Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Um Problema de Teoria Aditiva dos Números via Álgebra Multilinear e Representações do Grupo Simétrico

por

Aline Gomes da Silva Pinto

2002

Agradecimentos

- Aos meus pais pela base sólida que tornou possível a subida de mais um degrau;

- Ao Marcelo por todo o companheirismo, conselhos e ajuda na conclusão e escrita da dissertação;

- Aos amigos, em particular, Cleida, Daniela, Marcelo Novais e Maxwell;

- Ao prof. Célius por toda sua dedicação desde o início da graduação;

- Ao prof. Hemar Godinho pela orientação na escolha do tema da dissertação e por toda a atenção durante o desenvolvimento do trabalho;

- Aos professores da banca examinadora pelas sugestões e correções, em especial, ao prof. Said Sidki que além disso auxiliou no esclarecimento de dúvidas e na sugestão de bibliografias;

- Aos demais professores do departamento e aos funcionários, em particular, Tânia e Manoel.

Resumo

O presente trabalho é baseado no artigo de Dias da Silva e Hamidoune, onde uma cota inferior para a cardinalidade do conjunto de todas as somas de h elementos distintos de um subconjunto A de um corpo K é apresentada. Em particular, a seguinte conjectura de Erdős e Heilbronn é provada:

> *"Seja p um primo, A um subconjunto não vazio de $\mathbb{Z}_p$ e $2^\wedge A$ o conjunto de todas as somas de dois elementos distintos de A. Então,* $|2^\wedge A| \geqslant \min\{p, 2|A| - 3\}$."

A demonstração do resultado principal é baseada na determinação de uma cota inferior para a dimensão do espaço cíclico do operador derivativo DT definido sobre o espaço de Grassmann $V \wedge \cdots \wedge V$, onde V é um espaço vetorial sobre o corpo K. Uma característica importante deste trabalho é o uso de representação do Grupo Simétrico na determinação desta cota inferior.

Abstract

This work is based upon a paper by Dias da Silva and Hamidoune, where a lower bound for the cardinality of the set of all sums of h distinct elements of a set A contained in a field K is presented. In particular, the following conjecture of Erdős and Heilbronn is proved:

> *"Let p be a prime number, A a nonempty subset of $\mathbb{Z}_p$ and $2^\wedge A$ the set of all sums of two distinct elements of A. Then,* $|2^\wedge A| \geqslant \min\{p, 2|A| - 3\}$."

The proof of the main result is based on the determination of a lower bound for dimension of the cyclic space of the derivative operator DT defined over the Grassmann space $V \wedge \cdots \wedge V$, where V is a vector space over a field K. An important characteristic of this work is the use of representation of the Symmetric Group on the determination of this lower bound.

Sumário

Introdução **2**

1 A Conjectura de Erdős e Heilbronn **7**

2 Representação de Grupos Finitos **14**

2.1 Representações e módulos 14

2.2 Produto tensorial de módulos 18

2.3 Representações e módulos induzidos 21

2.4 Critérios de irredutibilidade 23

2.5 Produto tensorial externo 26

2.6 O teorema do número de constituintes comuns 27

2.7 Os caracteres de um grupo finito 31

3 Representações do Grupo Simétrico **34**

3.1 Subgrupos de Young e suas 1-representações 34

3.2 Representações irredutíveis ordinárias de S_n 38

3.3 Os caracteres irredutíveis ordinários de S_n 45

3.4 Fórmulas de recursão 52

4 Espaços de Grassmann **55**

4.1 Definições e exemplos 55

4.2 Alguns resultados de álgebra linear 57

4.3 Operadores derivativos 60

4.4 Demonstração do Teorema 1.1 65

Bibliografia **70**

Índice Remissivo **71**

Introdução

Os problemas de contagem sempre fascinaram os homens. Um exemplo de problemas dessa natureza é o estudo da soma de dois subconjuntos A e B de um grupo abeliano $(G,+)$, que é dada por

$$A+B=\{a+b : a\in A, b\in B\}.$$

A teoria aditiva consiste no estudo desses subconjuntos de somas. Um *problema direto em teoria aditiva* é um problema em que se pretende descrever propriedades da soma de conjuntos em função das parcelas como, por exemplo, relacionar a cardinalidade da soma com as cardinalidades das parcelas.

Um resultado em problemas diretos bastante conhecido é o *Teorema de Cauchy-Davenport* que estabelece um minorante para a cardinalidade da soma de dois subconjuntos não vazios de $\mathbb{Z}_p$, com p primo, que depende apenas de p e das cardinalidades dos subconjuntos envolvidos.

