xi([x,y]) = \begin{cases} 1 & \text{se } x = y \\ 0 & \text{se } x \neq y \end{cases}$$

Com as identificações usuais, a comultiplicação e a counidade que dão origem à coálgebra obtida através desses coeficientes são obviamente definidas por

$$\Delta([x,y]) = \sum_{x\leqslant z\leqslant y} [x,z] \otimes [z,y]$$

$$\varepsilon([x,y]) = \begin{cases} 1 & \text{se } x = y \\ 0 & \text{se } x \neq y \end{cases}$$

A coálgebra assim obtida, que indicaremos por C(P), é chamada coálgebra de incidência de P.

Nem sempre se lidam com as coálgebras de incidência planas, no sentido acima, mas apenas com certos quocientes obtidos de C(P) mediante relações de equivalência convenientes. Obtemos então as coálgebras de incidência reduzidas.

Uma relação de equivalência ~ sobre o conjunto dos segmentos de P se diz ordem-compatível se é um coideal em C(P) o

conjunto

$$H = \{[x,y] - [u,v] \mid [x,y] \sim [u,v]\}$$

Pode-se provar que se, para todo par de segmentos $[x,y]$ e $[u,v]$ equivalentes segundo $\sim$, existe uma bijeção $\phi:[x,y] \to [u,v]$, dependendo em geral de $[x,y]$, de maneira que $[x_1,y_1] \sim [\phi(x_1),\phi(y_1)]$, para quaisquer x_1,y_1, $x \leqslant x_1 \leqslant y_1 \leqslant y$, então $\sim$ é ordem-compatível.

Se $\sim$ é ordem compatível sobre o conjunto dos segmentos de P, então existe uma única estrutura de coálgebra sobre o espaço vetorial $C(P)/H$ de maneira que o homomorfismo canônico

$$\pi: C(P) \to C(P)/H$$

é um homomorfismo de coálgebras. A comultiplicação Δ neste caso está definida por

$$\Delta([x,z] + H) = \sum_{x \leqslant y \leqslant z} ([x,y] + H) \otimes ([y,z] + H)$$

ao passo que a counidade ε é dada por

$$\varepsilon([x,y] + H) = \varepsilon([x,y])$$

onde ε, no segundo membro, é a counidade de $C(P)$.

Cada classe de equivalência de $C(P)/H$ é chamada tipo. Se α indica um tipo, pela notação x_α se denota uma representação indistinta de α. Assim, se α, β e γ são tipos e se $(\alpha|\beta,\gamma)$ indica o número de elementos $z \in [x,y]$, distintos entre si, de maneira que $[x,y] + H$, $[x,z] + H$ e $[z,y] + H$ são do tipo α, β e γ, respectivamente, então a fórmula que exprime Δ passa a se escrever assim

$$\Delta x_\alpha = \sum_{\beta,\gamma} (\alpha|\beta,\gamma) x_\beta \otimes x_\gamma$$

Os números $(\alpha|\beta,\gamma)$ assim obtidos formam uma coleção de coeficientes que satisfazem (s_1) e (s_2).

Se a relação definida sobre o conjunto dos intervalos de P é o isomorfismo, conforme a teoria dos conjuntos, obtemos a chamada coálgebra de incidência reduzida padrão.

Exemplo 1.

Sobre N consideremos a relação de ordem usual. Então: $[x,y] \simeq [u,v] \iff y-x = v-u$. Mantidas as notações anteriores, como $[x,y] + H = [0,y-x] + H$, para todo intervalo $[x,y]$, então os tipos podem ser representados por

$$x_n = [0,n] + H \qquad (n = 0,1,2,\ldots)$$

Notemos que neste caso $(n|p,q) = 1$ se $p+q = n$ e $(n|p,q) = 0$ em caso contrário. Assim

$$\Delta x_n = \sum_{p+q=n} x_p \otimes x_q$$

ao passo que

$$\varepsilon(x_n) = \delta_{on} \qquad (n \geq 0)$$

A álgebra dual da coálgebra $C(N)/H$ é isomorfa à álgebra de incidência reduzida $B(N)$. De fato, se f e g são elementos dessa álgebra dual, mantidas as notações do item 1, temos

$$(\Delta^t \rho)(f \underset{K}{\otimes} g)(x_n) = \Delta^t(f \otimes g)(x_n) = (f \otimes g)\Delta(x_n) =$$

$$= (f \otimes g) \sum_{p+q=n} x_p \otimes x_q = \sum_{p+q=n} f(x_p) \otimes g(x_q)$$

Ou seja, com as notações simplificadas habituais:

$$(fg)(x_n) = \sum_{p+q=n} f(x_p)g(x_q)$$

Ou ainda, fazendo $f(x_k) = a_k$, $g(x_k) = b_k$ e $(fg)(x_k) = c_k$ $(k = 0,1,2,\ldots)$:

$$c_n = \sum_{p+q=n} a_p b_q$$

Exemplo 2.

Seja β a álgebra booleana dos subconjuntos finitos de N* em relação à inclusão. Então: $[A,B] \simeq [C,D] \iff |B-A| = |D-C|$. Usando a notação $X_n = \{1,2,\ldots, n\}$, então os tipos podem ser representados por

$$Y_n = [\emptyset, X_n] + H \qquad (n = 0,1,2,\ldots)$$

onde $X_o = \emptyset$. Como

$$\Delta([\emptyset, X_n] + H) = \sum_{X \subset X_n} ([\emptyset, X] + H) \otimes ([X, X_n] + H)$$

e para cada X_n, o número de subconjuntos de X_n de cardinal p é $\binom{n}{p}$, então

$$\Delta(Y_n) = \sum_{p=o}^{n} \binom{n}{p} Y_p \otimes Y_{n-p}$$

De fato, é claro que neste caso

$$(n|p,q) = \begin{cases} \binom{n}{p} & \text{se} \quad n = p+q \\ 0, & \text{caso contrário} \end{cases}$$

É óbvio então que a álgebra dual de $C(\beta)/H$ neste caso é isomorfa à álgebra de incidência reduzida $B(\beta)$. Aliás isto é obviamente mais geral: a álgebra dual de uma coálgebra de incidência reduzida padrão é isomorfa à álgebra de incidência reduzida correspondente ao mesmo conjunto parcialmente ordenado e localmente finito.

(3.2) A questão anterior pode ser situada num contexto ainda mais amplo.

Seja A um conjunto não vazio e seja

$$(i,j,k) \rightarrow (i|j,k) \in Z$$

uma função definida em A x A x A e que satisfaça às condições (s_1) e (s_2) do item 2. A álgebra de incidência associada à coleção de coeficientes assim obtidos é o espaço vetorial das funções de A em R (operações usuais) com a "multiplicação" definida por

$$(f*g)(i) = \sum_{j,k} (i|j,k) f(j) g(k)$$

É fácil ver que se trata de álgebras associativas, em virtude de (s_2). Se usarmos a notação $i = j \oplus k$ para indicar que $(i|j,k) \neq 0$, então

$$(f*g)(i) = \sum_{j \oplus k = i} (i|j,k) f(j) g(k)$$

Por exemplo, no conjunto N podemos considerar a coleção de coefi

cientes definidos assim:

$$(i|j,k) = \begin{cases} 1 & \text{se } j+k = i \\ 0\ , & \text{caso contrário} \end{cases}$$

Trata-se neste caso da álgebra B(N), visto que

$$(f*g)(i) = \sum_{k+j=i} f(j)f(k)$$

Sempre que $(i|j,k) = 1$ quando $i = j \oplus k$, nos referiremos à álgebra de incidência respectiva como usual para a coleção considerada.