Teorema (Cauchy-Davenport). *Sejam A e B subconjuntos não vazios de $\mathbb{Z}_p$. Então*

$$|\ A+B\ |\geqslant \min\{p, |\ A\ |+|\ B\ |-1\}.$$

Davenport [6] apresentou a prova desse teorema em 1935 e em 1947 publicou uma nota [7] dizendo ter descoberto que o teorema já havia sido provado por Cauchy [4] em 1813. Nessa mesma nota, Davenport explica que Cauchy provou o teorema para dar uma demonstração alternativa do resultado de Lagrange que diz que a equação

$$ax^2+by^2+c\equiv 0 \pmod p, \qquad \text{com}\quad a,b\not\equiv 0 \pmod p,$$

sempre possui solução. Como x^2 possui $\frac{p+1}{2}$ valores incongruentes módulo p, o mesmo vale para ax^2 e by^2. Representando por A e B os conjuntos de tais valores, em virtude do teorema, temos que a soma ax^2+by^2 possui no mínimo $\min\{p, |\ A\ |+|\ B\ |-1\}$ valores incongruentes. Como $|\ A\ |+|\ B\ |-1=p$, segue que toda classe de resíduos módulo p pode ser representada por ax^2+by^2.

O Teorema de Cauchy-Davenport pode ser facilmente generalizado para a soma de h subconjuntos de $\mathbb{Z}_p$ (usando indução sobre h), dando

$$| A_1 + A_2 + \cdots + A_h | \geqslant \min\{p, | A_1 | + \cdots + | A_h | - h + 1\}.$$

Outro resultado que generaliza o Teorema de Cauchy-Davenport é devido a Dias da Silva e Godinho [10, 13]. Seja

$$s_{k,h}(x_1, \ldots, x_h) = \sum_{1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant h} x_{i_1} x_{i_2} \cdots x_{i_k}$$

o polinômio simétrico elementar de grau k em h variáveis e considere o conjunto

$$s_{k,h}(A_1, \ldots, A_h) := \{s_{k,h}(a_1, \ldots, a_h) : (a_1, \ldots, a_h) \in A_1 \times \cdots \times A_h\}.$$

Dias da Silva e Godinho apresentaram a seguinte estimativa para a cardinalidade do conjunto acima:

$$| s_{k,h}(A_1, \ldots, A_h) | \geqslant \left\lfloor \frac{| A_1 | + \cdots + | A_h | - h}{k} \right\rfloor + 1,$$

para p suficientemente grande. Observemos que quando $k = 1$ obtemos o Teorema de Cauchy-Davenport, ou seja,

$$| s_{1,h}(A_1, \ldots, A_h) | \geqslant \min\{p, | A_1 | + \cdots + | A_h | - h + 1\}.$$

Nesta dissertação consideramos o problema de estimar a cardinalidade do conjunto

$$2^{\wedge}A := \{a + a' : a, a' \in A \text{ e } a \neq a'\}$$

de todas as somas de dois elementos distintos de um subconjunto A de $\mathbb{Z}_p$. O Teorema de Cauchy-Davenport diz que $| A+A | \geqslant \min\{p, 2 | A | - 1\}$. Certamente essa estimativa não serve como minorante para a cardinalidade de $2^{\wedge}A$, visto que estamos considerando uma quantidade bem menor de somas. Por exemplo, para $A = \{1, 3, 6\} \subset \mathbb{Z}_7$ temos $A + A = \{0, 2, 4, 5, 6\}$, $2^{\wedge}A = \{0, 2, 4\}$ e $2 | A | - 1 = 5$.

Nos anos 60, *Erdős* e *Heilbronn* conjecturaram que

$$| 2^{\wedge}A | \geqslant \min\{p, 2 | A | - 3\}.$$

Apesar de Erdős e Heilbronn não terem incluído a conjuctura em [12], Erdős a apresentou numa conferência de Teoria dos Números na Universidade do Colorado em 1963 [11].

No caso em que $A \subset \mathbb{Z}$, é fácil mostrar que $| 2^{\wedge}A | \geqslant 2 | A | - 3$. De fato, seja

$$A = \{a_1, a_2 \ldots, a_k\}, \quad \text{com } a_1 < a_2 < \cdots < a_k.$$

Então,

$$a_1 + a_2 < a_1 + a_3 < a_2 + a_3 < a_2 + a_4 < \cdots < a_{k-2} + a_{k-1} < a_{k-2} + a_k < a_{k-1} + a_k,$$

donde segue que $| 2^{\wedge}A | \geqslant 2(k-2) + 1 = 2 | A | -3$. Mas quando consideramos A como um subconjunto de $\mathbb{Z}_p$, pode haver muito mais somas repetidas, por causa da característica finita. Uma outra dificuldade é controlar o comportamento das somas módulo p de forma geral, ou seja, para todo p.

Dias da Silva e *Hamidoune* [8] apresentaram, em 1994, a prova da conjectura. Essa demonstração utiliza resultados obtidos em álgebra multilinear e resultados da teoria de representações do grupo simétrico S_n. Na verdade, eles mostraram um resultado bem mais geral que o da conjectura.

Teorema (Dias da Silva-Hamidoune). *Seja K um corpo, p a característica de K, se ela é finita, e $p = \infty$ se a característica de K é igual a 0. Sejam A um subconjunto finito de K e h um inteiro positivo. Então,*

$$| h^{\wedge}A | \geqslant \min\{p, h | A | -h^2 + 1\}, \tag{1}$$

onde $h^{\wedge}A$ é o conjunto das somas de h elementos distintos de A.

Demonstrações posteriores para o Teorema de Dias da Silva-Hamidoune foram apresentadas por Nathanson [17] e Alon, Nathanson e Ruzsa [1]. Em [17], Nathanson substitui os resultados de representações de grupos por resultados de caminhos em $\mathbb{Z}^n$ (um caminho em $\mathbb{Z}^2$ é uma seqüência finita de inteiros $a_1, a_2, \ldots, a_r$, tal que $a_i - a_{i-1} = (1,0)$ ou $(0,1)$, para todo i). Uma observação a esse respeito enconta-se no final do Capítulo 4. Em [1], os autores dão uma prova polinomial para a conjectura, utilizando princípios de contagem semelhantes aos usados em [17].

Nesta dissertação apresentamos a prova dada por Dias da Silva e Hamidoune do teorema acima e a teoria necessária para o entendimento dos resultados utilizados. A escolha dessa demonstração se deve a riqueza de tópicos que são aplicados na resolução do problema.

Dias da Silva e Hamidoune também mostraram que a estimativa do teorema (e, conseqüentemente, da conjectura) é a melhor possível, isto é, quando o subconjunto $A \subset \mathbb{Z}_p$ possui seus elementos em progressão aritmética, o mínimo da estimativa (1) é atingido. Uma pergunta natural é se somente esses subconjuntos atingem o mínimo. Este tipo de problema, que pretende deduzir propriedades das parcelas a partir de propriedades do conjunto soma, é chamado de *problema inverso*. Assim, perguntar se conjuntos que atingem o mínimo na estimativa (1)

possuem seus elementos em progressão aritmética é um problema inverso que consideramos nesta dissertação.

Os exemplos e resultados de teoria aditiva encontram-se no Capítulo 1. Os capítulos seguintes consistem no desenvolvimento da teoria e dos resultados utilizados na demonstração do Teorema de Dias da Silva e Hamidoune.

No Capítulo 2 expomos alguns resultados de representações de grupos finitos. O leitor já familiarizado com essa teoria pode perfeitamente seguir direto para a leitura do Capítulo 3. O objetivo do Capítulo 2 é apenas introduzir algumas terminologias necessárias para o capítulo seguinte e dar subsídio para o entendimento do mesmo. Alguns resultados são enunciados sem demonstração tendo em vista não extender por demais o texto, evitando assim nos afastar de nosso objetivo principal. As demonstrações omitidas podem ser encontradas em [5].

No Capítulo 3 apresentamos resultados a partir dos quais é possível obter uma fórmula para os graus das representações irredutíveis de S_n (Teorema 3.20), que depende apenas de n e de suas partições. Para isso associamos à cada partição de n um subgrupo de S_n, chamado *subgrupo de Young*. Depois induzimos em S_n as 1-representações desses subgrupos e vamos em busca do número de constituintes comuns entre as representações obtidas, com o objetivo de construir um conjunto completo de representações irredutíveis. Aplicando o Teorema 2.24, conhecido como "*intertwining number theorem*", vemos que esse número de constituintes comuns pode ser determinado através do número de classes duplas dos subgrupos de Young cujas representações foram induzidas em S_n. Então transformamos um problema de representações de grupos em um problema de combinatória. *Diagramas de Young* e resultados como o Teorema 3.10, de Gale-Ryser [19], são as ferramentas utilizadas para determinarmos esse número de classes duplas. Com um conjunto completo de representações irredutíveis de S_n em mãos, aplicamos os resultados da teoria de caracteres e obtemos a fórmula desejada.

Um outro resultado importante do Capítulo 3 é o Teorema 3.23 que dá uma fórmula de recursão para os caracteres irredutíveis de S_n. Restringindo um caracter irredutível de S_{n+1} a S_n obtemos um caracter escrito como uma soma, tomada sobre partições de n, de caracteres irredutíveis de S_n.

As fórmula obtidas nos Teoremas 3.20 e 3.23 são utilizadas para a obtenção de resultados de álgebra multilinear que apresentamos no Capítulo 4. A partir de um espaço vetorial V (de dimensão finita) e uma aplicação h-linear e anti-simétrica, definida no produto direto de h cópias de V, definimos o espaço de Grassmann $\bigwedge^h V$, que pode ser visto como a "restrição"do produto tensorial de espaços vetoriais a uma aplicação anti-simétrica. Nesse espaço, construímos uma base associada a partições e definimos um operador linear DT induzido de um

operador T em V, chamado *operador derivativo*. Naturalmente, as potências $(DT)^n$ do operador derivativo podem ser escritas como combinação linear dos elementos da base de $\bigwedge^h V$ associada a partições. Com o auxílio do Teorema 3.23, mostramos que os coeficientes dessas expressões são dados pela fórmula do Teorema 3.20. Conhecendo as potências do operador derivativo podemos obter um minorante para a dimensão de um subespaço cíclico particular com respeito a esse operador (Teorema 4.9). O Teorema de Dias da Silva e Hamidoune segue diretamente desse último resultado.