Supondo verificadas as condições (s_1), (s_2) e (s_3) para uma coleção de coeficientes sobre A e considerando a coálgebra relativa a essa coleção, então a álgebra dual desta coálgebra é isomorfa à álgebra de incidência associada à mesma coleção. A cada $f: R^{(A)} \to R$ do dual associemos $\hat{f}: A \to R$ definida por $\hat{f}(i) = f(x_i)$, para todo x_i da base canônica de $R^{(A)}$. É imediato verificar que se trata de um isomorfismo de espaços vetoriais. Para mostrar que conserva as multiplicações notemos que

$$(fg)(x_i) = \Delta^t(f \otimes g)(x_i) = (f \otimes g)\Delta(x_i) =$$

$$= (f \otimes g) \sum_{j \oplus k=i} (i|j,k)x_j \otimes x_k = \sum_{j \oplus k=i} (i|j,k)f(x_j) \otimes g(x_k) =$$

$$= \sum_{j \oplus k=i} (i|j,k)\hat{f}(j) \otimes \hat{g}(k) = (\hat{f} * \hat{g})(i)$$

(3.3) Vejamos agora uma interpretação combinatória do que acabamos de ver. Seja C(P) a coálgebra de incidência de um conjunto parcialmente ordenado e localmente finito P. Então C(P)* é isomorfa à álgebra de incidência associada à coleção de coeficientes definidos em (3.1). Em particular, se f, g são duas funções desta álgebra

$$(f*g)[x,y] = \sum_{x \leq z \leq y} f([x,z])g([z,y])$$

e, por indução

$$f^{n+1}[x,y] = \Sigma f[x,z_1]f[z_1,z_2] \ldots f[z_n,y] \qquad (*)$$

onde a somatória é estendida a todas as sequencias $z_1, z_2, \ldots, z_n$ tais que $x \leqslant z_1 \leqslant z_2 \leqslant \ldots \leqslant z_n \leqslant y$.

Para a interpretação pretendida, se $x,y \in P$, $x \leqslant y$, chamemos de m-cadeia de comprimento n+2, de x a y, todo produto

$$[x,z_1] \mathbin{0} [z_1,z_2] \mathbin{0} \ldots \mathbin{0} [z_n,y]$$

onde $x \leqslant z_1 \leqslant z_2 \leqslant \ldots \leqslant z_n \leqslant y$. Cada um dos n+1 termos de uma dessas m-cadeias, inclusive os triviais $[a,a]$, são chamados elos.

Se $x,y \in P$, $x \leqslant y$, suponhamos que para cada elo $[a,b]$ de cada m-cadeia de x a y, de comprimento n+2, esteja associado um conjunto finito E(a,b) de etiquetas. Com as identificações de (3.2) podemos considerar o funcional $f \in C(P)^*$ definido de maneira que $f([a,b]) = |E(a,b)|$ para cada um desses elos e nulo nos demais intervalos de P. Nessas condições, considerando a identidade (*), podemos afirmar que $f^{n+1}[x,y]$ fornece o número de m-cadeias etiquetadas de comprimento n+2, de x a y.

Seja G um reticulado geométrico finito e seja $[x,y]$ um intervalo em G. Suponhamos que se queira contar o número de m-cadeias de x a y, de dois elos, de maneira que os conjuntos de etiquetas associados a dois intervalos de mesma altura coincidam. Supondo $[x,y]$ de altura r, se $x \leqslant a \leqslant y$ e $[x,a]$ é de altura k, então $[a,y]$ é de altura r-k. Indiquemos por $\begin{bmatrix} r \\ k \end{bmatrix}$ o número de m-cadeias $[x,a] \mathbin{0} [a,y]$ de maneira que $[x,a]$ é de altura k e $[a,y]$ de altura r-k. Se f_r indica a função etiquetagem, como no parágrafo anterior, se o primeiro elo pode ser etiquetado de a_k maneiras ($a_k = f_r(x,a)$) e o segundo de a_{r-k} maneiras, então

$$f_r^2[x,y] = \sum_{k=o}^{r} \begin{bmatrix} r \\ k \end{bmatrix} a_k \, a_{n-k}$$

Por exemplo, no reticulado $L(V_n)$, se $\binom{n}{k}_q$ indica o número de subespaços de V_n de dimensão k, então

$$f_r^2[x,y] = \sum_{k=o}^{r} \binom{r}{k}_q a_k \, a_{n-k}$$

4. A Coálgebra de Dirichlet.

(4.1). Construção.

Consideremos N* ordenado pela relação da divisibilidade. A coálgebra de incidência reduzida padrão neste caso recebe o nome de coálgebra de Dirichlet. Evidentemente temos então

$$[x,y] \simeq [u,v] \iff y : x = v : u$$

e como consequencia, mantidas as notações anteriores: $[x,y] + H = [0,y : x] + H$ para qualquer intervalo $[x,y]$. Mais ainda, se fizermos

$$[1,n] + H = e_n \qquad (n = 1,2,\ldots)$$

os e_n formam obviamente uma representação completa dos tipos desta coálgebra. Observando que

$$[1,p] + H = [1,q] + H \iff p = q$$

então os coeficientes $(n|r,s)$ não nulos são todos iguais a 1 e daí

$$\Delta(e_n) = \sum_{pq=n} e_p \otimes e_q$$

e $\varepsilon(e_n) = \delta_{n1}$ $(n = 1,2,\ldots)$ definem, respectivamente a comultiplicação e o homomorfismo counitário da coálgebra de Dirichlet.

(4.2). A álgebra dual da coálgebra de Dirichlet.

Indiquemos por V simplesmente, daqui por diante, a coálgebra de Dirichlet. Como já observamos no final do item 3 o dual de V, $V^* = L(V,R)$, pode ser dotado, de maneira natural, de uma estrutura de álgebra isomorfa à álgebra de incidência reduzida $B(N^*)$. A multiplicação de funcionais de V^* está definida por

$$(gh)(e_n) = \sum_{pq=n} g(e_p)h(e_q)$$

para quaisquer $f,g \in V^*$ e para todo $n \geq 1$. Esta álgebra é associativa, comutativa e unitária, sendo sua unidade o funcional $w : V \to K$ definido por $w(e_n) = \delta_{n1}$ $(n \geq 1)$. Notemos que a multiplicação assim obtida é uma generalização da convolução aritmética de Dirichlet.

(4.3) A estrutura de anel fatorial subjacente em V^*.

Definição 1. Seja $g \in V^*$ um funcional não nulo. Damos o nome de ordem de g (notação: $0(g)$) ao menor número natural $n > 0$ tal que $g(e_n) \neq 0$.

É claro que para cada $n \in N^*$ existe $g \in V^*$ de maneira que $0(g) = n$. Também é evidente que $0(w) = 1$.

Proposição 1. Para quaisquer funcionais não nulos $g,h \in V^*$, se $0(g) = r$ e $0(h) = s$, então $0(gh) = rs$.