Capítulo 1

A Conjectura de Erdős e Heilbronn

Seja $\mathbb{Z}_p$ o corpo dos inteiros módulo p e A um subconjunto não vazio de $\mathbb{Z}_p$. Denotemos por $2^\wedge A$ o subconjunto de todas as somas de dois elementos distintos de A, ou seja,

$$2^\wedge A = \{a + a' : a, a' \in A \text{ e } a \neq a'\}.$$

A conjectura de Erdős e Heilbronn afirma que

$$| \, 2^\wedge A \, | \geqslant \min\{p, 2 \mid A \mid -3\}.$$

Neste capítulo expomos alguns resultados de teoria aditiva dos números que estão relacionados com essa conjectura.

Dias da Silva e Hamidoune [9] provaram que a conjectura é verdadeira, numa forma bem mais geral. O resultado provado por eles foi o seguinte.

Teorema 1.1 (Dias da Silva-Hamidoune). *Seja K um corpo, p a característica de K, se ela é finita, e $p = \infty$ se a característica de K é igual a 0. Seja A um subconjunto finito de K e h um inteiro positivo. Então,*

$$| \, h^\wedge A \, | \geqslant \min\{p, h \mid A \mid -h^2 + 1\},$$

onde $h^\wedge A$ é o conjunto das somas de h elementos distintos de A.

A demonstração do teorema acima encontra-se no Capítulo 4, seção 4. Quando $h = 2$ e $A \subset \mathbb{Z}_p$, temos a conjectura de Erdős e Heilbronn.

Dias da Silva e Hamidoune provaram também que a estimativa do Teorema 1.1 é a melhor possível, independente da característica de K. Para isso, eles apresentaram conjuntos que satisfazem a igualdade na estimativa, como veremos a seguir.

Seja $A = \{0, 1, \ldots, k-1\} \subset \mathbb{Z}$ e $k \geqslant h$, então a menor soma possível de h elementos distintos de A é dada por

$$0 + 1 + \cdots + (h-1) = \frac{h(h-1)}{2}$$

e a maior, por

$$(k-1) + ((k-1)-1) + \cdots + ((k-1)-(h-1)) = hk - (1 + 2 + \cdots + h) = hk - \frac{h(h+1)}{2}.$$

Para $a, b \in \mathbb{Z}$, com $a < b$, denotemos por $[a, b]$ o subconjunto de $\mathbb{Z}$ dado por $\{x \in \mathbb{Z} : a \leqslant x \leqslant b\}$. A escolha do conjunto A nos permite concluir que todos os inteiros entre a menor e a maior soma de h elementos distintos de A estão em $h^\wedge A$. Então,

$$h^\wedge A = \left[\frac{h(h-1)}{2}, hk - \frac{h(h+1)}{2}\right],$$

donde segue que

$$| h^\wedge A | = hk - \frac{h(h+1)}{2} - \frac{h(h-1)}{2} + 1 = hk - h^2 + 1. \tag{1.1}$$

Seja agora A um subconjunto de $\mathbb{Z}$ cujos elementos estão em progressão aritmética com razão igual a r e primeiro termo igual a a_0, ou seja,

$$A = \{a_0, a_0 + r, a_0 + 2r, \ldots, a_0 + (k-1)r\} = \{a_0\} + r * [0, k-1]. \tag{1.2}$$

Como $| h^\wedge[0, k-1] | = hk - h^2 + 1$, segue que o mesmo é válido para A. Isto nos diz que, se os elementos de $A \subset \mathbb{Z}$ estão em progressão aritmética, a igualdade na estimativa do Teorema 1.1 é atingida.

Vamos agora mostrar que o mesmo é válido quando $A \subset \mathbb{Z}_p$. Como a igualdade (1.2) também se verifica em $\mathbb{Z}_p$, basta considerarmos $A = \{0, 1, \ldots, k-1\} \subset \mathbb{Z}_p$, com $k \geqslant h$. Se $hk - h^2 + 1 \geqslant p$, então o Teorema 1.1 nos permite concluir que $| h^\wedge A | = \min\{p, hk - h^2 + 1\}$. Suponhamos então que $hk - h^2 \leqslant p - 2$. Seja $\nu : \mathbb{Z} \to \mathbb{Z}_p$ o homomorfismo canônico e $S = \{0, 1, \ldots, k-1\} \subset \mathbb{Z}$. Então $A = \nu(S)$ e

$$h^\wedge A = \nu(h^\wedge S) = \nu\left(\left[\frac{h(h-1)}{2}, hk - \frac{h(h+1)}{2}\right]\right).$$

Para $i, j \in \left[\frac{h(h+1)}{2}, hk - \frac{h(h-1)}{2}\right]$, com $i < j$, temos $j - i \in [1, h(k-h)]$ e, como $h(k-h) \leqslant p-2$, segue que $\nu(i) \neq \nu(j)$. Assim,

$$| h^\wedge A | = \left|\left[\frac{h(h+1)}{2}, hk - \frac{h(h-1)}{2}\right]\right| = h(k-h) + 1 = \min\{p, hk - h^2 + 1\},$$

como queríamos.

Dizemos que A é um *conjunto crítico* quando A satisfaz a igualdade na estimativa do Teorema 1.1. O estudo de tais conjuntos é relevante somente quando $\mid A \mid \geqslant 4$, pois nos outros casos A é claramente um conjunto crítico. Uma observação interessante é que nem todos os subconjuntos de $\mathbb{Z}$ ou $\mathbb{Z}_p$ que são críticos estão em progressão aritmética, como podemos ver nos exemplos abaixo (convencionado $p = +\infty$ se $A \subset \mathbb{Z}$).

Exemplo 1.2. Seja $A \subset \mathbb{Z}$ ou $A \subset \mathbb{Z}_p$ um subconjunto com k elementos. Se $h = k$, então $hk - h^2 + 1 = 1$ e $\mid h^\wedge A \mid = 1 = \min\{p, hk - h^2 + 1\}$.

Exemplo 1.3. Seja $A \subset \mathbb{Z}$ ou $A \subset \mathbb{Z}_p$ um subconjunto com k elementos. Se $h = 1$ ou $h = k-1$, então $hk - h^2 + 1 = k$ e $\mid 1^\wedge A \mid = \mid (k-1)^\wedge A \mid = k = \min\{p, hk - h^2 + 1\}$.

Exemplo 1.4. Se $h = 2$ e $k = 4$, então $hk - h^2 + 1 = 5$. Seja $A = \{a_0, a_1, a_2, a_3\} \subset \mathbb{Z}$, com $a_0 < a_1 < a_2 < a_3$. Então $2^\wedge A = \{a_0 + a_1, a_0 + a_2, a_0 + a_3, a_1 + a_2, a_1 + a_3, a_2 + a_3\}$. Como

$$a_0 + a_1 < a_0 + a_2 < \boldsymbol{a_0 + a_3} < a_1 + a_3 < a_2 + a_3$$

temos que $\mid 2^\wedge A \mid = 5$ ou 6. Além disso,

$$a_0 + a_2 < \boldsymbol{a_1 + a_2} < a_1 + a_3$$

e portanto $\mid 2^\wedge A \mid = 5$ se, e somente se, $a_0 + a_3 = a_1 + a_2$. Então $A = \{a_0, a_1, a_2, a_2 + a_1 - a_0\}$, com $a_0 < a_1 < a_2$, é um conjunto crítico.

No caso em que A é um subconjunto de $\mathbb{Z}$, o teorema abaixo garante que os exemplos acima são os únicos exemplos de conjuntos críticos cujos os elementos não estão em progressão aritmética.

Teorema 1.5. *Seja $k \geqslant 5$ e $2 \leqslant h \leqslant k - 2$. Se A é um conjunto com k inteiros tal que*

$$\mid h^\wedge A \mid = hk - h^2 + 1,$$

então os elementos de A estão em progressão aritmética.

Demonstração. Seja $A = \{a_1, a_2, \ldots, a_k\} \subset \mathbb{Z}$, com $a_1 < a_2 < \cdots < a_k$. Vamos provar que o teorema é válido para $h = 2$. A demonstração para os outros valores de h é feita com as mesmas idéias e encontra-se em [18], pg. 16.

Precisamos mostrar que $a_i - a_{i-1} = a_2 - a_1$, para todo $i = 3, \ldots, k$. Como $\mid 2^\wedge A \mid = 2k - 3$ e

$$a_1 + a_2 < a_1 + a_3 < a_2 + a_3 < a_2 + a_4 < \cdots < a_{k-2} + a_{k-1} < a_{k-2} + a_k < a_{k-1} + a_k,$$

o conjunto $2^\wedge A$ consiste exatamente dos elementos da expressão acima.

Uma vez que $a_1+a_3 < a_1+a_4 < a_2+a_4$, temos $a_1+a_4 = a_2+a_3$, ou seja, $a_2-a_1 = a_4-a_3$. Analogamente, para $i = 1, \ldots, k-3$,

$$a_i + a_{i+2} < a_i + a_{i+3} < a_{i+1} + a_{i+3} \quad \text{e} \quad a_{i+1} + a_{i+3} < a_{i+1} + a_{i+4} < a_{i+2} + a_{i+4}$$

implicam que

$$a_{i+1} - a_i = a_{i+3} - a_{i+2} \quad \text{e} \quad a_{i+2} - a_{i+1} = a_{i+4} - a_{i+3}.$$

Além disso,

$$a_2 + a_3 = a_1 + a_4 < a_1 + a_5 < a_2 + a_5 = a_3 + a_4,$$

donde segue que $a_2 - a_1 = a_5 - a_4$ e portanto A está em progressão aritmética.

■

Vamos agora analizar o caso em que $A \subset \mathbb{Z}_p$ e $h = 2$. No Exemplo 1.4, caracterizamos os conjuntos críticos de inteiros com cardinalidade igual a 4 (observe que a condição $a_0+a_3 = a_1+a_2$ inclui o caso em que os elementos do conjunto estão em progressão aritmética). Isso também pode ser feito para subconjuntos de $\mathbb{Z}_p$ com essa cardinalidade.