Demonstração. Mostremos primeiro que $(gh)(e_{r+s}) = \sum_{pq=rs} g(e_p)h(e_q) = g(e_r)h(e_s) \neq 0$. De fato, se $p < r$, então $g(e_p) = 0$ e se $p > r$, então $p > 1$ e $q < s$ o que implica $h(e_q) = 0$. Como $p = r$ acarreta $q = s$, fica provada esta primeira afirmação. Vejamos agora que $(gh)(e_n) = 0$, sempre que $n < rs$ o que concluirá a demonstração. Como

$$(gh)(e_n) = \sum_{pq=n} g(e_p)h(e_q)$$

para $p < r$ se tem $g(e_p) = 0$ e para $p \geq r$, como então $p^{-1} \leq r^{-1}$ e daí $q = np^{-1} \leq nr^{-1} < s$, então $h(e_q) = 0$.

Corolário. O anel V^* não possui divisores próprios do zero.

Demonstração. Se g e h são elementos não nulos de V, se $0(g) = r$ e $0(h) = s$, então $(gh)(e_{r+s}) \neq 0$ e portanto $gh \neq 0$.

Como é usual na teoria dos anéis, se $g,h \in V^*$, a notação $g|h$ indica que g divide h, isto é, que existe $f \in V^*$ de maneira que $h = gf$. Se $g|h$ e $h|g$ então g e h se dizem associados, o que indicaremos por $g \approx h$.

Proposição 2. Sejam $g,h \in V^*$ funcionais não nulos. Então: $g|h$ se, e somente se, $0(g)|0(h)$.

Demonstração.

($\rightarrow$) Por hipótese existe $f \in V^*$ de maneira que $h = gf$. Donde $0(h) = 0(g)0(f)$, o que garante a tese.

($\leftarrow$) Façamos $0(g) = r$ e $0(h) = s$. Por hipótese existe $k \in N^*$ de maneira que $s = rk$. Como o funcional f, cuja existência queremos provar, satisfazendo $h = gf$, deve ter ordem k, devemos impor que $f(e_1) = \ldots = f(e_{k-1}) = 0$. Observemos que

$$h(e_s) = (gf)(e_s) = \sum_{pq=s} g(e_p)f(e_q)$$

Quando $p < r$ vale $g(e_p) = 0$; quando $p > r$, então $p^{-1} < r^{-1}$ e daí $sp^{-1} < sr^{-1}$, ou seja, $q < k$ o que implica $f(e_q) = 0$. Assim $h(e_s) = g(e_r)f(e_k)$ e portanto

$$f(e_k) = h(e_s).(g(e_r))^{-1}$$

o que define univocamente $f(e_k)$.

Suponhamos agora que $f(e_n)$ seja conhecido, sempre que $n \leq k+i$ $(i \geq 1)$, e mostremos então que $f(e_{k+i})$ pode ser determinado de uma única maneira. Considerando

$$(gf)(e_{s+ri}) = \sum_{pq=s+ri} g(e_p)f(e_q)$$

observemos as seguintes situações

. $p < r \Longrightarrow g(e_p) = 0$

. $p = r \Longrightarrow q = (s+ri)p^{-1} = sr^{-1} + i = k + i$ o que implica $g(e_p) = g(e_r)$ e $f(e_q) = f(e_{k+i})$

. $p > r \Longrightarrow p^{-1} < r^{-1} \Longrightarrow q = (s+ri)p^{-1} < (s+ri)r^{-1} = k + i$ o que mostra que todos os $f(e_q)$ são conhecidos neste caso.

Levando em conta essas conclusões:

$$(gf)(e_{s+ri}) = g(e_r)f(e_{k+i}) + \sum_{pq=r+si,\,p>r} g(e_p)f(e_q)$$

Donde

$$f(e_{k+i}) = (g(e_r))^{-1}.\left[h(e_{s+ri}) - \sum_{pq=s+ri,\,p>r} g(e_p)f(e_q)\right]$$

o que fornece univocamente $f(e_{k+i})$ em função dos valores já conhe

cidos.

Corolário 1. Seja $h \in V^*$ um funcional não nulo. Então: h é inversível se, e somente se, $0(h) = 1$.

Demonstração.

($\rightarrow$) Por hipótese existe $g \in V^*$ de maneira que $w = hg$. Daí $1 = 0(h)0(g)$ e então $0(h) = 1$.

($\leftarrow$) Se $0(h) = 1$, então $0(h) \mid 0(w)$ e portanto $h \mid w$.

Corolário 2. Para quaisquer elementos não nulos $h,g \in V^*$: $h \approx g \iff 0(h) = 0(g)$.

Corolário 3. Seja $h \in V^*$, $h \neq 0$ e h não inversível. Então: h é irredutível se, e somente se, $0(h)$ é um número primo.

Demonstração.

($\rightarrow$) Suponhamos por absurdo que $h \in V^*$ seja irredutível e $0(h) = rs$ ($r,s \in N$, $r > 1$ e $s > 1$). Considerando um elemento $g \in V^*$ de ordem r, então $g \mid h$ e g não é inversível, pois $0(g) > 1$.

($\leftarrow$) Suponhamos $h = gf$, com $g,f \in V^*$ não inversíveis. Então $0(h) = 0(g)0(f)$, onde $0(g) > 1$ e $0(f) > 1$, o que é absurdo, visto que $0(h)$ é por hipótese um número primo.

Proposição 3. Seja $h \in V^*$ um funcional não nulo. Então: h é primo se, e somente se, h é irredutível.

Demonstração. Precisamos provar apenas que se h é irredutível, então h é primo. Suponhamos $g,f \in V^*$ e que $h \mid fg$. Então $0(h) \mid 0(f)0(g)$ e daí $0(h) \mid 0(f)$ ou $0(h) \mid 0(g)$, posto que $0(h)$ é um número primo. Donde $h \mid f$ ou $h \mid g$.

Lema 1. Seja $h \in V^*$ um funcional não nulo e não inversível. Suponhamos que g é um divisor não trivial de h e que qualquer outro divisor de h, não associado a g, tem ordem maior

que a de g. Então g é irredutível.

Demonstração. Suponhamos $g = f_1 f_2$ uma decomposição não trivial de g em V* o que implica $0(f_1) < 0(g)$. Por outro lado, como $g|h$, então $h = gf_3$, onde $f_3 \in V^*$. Donde $h = f_1(f_2 f_3)$ e $f_1|h$ o que acarreta, considerando a hipótese, que $0(f_1) = 0(g)$ (se $f_1 \simeq g$) ou $0(f_1) > 0(g)$. Em ambos os casos temos uma contradição.

Dos resultados anteriores decorre, de maneira análoga a todas as situações semelhantes, a

Proposição 4. O anel de integridade subjacente a V* é fatorial.

Vejamos agora alguma coisa a respeito dos ideais em V*.

Lema 2. Seja $I = \langle f_1, f_2, \ldots, f_n \rangle$ um ideal finitamente gerado em V* e suponhamos $f_i \neq 0$, para todo i, $1 \leq i \leq n$. Então $I = V^*$ se, e somente se, existe um índice k, $1 \leq k \leq n$, de maneira que f_k é inversível.