Exemplo 1.6. Na tabela abaixo, apresentamos todos os subconjuntos críticos A de $\mathbb{Z}_{11}$ tais que $\mid A \mid = 4$. A tabela também descreve o conjunto $2^\wedge A$ e diz se o conjunto A está em progressão aritmética (p.a. A). Neste caso, a coordenada a de (a, b) indica o primeiro termo da p.a. e b indica a razão.

A	$2^\wedge A$	p.a. A	A	$2^\wedge A$	p.a. A
{ 0, 1, 2, 3}	{ 1, 2, 3, 4, 5}	(0,1) (3,10)	{ 0, 1, 2,10}	{ 0, 1, 2, 3,10}	(2,10) (10,1)
{ 0, 1, 3, 4}	{ 1, 3, 4, 5, 7}		{ 0, 1, 3, 9}	{ 1, 3, 4, 9,10}	
{ 0, 1, 4, 5}	{ 1, 4, 5, 6, 9}		{ 0, 1, 4, 8}	{ 1, 4, 5, 8, 9}	(0,4) (1,7)
{ 0, 1, 5, 6}	{ 0, 1, 5, 6, 7}	(1,5) (5,6)	{ 0, 1, 5, 7}	{ 1, 5, 6, 7, 8}	
{ 0, 1, 6, 7}	{ 1, 2, 6, 7, 8}	(0,6) (7,5)	{ 0, 1, 7, 8}	{ 1, 4, 7, 8, 9}	
{ 0, 1, 8, 9}	{ 1, 6, 8, 9,10}		{ 0, 1, 9,10}	{ 0, 1, 8, 9,10}	(1,10) (9,1)
{ 0, 2, 3, 5}	{ 2, 3, 5, 7, 8}		{ 0, 2, 3,10}	{ 1, 2, 3, 5,10}	
{ 0, 2, 4, 6}	{ 2, 4, 6, 8,10}	(0,2) (6,9)	{ 0, 2, 4, 9}	{ 0, 2, 4, 6, 9}	(4,9) (9,2)
{ 0, 2, 5, 7}	{ 1, 2, 5, 7, 9}		{ 0, 2, 5, 8}	{ 2, 5, 7, 8,10}	(0,8) (2,3)
{ 0, 2, 6, 7}	{ 2, 6, 7, 8, 9}		{ 0, 2, 6, 8}	{ 2, 3, 6, 8,10}	
{ 0, 2, 7, 9}	{ 0, 2, 5, 7, 9}	(2,9) (7,2)	{ 0, 2, 8,10}	{ 1, 2, 7, 8,10}	
{ 0, 3, 4, 7}	{ 0, 3, 4, 7,10}	(3,4) (4,7)	{ 0, 3, 4,10}	{ 2, 3, 4, 7,10}	
{ 0, 3, 5, 8}	{ 0, 2, 3, 5, 8}	(3,8) (5,3)	{ 0, 3, 5, 9}	{ 1, 3, 5, 8, 9}	
{ 0, 3, 6, 8}	{ 0, 3, 6, 8, 9}	(6,8) (8,3)	{ 0, 3, 6, 9}	{ 1, 3, 4, 6, 9}	(0,3) (9,8)