Demonstração.

($\rightarrow$) Suponhamos $\langle f_1, f_2, \ldots, f_n \rangle = \langle w \rangle$ e, por absurdo, que $0(f_1) > 1, \ldots, 0(f_n) > 1$. Da igualdade $I = \langle w \rangle$ decorre que existem $g_1, \ldots, g_n \in V^*$ de modo que $w = f_1 g_1 + \ldots + f_n g_n$. Portanto

$$1 = w(e_1) = (f_1 g_1 + \ldots + f_n g_n)(e_1) =$$

$$= (f_1 g_1)(e_1) + \ldots + (f_n g_n)(e_1) = f_1(e_1) g_1(e_1) + \ldots + f_n(e_1) g_n(e_1) = 0$$

o que é impossível.

($\leftarrow$) Evidente.

Proposição 5. O anel de integridade subjacente a V* não é principal.

Demonstração. Admitamos que V* seja principal. Tomemos então $h_1, h_2 \in V^*$ irredutíveis, de maneira que $h_1 \not\sim h_2$, por

exemplo, $0(h_1) < 0(h_2)$. Com a hipótese feita somos levados à conclusão de que existe $g \in V^*$ para o qual se verifica $\langle h_1, h_2 \rangle = \langle g \rangle$ o que implica $g|h_1$ e $g|h_2$. Mas não podemos ter $g \simeq h_2$ pois isto implicaria $h_2|h_1$, o que é impossível. Sendo h_2 irredutível resta a conclusão de que g é inversível. Daí $\langle h_1, h_2 \rangle = \langle w \rangle$ e pelo lema ou h_1 ou h_2 deve ser inversível, o que é absurdo.

Proposição 6. O anel de integridade subjacente a V^* é semiprimo, local mas não é subdiretamente irredutível.

Demonstração. A primeira afirmação é imediata pois $\langle 0 \rangle$ é um ideal primo em V^*. Seja f um elemento não inversível de V^*. Como $f(e_1) = 0$, então, para todo $g \in V^*$: $(w-fg)(e_1) = w(e_1) - f(e_1)g(e_1) = 1$. Assim $w-fg$ é inversível para todo $g \in V^*$, o que garante que o radical de Jacobson de V^* é o conjunto dos elementos não inversíveis de V^*. Quanto à última afirmação, se existisse $f \in V^*$ não nulo em todos os ideais não nulos, então $f \in \langle h \rangle$ para todo h irredutível. Daí a ordem de f teria de ser maior que ou igual a todos os números primos, o que é impossível.

Observe-se que o fato de V^* ser local poderia ser deduzido também a partir da proposição 15, cap. II, considerando o último parágrafo de (3.1).

5. Álgebras e Coálgebras associadas a recobrimentos.

(5.1) Seja A um conjunto finito e não vazio e indiquemos por R(A) um recobrimento de A o qual suporemos formado de subconjuntos minimais em relação à inclusão.

Para todo $p \in A$, definamos como estrela de p (notação: st(p)) a união dos membros de R(A) que contem p. Se $X \subset A$, então a estrela de X, indicada st(X), é definida como

$$st(X) = \bigcup_{p \in X} st(p)$$

Obviamente: (i) $p \in st(p)$, $\forall p \in A$; (ii) $X \subset st(X)$, para todo $X \subset A$; (iii) $X \subset Y \subset A \Longrightarrow st(X) \subset st(Y)$; (iv) $st(X) \cup st(Y) = st(X \cup Y)$, para quaisquer $X, Y \subset A$; (v) $p \in st(q) \Longleftrightarrow q \in st(p)$. Para provar esta última, supondo $st(q) = A_1 \cup \ldots \cup A_k$, onde $A_1, \ldots, A_k$ são os membros da R(A) que contêm q, se $p \in st(q)$, então $p \in A_i$, para algum A_i $(1 \leq i \leq k)$. Daí se pode concluir que $A_i \subset st(p)$ e, como $q \in A_i$, então $q \in st(p)$. Uma estrela st(X) será chamada genericamente de estrela sobre A e o conjunto destas estrelas, associado ao recobrimento R(A), por St(A,R(A)).

Mostremos que, para cada conjunto finito A e para cada recobrimento R(A) desse conjunto, nas condições propostas, o conjunto St(A,R(A)) se torna um reticulado, em relação à inclusão, ao se definir

$S \wedge T$ = união das estrelas contidas em $S \cap T$

$S \vee T = S \cup T$

para quaisquer estrelas S e T sobre A. Observemos primeiro que $st(\emptyset) = \emptyset$. Assim, como uma união de estrelas é também uma estrela, podemos garantir que $S \wedge T \in St(A,R(A))$, sempre que $S,T \in St(A,R(A))$. Mostremos então que $S \wedge T = \inf \{S,T\}$. É evidente, primeiro, que $S \wedge T \subset S$ e $S \wedge T \subset T$. Agora, se L é uma estrela contida em S e em T, então $L \subset T \cap S$ e daí $L \subset T \wedge S$.

Os reticulados assim construidos não são em geral modulares e, por consequencia, não são distributivos, como mostra o seguinte exemplo. Sejam

$A = \{1,2,3,4,5\}$ e $R(A) = \{\{1\}; \{2,3\}; \{3,4\}; \{4,5\}\}$

Neste caso

$St(A,R(A)) = \{\emptyset, \{1\}; \{2,3\}; \{2,3,4\}; \{3,4,5\}; \{4,5\}; \{1,2,3\}; \{1,2,3,4\}; \{1,3,4,5\}; \{1,4,5\}; \{2,3,4\}; \{2,3,4,5\}; \{3,4,5\}; \{1,2,3,4,5\}\}$.

Considerando as estrelas $T = \{4,5\}$, $S = \{1,2,3,4\}$ e $L = \{3,4,5\}$,

então $T \subset L$ e

$$T \vee (S \wedge L) = T \vee \emptyset = T = \{4,5\}$$

ao passo que

$$(T \vee S) \wedge L = \{1,2,3,4,5\} \wedge \{3,4,5\} = \{3,4,5\}$$

(5.2) Consideremos um reticulado $St(A,R(A))$, conforme item anterior. Se X, Y e Z são subconjuntos de A, dizemos que X e Y formam uma cisão de Z se $X \cup Y = Z$ e $X \cap st(Y) = st(X) \cap Y = \emptyset$. Usaremos a notação $Z = X \oplus Y$ para indicar esta situação. Isto, aliás, é decorrência do fato que, em se definindo

$$(Z|X,Y) = \begin{cases} 1 & \text{se } X \oplus Y = Z \\ 0, & \text{caso contrário} \end{cases}$$

a coleção dos $(Z|X,Y)$, para quaisquer Z, X, Y subconjuntos de A, determina sobre $\mathcal{P}(A)$ uma estrutura de coeficientes de secção, como mostraremos.

. Para cada $Z \subset A$, o número de pares de conjuntos X e Y de $\mathcal{P}(A)$ tais que $(Z|X,Y) = 1$ é finito uma vez que A é finito.

. Para mostrar (s_2) basta verificar que o número de parcelas não nulas em $\sum_K (I|J,K)(K|P,Q)$ é o mesmo que em $\sum_S (I|S,Q)(S|J,P)$. Supondo $(I|J,K)(K|P,Q)$ uma parcela não nula da primeira somatória, então

$$I = J \cup K, \quad st(J) \cap K = J \cap st(K) = \emptyset$$

e

$$K = P \cup Q, \quad st(P) \cap Q = P \cap st(Q) = \emptyset$$

Fazendo $J \cup P = S$, então

$$st(P) \cap J \subset st(K) \cap J = \emptyset \quad \text{e} \quad st(J) \cap P \subset st(J) \cap K = \emptyset$$

o que garante que $(S|J,P) = 1$. Além disso:

$$S \cup Q = J \cup P \cup Q = J \cup K = I$$

$$st(S) \cap Q = (st(J) \cup st(P) \cap Q = (st(J) \cap Q) \cup (st(P) \cap Q) =$$

$$= st(J) \cap Q \subset st(J) \cap K = \emptyset.$$

$$S \cap st(Q) = (J \cup P) \cap st(Q) = (J \cap st(Q)) \cup (P \cap st(Q)) =$$

$= J \cap st(Q) \subset J \cap st(K) = \emptyset$

e portanto $(I|S,Q) = 1$. Estas considerações obviamente justificam a afirmação feita.

A esta altura já podemos falar da álgebra de incidência associada à coleção de coeficientes $(Z|X,Y)$ introduzidos da maneira acima: é o espaço vetorial das funções $f: \mathcal{P}(A) \to R$ dotado da multiplicação definida assim

$$(f*g)(Z) = \sum_{X \oplus Y = Z} f(X) f(Y)$$

. Ainda no caso em pauta, se definirmos $\xi: \mathcal{P}(A) \to R$ por $\xi(\emptyset) = 1$ e $\xi(X) = 0$, sempre que $X \neq \emptyset$, temos

$$\sum_J (I|J,K)\xi(J) = (I|\emptyset,K)$$

Mas, para que $(I|\emptyset,K) = 1$ é necessário e suficiente que $K = I$, $st(K) \cap \emptyset = K \cap st(\emptyset) = \emptyset$, o que equivale a $K = I$. Assim

$$\sum_J (I|J,K)\xi(I) = \delta_{IK}$$

De maneira análoga

$$\sum_K (I|J,K)\xi(K) = \delta_{IJ}$$

Nestas condições, se $C = R^{(\mathcal{P}(A))}$, cuja base canônica indicaremos por (x_I), onde I percorre $\mathcal{P}(A)$, considerando as identificações usuais e indicando por $\Delta: C \to C \otimes C$ e $\varepsilon: C \to R$ as transformações lineares definidas por

$$\Delta(I) = \sum_{J \oplus K = I} J \otimes K$$

$$\varepsilon(J) = \begin{cases} 1 & \text{se } J = \emptyset \\ 0, & \text{caso contrário} \end{cases}$$

então (C, Δ, ε) é a coálgebra de incidência associada aos coeficientes de secção $(I|J,K)$.

Como caso particular, se $A = \{1,2,\ldots,n\}$ e

$R(A) = \{\{1\}, \{2\}, \ldots, \{n\}\}$, então $st(r) = \{r\}$, para todo $r \in A$, e como consequencia: $T \in St(A,R(A)) \iff T \subset A$. Neste caso a coálgebra de incidência é a coálgebra booleana sobre A, onde

$$\Delta(Z) = \sum_{X \cap Y = \emptyset;\, X \cup Y = Z} X \otimes Y$$

e

$$\varepsilon(Z) = \begin{cases} 1 & \text{se } Z = \emptyset \\ 0 & \text{se } Z \neq \emptyset \end{cases}$$

para todo $Z \subset A$.

(5.3) Consideremos um reticulado $St(A,R(A))$, conforme o item (5.1). Um conjunto $X \subset A$ é chamado não-tomador se, para quaisquer $p,q \in X$, $p \neq q$, se tem $p \notin st(q)$ (e $q \notin st(p)$, como consequencia).

Lema. Sejam I, J e K subconjuntos de A tais que $K = I \oplus J$. Se $S \subset K$ é um conjunto não-tomador, então $S \cap I$ e $S \cap J$ também o são. Recíprocamente, se S é um subconjunto de I não-tomador e T é um subconjunto de J não tomador, então $S \cup T$ é um subconjunto não-tomador de K.

Demonstração. A primeira afirmação é imediata. Quanto à segunda, suponhamos que existam por absurdo, com as hipóteses feitas, $x,y \in S \cup T$ de maneira que $x \in st(y)$ e $y \in st(x)$. Obviamente não podemos ter $x,y \in S$ ou $x,y \in T$, uma vez que S e T são não-tomadores. Admitindo, por exemplo, $x \in S$, $y \in T$ e $x \in st(y)$, obtemos como consequencia que $x \in I$, $y \in J$ e $x \in st(y) \subset st(J)$. Donde $x \in I \cap st(J) = \emptyset$, o que é impossível.

Proposição 7. Para cada $S \subset A$ e para cada número natural n, indiquemos por $\binom{S}{n}$ o número de subconjuntos de S, não-tomadores, de cardinal n. Então, se I, J e W são subconjuntos de A para os quais $I \oplus J = W$, vale a igualdade

$$\binom{W}{n} = \sum_{k=o}^{n} \binom{I}{k} \cdot \binom{J}{n-k}$$

Demonstração. Seja $T \subset W$ um conjunto não-tomador de cardinal n. Pelo lema $T \cap I$ e $T \cap J$ são subconjuntos não-tomadores de I e J, respectivamente. Mas

$$(T \cap I) \cup (T \cap J) = T \cap (I \cup J) = T \cap W = T$$

e

$$(T \cap I) \cap (T \cap J) = T \cap (I \cap J) = T \cap \emptyset = \emptyset$$

Assim: $|T \cap I| + |T \cup J| = |T| = n$. Por outro lado, se $S \subset I$ e $L \subset J$ são subconjuntos não-tomadores, ainda pelo lema, $S \cup L = T$ é também não-tomador e como $S \cap L = \emptyset$, visto que $I \cap J = \emptyset$, então $|S| + |L| = |T|$.

Seja α o conjunto dos subconjuntos de W, não-tomadores, de cardinal n. Sejam, ainda, β_i $(i = 0,\ldots, n)$, a coleção de subconjuntos não-tomadores de I, de cardinal i e γ_j $(j = 0,..,n)$ a coleção dos não-tomadores de J, de cardinal j. Isto posto a aplicação

$$T \mapsto (T \cap I, T \cap J)$$

de α em $(\beta_o \times \gamma_n) \cup (\beta_1 \times \gamma_{n-1}) \cup \ldots \cup (\beta_n \times \gamma_o)$ está bem definida em virtude das considerações anteriores e é bijetora como mostraremos. Se $T \cap I = T_1 \cap I$ e $T \cap J = T_1 \cap J$, então $(T \cap I) \cup (T \cap J) = (T_1 \cap I) \cup (T_1 \cap J)$ ou $T \cap (I \cup J) = T_1 \cap (I \cup J)$ e daí $T \cap W = T_1 \cap W$ o que dá $T = T_1$. Além disso, se $(S,L) \in \beta_k \times \gamma_{n-k}$, então $|S| = k$, $|L| = n-k$ e, como já vimos, $S \cup L$ é não-tomador de cardinal n. Como porém $(S \cup L) \cap I = (S \cap I) \cup (L \cap I) = S \cup \emptyset = S$ e, analogamente, $(S \cup L) \cap J = L$, então

$$S \cup L \mapsto (S,L)$$

e portanto a aplicação considerada é sobrejetora. Donde

$$|\alpha| = |\beta_o||\gamma_n| + |\beta_1||\gamma_{n-1}| + \ldots + |\beta_n||\gamma_o|$$

ou seja

$$\binom{W}{n} = \sum_{k=o}^{n} \binom{I}{k} \binom{J}{n-k}$$

Vejamos agora algumas aplicações dos últimos resultados:

(I) Seja St(A,R(A)) um reticulado conforme o item (5.1). Dada uma estrela S sobre A, seja g(S) o número de subconjuntos de A, não-tomadores, cujas estrelas contêm S e seja f(S) o número desses subconjuntos cuja estrela é igual a S. É evidente então que

$$g(S) = \sum_{T \supset S} f(T)$$

onde T percorre o conjunto das estrelas que contêm S. Logo, pela fórmula de inversão de Möbius

$$f(S) = \sum_{T \supset S} \mu(S,T)\, g(T)$$

Em particular, como $f(\emptyset) = 1$:

$$1 = \sum_{T} \mu(\emptyset,T)\, g(T)$$

Como $\mu(\emptyset,\emptyset) = 1$, então

$$g(\emptyset) = -\sum_{T \neq \emptyset} \mu(\emptyset,T)\, g(T)$$

onde $g(\emptyset)$ é o número de subconjuntos de A não-tomadores.

(II) Consideremos o caso em que $A = \{1,2,\ldots, n\}$ e $R(A) = \{\{1\}, \{2\}, \ldots, \{n\}\}$. Como já vimos, na situação considerada: T é uma estrela sobre A se, e somente se, $T \subset A$.

Como, obviamente, todo $X \subset A$ é não-tomador, então $f(S) = 1$, para toda estrela S. Ademais, se $X \subset A$ tem k elementos, o número de subconjuntos de A que contêm X é 2^{n-k}. Observemos ainda que, como $St(A,R(A)) = \beta(A)$ (álgebra boolena sobre A), então $[\emptyset,X] \simeq [\emptyset,Y]$ sempre que $|X| = |Y|$. Assim sendo:

$$1 = \sum_{T} \mu(\emptyset,T)\, g(T) =$$

$$= \mu(\emptyset,\emptyset)g(\emptyset) + (-1)n\, g(\{1\}) + (-1)^2\binom{n}{2} g(\{1,2\}) + \ldots + (-1)^n \binom{n}{n} g(A)$$

e portanto

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

Observemos, por outro lado, como fica a fórmula obtida na proposição 7 neste caso, considerando que então: $W = I \oplus J \iff I \cap J = \emptyset$ e $I \cup J = W$. Se $|I| = i$, $|J| = j$, então $|W| = i + j$ e a fórmula citada fica

$$\binom{i+j}{n} = \sum_{k=o}^{n} \binom{i}{k}\binom{j}{n-k}$$

ou

$$\binom{i+j}{n} = \sum_{n_1+n_2=n} \binom{i}{n_1}\binom{j}{n_2}$$

o que mostra que esta bem conhecida identidade (fórmula de convolução de Vandermonde) pode ser considerada como um caso particular da fórmula da proposição mencionada.

(III) Um conjunto $A \times B$ tal que $|A| = |B| = n$ é chamado tabuleiro de ordem n. Se $T = \{a_{ij} \mid i,j = 1,2,\ldots, n\}$ é um tabuleiro de ordem n, facilita imaginar cada a_{ij} colocado num tabuleiro de xadrez na posição respectiva dos índices, segundo as convenções usuais a respeito. Definimos a linha i-ésima e a coluna j-ésima de T respectivamente por

$$L_i = \{a_{i1},\ldots, a_{in}\} \quad \text{e} \quad C_j = \{a_{1j},\ldots, a_{nj}\}$$

onde $1 \leqslant i, j \leqslant n$. É claro que $R(T) = \{L_1,\ldots, L_n, C_1,\ldots, C_n\}$ é um recobrimento de T e assim podemos considerar $St(T,R(T))$. Obviamente $st(a_{ij}) = L_i \cup C_j$, para cada $a_{ij} \in T$.

Um conjunto $X \subset T$ é não-tomador se, e somente se, para quaisquer a_{ij}, $a_{pq} \in X$, $i \neq p$ e $j \neq q$. De fato, se por exemplo $i = p$, então

$$a_{pq} = a_{iq} \in \{a_{i1},\ldots,a_{iq},\ldots,a_{in}\} \cup C_j = st(a_{ij})$$

o que não é possível quando se supõe X não-tomador. Reciprocamente, se existem a_{ij}, $a_{pq} \in X$ de maneira que $a_{ij} \in st(a_{pq}) = \{a_{p1},\ldots$

$\ldots, a_{pn}\} \cup \{a_{1q}, \ldots, a_{nq}\}$, então $a_{ij} \in L_p$ ou $a_{ij} \in C_q$, o que implica $i = p$ ou $j = q$.

Seja S uma estrela de St(T,R(T)). Dizemos que um conjunto $X \subset S$ gera S se $st(X) = S$ e, para todo $Y \subsetneq X$, $st(Y) \neq S$. É claro que sempre existe um gerador pelo menos de S.

Se $S \in St(T,R(T))$, façamos $L(S) = \{i | L_i \subset S\}$ e $C(S) = \{j | C_j \subset S\}$. Se fizermos $\ell(S) = |L(S)|$ e $c(S) = |C(S)|$, vale a seguinte equivalência: "Um gerador X de uma estrela S é um conjunto não-tomador se, e somente se, $\ell(S) = c(S)$."

Suponhamos X não-tomador e, por exemplo, $\ell(S) > c(S)$. Como

$$S = st(X) = (L_{i_1} \cup C_{j_1}) \cup \ldots \cup (L_{i_k} \cup C_{j_k})$$

a hipótese feita significa que no segundo membro devem existir duas colunas iguais, digamos $C_u = C_v$, ao passo que as linhas podem ser supostas diferentes entre si. Supondo $u = j_p$, $v = j_q$, $i_p = r$ e $i_q = s$, então

$$st(a_{ru}) = L_r \cup C_u \quad e \quad st(a_{sv}) = L_s \cup C_v = L_s \cup C_u$$

Como $a_{ru} \in C_u$, então $a_{ru} \in st(a_{sv})$, o que é absurdo pois $a_{ru}, a_{sv} \in X$ e $r \neq s$.

Reciprocamente, suponhamos S gerada por X e $\ell(S) = c(S)$. Fazendo

$$S = st(X) = (L_{i_1} \cup C_{j_1}) \cup \ldots \cup (L_{i_k} \cup C_{j_k})$$

onde as expressões entre parênteses no segundo membro são as estrelas dos diversos elementos de X, as hipóteses feitas nos garantem que não há linhas nem colunas repetidas no segundo membro. Assim, se existissem $a_{rs}, a_{pq} \overset{(*)}{\in} X$ de modo que $a_{rs} \in st(a_{pq}) = L_p \cup C_q$, teríamos que ter $r = p$ ou $s = q$ e daí $L_r = L_p$ ou $C_s = C_q$ onde $i_1 \leq r, p \leq i_k$ e $j_1 \leq s, q \leq j_k$, o que é impossível.