A	$2\hat{}A$	p.a. A	A	$2\hat{}A$	p.a. A
{ 0, 3, 7,10}	{ 2, 3, 6, 7,10}	(0,7) (10,4)	{ 0, 4, 5, 9}	{ 2, 3, 4, 5, 9}	
{ 0, 4, 5,10}	{ 3, 4, 5, 9,10}	(0,5) (4,6)	{ 0, 4, 6, 9}	{ 2, 4, 6, 9,10}	
{ 0, 4, 6,10}	{ 3, 4, 5, 6,10}		{ 0, 4, 7, 8}	{ 0, 1, 4, 7, 8}	(7,4) (8,7)
{ 0, 5, 6,10}	{ 0, 4, 5, 6,10}	(6,5) (10,6)	{ 0, 5, 7, 9}	{ 1, 3, 5, 7, 9}	(0,9) (5,2)
{ 0, 6, 7,10}	{ 2, 5, 6, 7,10}		{ 0, 6, 8, 9}	{ 3, 4, 6, 8, 9}	
{ 0, 7, 8,10}	{ 4, 6, 7, 8,10}		{ 0, 8, 9,10}	{ 6, 7, 8, 9,10}	(0,10) (8,1)
{ 1, 2, 3, 4}	{ 3, 4, 5, 6, 7}	(1,1) (4,10)	{ 1, 2, 4, 5}	{ 3, 5, 6, 7, 9}	
{ 1, 2, 4,10}	{ 0, 1, 3, 5, 6}		{ 1, 2, 5, 6}	{ 0, 3, 6, 7, 8}	
{ 1, 2, 5, 9}	{ 0, 3, 6, 7,10}	(1,4) (2,7)	{ 1, 2, 6, 7}	{ 2, 3, 7, 8, 9}	(2,5) (6,6)
{ 1, 2, 6, 8}	{ 3, 7, 8, 9,10}		{ 1, 2, 7, 8}	{ 3, 4, 8, 9,10}	(1,6) (8,5)
{ 1, 2, 8, 9}	{ 0, 3, 6, 9,10}		{ 1, 2, 9,10}	{ 0, 1, 3, 8,10}	
{ 1, 3, 4, 6}	{ 4, 5, 7, 9,10}		{ 1, 3, 5, 7}	{ 1, 4, 6, 8,10}	(1,2) (7,9)
{ 1, 3, 5,10}	{ 0, 2, 4, 6, 8}	(5,9) (10,2)	{ 1, 3, 6, 8}	{ 0, 3, 4, 7, 9}	
{ 1, 3, 6, 9}	{ 1, 4, 7, 9,10}	(1,8) (3,3)	{ 1, 3, 7, 8}	{ 0, 4, 8, 9,10}	
{ 1, 3, 7, 9}	{ 1, 4, 5, 8,10}		{ 1, 3, 8,10}	{ 0, 2, 4, 7, 9}	(3,9) (8,2)
{ 1, 4, 5, 8}	{ 1, 2, 5, 6, 9}	(4,4) (5,7)	{ 1, 4, 6, 9}	{ 2, 4, 5, 7,10}	(4,8) (6,3)
{ 1, 4, 6,10}	{ 0, 3, 5, 7,10}		{ 1, 4, 7, 9}	{ 0, 2, 5, 8,10}	(7,8) (9,3)
{ 1, 4, 7,10}	{ 0, 3, 5, 6, 8}	(1,3) (10,8)	{ 1, 5, 6,10}	{ 0, 4, 5, 6, 7}	
{ 1, 5, 7,10}	{ 0, 1, 4, 6, 8}		{ 1, 5, 8, 9}	{ 2, 3, 6, 9,10}	(8,4) (9,7)
{ 1, 6, 8,10}	{ 0, 3, 5, 7, 9}	(1,9) (6,2)	{ 1, 7, 9,10}	{ 0, 5, 6, 8,10}	
{ 2, 3, 4, 5}	{ 5, 6, 7, 8, 9}	(2,1) (5,10)	{ 2, 3, 5, 6}	{ 0, 5, 7, 8, 9}	
{ 2, 3, 6, 7}	{ 2, 5, 8, 9,10}		{ 2, 3, 6,10}	{ 1, 2, 5, 8, 9}	(2,4) (3,7)
{ 2, 3, 7, 8}	{ 0, 4, 5, 9,10}	(3,5) (7,6)	{ 2, 3, 7, 9}	{ 0, 1, 5, 9,10}	
{ 2, 3, 8, 9}	{ 0, 1, 5, 6,10}	(2,6) (9,5)	{ 2, 3, 9,10}	{ 0, 1, 2, 5, 8}	
{ 2, 4, 5, 7}	{ 0, 1, 6, 7, 9}		{ 2, 4, 6, 8}	{ 1, 3, 6, 8,10}	(2,2) (8,9)
{ 2, 4, 7, 9}	{ 0, 2, 5, 6, 9}		{ 2, 4, 7,10}	{ 0, 1, 3, 6, 9}	(2,8) (4,3)
{ 2, 4, 8, 9}	{ 0, 1, 2, 6,10}		{ 2, 4, 8,10}	{ 1, 3, 6, 7,10}	
{ 2, 5, 6, 9}	{ 0, 3, 4, 7, 8}	(5,4) (6,7)	{ 2, 5, 7,10}	{ 1, 4, 6, 7, 9}	(5,8) (7,3)
{ 2, 5, 8,10}	{ 1, 2, 4, 7,10}	(8,8) (10,3)	{ 2, 6, 9,10}	{ 0, 1, 4, 5, 8}	(9,4) (10,7)
{ 3, 4, 5, 6}	{ 0, 7, 8, 9,10}	(3,1) (6,10)	{ 3, 4, 6, 7}	{ 0, 2, 7, 9,10}	
{ 3, 4, 7, 8}	{ 0, 1, 4, 7,10}		{ 3, 4, 8, 9}	{ 0, 1, 2, 6, 7}	(4,5) (8,6)
{ 3, 4, 8,10}	{ 0, 1, 2, 3, 7}		{ 3, 4, 9,10}	{ 1, 2, 3, 7, 8}	(3,6) (10,5)
{ 3, 5, 6, 8}	{ 0, 2, 3, 8, 9}		{ 3, 5, 7, 9}	{ 1, 3, 5, 8,10}	(3,2) (9,9)
{ 3, 5, 8,10}	{ 0, 2, 4, 7, 8}		{ 3, 5, 9,10}	{ 1, 2, 3, 4, 8}	
{ 3, 6, 7,10}	{ 2, 5, 6, 9,10}	(6,4) (7,7)	{ 4, 5, 6, 7}	{ 0, 1, 2, 9,10}	(4,1) (7,10)