Seja S uma estrela tal que $\ell(S) = c(S) = m$. Supo

((*) $a_{rs} \neq a_{pq}$)

nhamos, o que não acarreta prejuizo de generalidade, que S é gerada por $X = \{a_{11}, \ldots, a_{mm}\}$. Então:

$$S = st(X) = st(a_{11}) \cup \ldots \cup st(a_{mm}) = (L_1 \cup C_1) \cup \ldots \cup (L_m \cup C_m) \qquad (*)$$

Ora, para cada permutação de $C_1, C_2, \ldots, C_m$ no segundo membro, fixando os L_i, obtemos

$$S = (L_1 \cup C_{r_1}) \cup \ldots \cup (L_m \cup C_{r_m})$$

onde

$$L_i \cup C_{r_i} = st(a_{ir_i})$$

Obviamente podemos garantir que $\{a_{1r_1}, \ldots, a_{mr_m}\}$ é gerador de S e como o número de linhas e o de colunas não sofreu nenhuma redução, podemos afirmar que este último conjunto é não-tomador para qualquer permutação $(r_1, r_2, \ldots, r_m)$ das colunas de S em (*). Assim já temos m! conjuntos não-tomadores que geram S. E não há outros. De fato, um conjunto não-tomador que gere S deve ter m elementos, um de cada linha e um de cada coluna de S.

Por outro lado, se $\ell(S) \neq c(S)$, não há subconjuntos de S, não-tomadores, que gerem S. Assim, neste caso: $f(S) = m!$ se $\ell(S) = c(S) = m$ e $f(S) = 0$, caso contrário.

Calculemos finalmente g(S). Se T é uma estrela gerada por um conjunto não-tomador e $T \supset S$, então $\ell(T) = c(T) = m \geq \max\{\ell(S), c(S)\}$. Logo existem

$$\binom{n - \ell(S)}{m - \ell(S)} \cdot \binom{n - c(S)}{m - c(S)}$$

estrelas T nessas condições. Como cada uma delas pode ser gerada por m! subconjuntos não-tomadores, então

$$\binom{n - \ell(S)}{m - \ell(S)} \cdot \binom{n - c(S)}{m - c(S)} \cdot m!$$

é o número de conjuntos não-tomadores, de cardinal m, cuja estrela contem S. Donde

$$g(S) = \sum_{m=\max\{\ell(S),c(S)\}}^{n} \binom{n-\ell(S)}{m-\ell(S)} \cdot \binom{n-c(S)}{m-c(S)} \cdot m!$$

(5.4) Seja A um conjunto finito. Um recobrimento R(A) desse conjunto se diz quase-independente se existem A_1, A_2, ..., $A_r \in R(A)$ de maneira que: (i) $A_1 \cup A_2 \cup \ldots \cup A_r = A$; (ii) $A - A_i \neq A$, para todo índice i, $1 \leqslant i \leqslant r$; (iii) qualquer que seja o índice i, $1 \leqslant i \leqslant r$, se X percorre o conjunto dos membros de R(A) diferentes de A_i, então $A_i \not\subset \bigcup X$.

Por exemplo, $R(A) = \{\{1\}; \{2,3\}; \{3,4\}; \{4,5\}\}$ é um recobrimento quase-independente de $A = \{1,2,3,4,5\}$, bastando considerar $A_1 = \{1\}$, $A_2 = \{2,3\}$ e $A_3 = \{4,5\}$ para se chegar a essa conclusão. Não é difícil verificar que o recobrimento $R(A) = \{\{1,2\}, \{1,3\}; \{4,5\}; \{2,5\}\}$ do mesmo conjunto A não é quase-independente.

Proposição 8. Seja $R(A) = \{A_1, \ldots, A_r, B_1, \ldots, B_s\}$ um recobrimento quase-independente de um conjunto A, onde $A_1, \ldots, A_r$ obedecem às condições (i), (ii) e (iii) acima. Então os átomos de St(A,R(A)) são exatamente $A_1, \ldots, A_r$.

Demonstração. Notemos primeiro que como existe em cada A_i um elemento p_i que não pertence a nenhum dos outros membros de R(A), então $st(p_i) = A_i$ $(i = 1,2,\ldots, r)$. Ou seja cada A_i é membro de St(A,R(A)).

Por outro lado, é evidente que nenhuma estrela do tipo

$$A_{i_1} \cup \ldots \cup A_{i_m} \qquad (m > 1)$$

ou

$$A_{i_1} \cup \ldots \cup A_{i_m} \cup B_{j_1} \cup \ldots \cup B_{j_n} \qquad (m \geqslant 1;\ n \geqslant 1)$$

é um átomo desse reticulado visto que cada uma delas contem propriamente A_{i_1}. Mostremos também que um elemento do tipo $B_{j_1} \cup \ldots \cup B_{j_n}$ não pode ser um átomo. Com efeito, observemos primeiro que os áto

mos de St(A,R(A)) devem ser procurados entre os elementos do tipo st(x), x ε A. Assim, se tivéssemos $B_{j_1} \cup \ldots \cup B_{j_n} = st(p)$, para algum p ε A, como $A = \cup A_i$, então algum dos A_i (i = 1,2,..., r) teria de ser igual a um dos B_{j_k}, o que é impossível em face das hipóteses.

Finalmente, observando que para quaisquer i, j ε {1,2,..., r}, i ≠ j, não se tem $A_i \subset A_j$ nem $A_j \subset A_i$, então efetivamente os átomos de St(A,R(A)) são $A_1, \ldots, A_r$.

Notemos que da proposição demonstrada decorre que os átomos de St(A,R(A)), nas condições exigidas, formam um recobrimento minimal de A em relação à inclusão.

Proposição 9. Para todo conjunto finito A e para todo recobrimento quase-independente R(A) do conjunto dado, se μ indica a função de Möbius de St(A,R(A)), então $\mu(\emptyset,A) = (-1)^r$, onde r indica o número de átomos do reticulado.

Demonstração. Sejam S e W estrelas sobre A tais que S ⊂ W. Façamos

$$Cob(S,W) = \{T \subset W \mid T \text{ cobre } S\}$$

e, para cada k ε N, $2 \leq k \leq |Cob(S,W)|$, façamos

$$c(S,W;k) = |\{Y \subset Cob(S,W) : |Y| = k \text{ e } \sup Y = W\}|$$

Ora, considerando o subreticulado [S,W], observemos que:

(a) $S \notin Cob(S,W)$

(b) Para todo X ε [S,W], X ≠ S, existe Y ε Cob(S,W) de maneira que Y ⊂ X, o que decorre do fato de que [S,X] é finito.

Isto mostra que as condições duais do teorema do corte transversal se verificam com relação a Cob(S,W). O teorema citado nos garante então que

$$\mu(S,W) = \sum_{k \geq 2} (-1)^k \, c(S,W;k)$$

Em particular, considerando os elementos nulo e universal de $St(A,R,(A))$, respectivamente $\emptyset$, e A, segue que

$$\mu(\emptyset,A) = \sum_{k\geq 2} (-1)^k c(\emptyset,A;k)$$

Notando porém que, como observamos logo após a demonstração da proposição anterior, $Cob(\emptyset,A)$ é minimal relativamente à inclusão e que, portanto, a única subcoleção Y de $Cob(\emptyset,A)$ cujo supremo (união) é A é o próprio $Cob(\emptyset,A)$, então

$$\mu(\emptyset,A) = (-1)^r c(\emptyset,A;r) = (-1)^r$$

onde $r = |Cob(\emptyset,A)|$.

Como caso particular suponhamos R(A) um recobrimento independente de A, ou seja, nenhum dos membros de R(A) está contido na união dos demais. Supondo $R(A) = \{A_1,\ldots, A_r\}$, então A_1, $A_2,\ldots, A_r$ são os átomos de $St(A,R(A))$. Se em cada A_i escolhermos um único $a_i \notin \cup_{j\neq i} A_j$, o que é possível neste caso, então $St(A,R(A)) \simeq \beta(E)$, onde $E = \{a_1,\ldots, a_r\}$. De fato, seja $f: \beta(E) \to St(A,R(A))$ definida por $f(\{a_{i_1},\ldots, a_{i_m}\}) = A_{i_1} \cup \ldots \cup A_{i_m}$. Se $A_{i_1} \cup \ldots \cup A_{i_m} = A_{j_1} \cup \ldots \cup A_{j_n}$, como cada átomo possui um elemento que não está em nenhum dos outros, cada átomo do primeiro membro deve figurar no segundo e vice-versa, do que segue que f é injetora. Seja $b \in A - E$. Então, se $A_1, A_2,\ldots, A_s$ são, para facilitar, os átomos que contêm b, $st(b) = A_1 \cup \ldots \cup A_s = st(a_1) \cup \ldots \cup st(a_s)$. Logo toda estrela S pode ser colocada como

$$S = st(x_1) \cup \ldots \cup st(x_p)$$

onde $x_1,\ldots, x_p \in E$ do que segue $f(\{x_1,\ldots, x_p\}) = S$ e f é sobrejetora. É imediato, por outro lado, que $f(X \cup Y) = f(X) \cup f(Y)$, para quaisquer $X,Y \subset E$ e que $X \subset Y \subset E$ implica $f(X) \subset f(Y)$. Donde, efetivamente, f é isomorfismo, já que f^{-1} também conserva as ordens.

Então, pelo que já vimos no capítulo 2, se S e W são estrelas sobre A tais que $S \subset W$, S é união de s átomos e W é a união de w átomos:

$$\mu(S,W) = (-1)^{w-s}$$

BIBLIOGRAFIA

(01) BARBOSA, R.M.: Partições bi-etiquetadas de conjuntos finitos. Combinatória 11, 1-19 (1980).

(02) BURTON, D.M.: Abstract and linear algebra. Addison- Wesley Pub.Co. (1972).

(03) CRAPO, H.: The Möbius function of a lattice. J. Combinatorial Theory 1, 126-131 (1966).

(04) DOMINGUES, H.H.: A álgebra dual da coálgebra de Dirichlet. Rev. Mat. Est.(UNESP). 1: 7-13 (1983).

(05) DOMINGUES, H.H.: Sobre a função de Möbius em reticulados modulares. Combinatória 23, 1-17 (1985).

(06) DOMINGUES, H.H.: Algumas aplicações da álgebra umbral à combinatória. Aprovada para publicação na Rev.Mat. Est. (UNESP).

(07) DOUBILET, P.: A Hopf algebra arising from the lattice of partitions of a set. J. Algebra. 28: 127-132 (1974).

(08) DOUBILET, P.; ROTA, G.C. & STANLEY, R.: On the foundations of combinatorial theory VI: the idea of generating function. In Berkeley symposium of mathematical statistics and probability, (6 th, Berkeley v.2, p. 267-318).

(09) DUBREIL-JACOTIN, M.L.; LESIEUR, L.& CROISOT, R.: Leçons sur la théorie des treillis des structores ordonnés et des treillis géométriques. Gauthier-Villars (1953).

(10) EISEN, M.: Elementary combinatorial analysis. Gordon and Breach (Science Publishers). (1969).

(11) FILLMORE, J & WILLIAMSON, S.G.: A linear algebra setting for the Mullin-Rota theory of polynomials of binomial type. Linear and Multilinear Algebra 1: 67 (1973).

(12) GARSIA, A.M.: An expose of the Mullin-Rota theory of polynomials of binomial type. Linear and Multilinear

Algebra 1: 43 (1973).

(13) GARSIA, A.M & JONI, S.A.: A new expression for umbral operators and power series inversion. Proc. Amer. Math. Soc. 64: 179-185 (1977).

(14) GOLDMAN, J.R. & ROTA, G.C.: On the foundations of combinatorial theory IV: finite vector spaces and eulerian generating functions. Studies in App. Math. XLIX (3): 239-258 (1970).

(15) GRAVER, J.E. & WATKINS, M.E.: Combinatories with enphasis on the theory of graphs. Springer-Verlag (1977).

(16) GREUB, W.: Linear algebra. Springer-Verlag. Fourth edition.

(17) GREUB, W.: Multilinear algebra. Springer-Verlag (1967).

(18) HENLE, M.: Binomial enumeration on dissects. Transactions of the American Mathematical Society. Vol. 202, pp 1-39 (1975).

(19) JONI, S.A. & ROTA, G.C.: Coalgebras and bialgebras in combinatories. Studies in Applied Mathematics 61: 93-139 (1979).

(20) MACLANE, S. & BIRKHOFF, G.: Algebra. MacMillan Publishing Co, Inc. Second Edition.

(21) ROMAN, M.R. & ROTA, G.C.: The umbral calculus. Advances in Mathematics 27, 95-188 (1978).

(22) ROTA, G.C.: Finite operator calculus. Academic Press, Inc. (1975).

(23) ROTA, G.C.: Hopf algebra methods in combinatorics. Colloque CNRS, Problémes Combinatoires et Théorie des Graphes, Orsay (1976): 363-365.

(24) ROTA, G.C.: On the foundations of combinatorial theory, I: theory of Möbius functions. Z. Warhrsch. 2: 340-368 (1964)

(25) SILVA, C.A. da: As funções aritméticas e a convolução de Dirichlet. São Paulo, PUC (Tese de Doutoramento) (1976).

(26) SMITH, D.A.: Incidence functions as generalized arithmetic functions, I. Duke Math. J., Vol. 34, pp 617-633 (1967).

(27) SMITH, D.A.: Incidence functions as generalized arithmetic functions, II. Duke Math. J., Vol.36, pp 15-30 (1969).

(28) STANLEY, P.S.: Binomial posets, Möbius inversion and permutation enumeration. Journal of Combinatorial Theory (A) 20, 336-356 (1976).

(29) SWEEDLER, M.E.: Hopf algebras. Benjamin (New York) (1969).

(30) WILSON, R.J.: The Möbius function in combinatorial mathematics. Proceedings of a Conference held at the Mathematical Inst., Oxford, from 7-10, July, pp 315-333 (1969).


cm 1 2 3 4 5 6 7 8 unesp 12 13 14 15 16 17 18 19