A	$2^\wedge A$	p.a. A	A	$2^\wedge A$	p.a. A
{ 4, 5, 7, 8}	{ 0, 1, 2, 4, 9}		{ 4, 5, 8, 9}	{ 1, 2, 3, 6, 9}	
{ 4, 5, 9,10}	{ 2, 3, 4, 8, 9}	(5,5) (9,6)	{ 4, 6, 7, 9}	{ 0, 2, 4, 5,10}	
{ 4, 6, 8,10}	{ 1, 3, 5, 7,10}	(4,2) (10,9)	{ 5, 6, 7, 8}	{ 0, 1, 2, 3, 4}	(5,1) (8,10)
{ 5, 6, 8, 9}	{ 0, 2, 3, 4, 6}		{ 5, 6, 9,10}	{ 0, 3, 4, 5, 8}	
{ 5, 7, 8,10}	{ 1, 2, 4, 6, 7}		{ 6, 7, 8, 9}	{ 2, 3, 4, 5, 6}	(6,1) (9,10)
{ 6, 7, 9,10}	{ 2, 4, 5, 6, 8}		{ 7, 8, 9,10}	{ 4, 5, 6, 7, 8}	(7,1) (10,10)

Pelo Exemplo 1.4, quando $A \subset \mathbb{Z}$, $h = 2$ e $\mid A \mid = 4$, A é um conjunto crítico se, e somente se,

$$a_0 + a_3 = a_1 + a_2.$$

No caso de $A \subset \mathbb{Z}_{11}$ podemos analizar a tabela acima e ver que se $A = \{a_0, a_1, a_2, a_3\}$, com $a_0 < a_1 < a_2 < a_3$, é um conjunto crítico, então

$$a_0 + a_3 \equiv a_1 + a_2 \quad \text{ou} \quad a_0 + a_1 \equiv a_2 + a_3. \tag{1.3}$$

Na verdade, essa observação independe de $p = 11$, ou seja, é verdadeira sempre que $A \subset \mathbb{Z}_p$ é um conjunto crítico com $\mid A \mid = 4$, para todo $p \geqslant 5$. De fato, temos

$$A = \{a_0 + a_1, a_0 + a_2, a_0 + a_3, a_1 + a_2, a_1 + a_3, a_2 + a_3\}.$$

Então $\mid 2^\wedge A \mid = 5$ se, e somente se,

$$a_0 + a_1 \equiv a_2 + a_3, \quad a_0 + a_2 \equiv a_1 + a_3 \quad \text{ou} \quad a_0 + a_1 \equiv a_2 + a_3.$$

Podemos considerar $a_0 = 0$ e assim $a_0 + a_2 \equiv a_1 + a_3$ implica em $a_3 \equiv a_2 - a_1$, o que é impossível uma vez que $0 < a_1 < a_2 < a_3 < p$. Com isso, $A \subset \mathbb{Z}_p$ com $\mid A \mid = 4$ é minimal se, e somente se, ocorre (1.3).

Um resultado equivalente ao Teorema 1.5 para subconjuntos de $\mathbb{Z}_p$ com cardinalidade maior do que ou igual a 5 ainda não foi estabelecido. Para $p \leqslant 17$, observamos através de tabelas como as do Exemplo 1.6 que, para $h = 2$, todos os subconjuntos críticos de $\mathbb{Z}_p$ com cardinalidade maior do que ou igual a 5 possuem seus elementos em progressão aritmética. Um resultado parcial sobre esse problema aparece em [16].

Por fim, apresentamos uma aplicação do Teorema 1.1, que também é devido a Dias da Silva e Hamidoune [9], a problemas de teoria aditiva estudados por Erdős e Heilbronn [12].

Para $x \in \mathbb{R}$, denotamos por $\lfloor x \rfloor$ o maior inteiro menor do que ou igual a x e por $\lceil x \rceil$ o menor inteiro maior do que ou igual a x.

Teorema 1.7. *Seja $A \subset \mathbb{Z}_p$ com cardinalidade igual a $\lfloor\sqrt{4p-7}\rfloor + 1$. Então todo elemento de $\mathbb{Z}_p$ pode ser escrito como uma soma de*

$$h = \left\lfloor \frac{\lfloor\sqrt{4p-7}\rfloor + 1}{2} \right\rfloor = \left\lfloor \frac{\mid A \mid}{2} \right\rfloor$$

elementos distintos de A.

Demonstração. Pelo Teorema 1.1, temos $\mid h\hat{}A \mid \geqslant \min\{p, h \mid A \mid -h^2+1\}$. Se $\mid A \mid$ é ímpar, então $\left\lfloor \frac{|A|}{2} \right\rfloor = \frac{|A|-1}{2}$ e

$$h \mid A \mid -h^2 = h(\mid A \mid -h) = \left(\frac{\mid A \mid -1}{2}\right)\left(\frac{\mid A \mid +1}{2}\right) = \frac{\mid A \mid^2 -1}{4} = \left\lfloor \frac{\mid A \mid^2}{4} \right\rfloor.$$

Se $\mid A \mid$ é par, então

$$h \mid A \mid -h^2 = \frac{\mid A \mid^2}{4} = \left\lfloor \frac{\mid A \mid^2}{4} \right\rfloor.$$

Assim,

$$\mid h\hat{}A \mid \geqslant \min\{p, \left\lfloor \frac{\mid A \mid^2}{4} \right\rfloor + 1\}.$$

Vamos agora mostrar que $\left\lfloor \frac{|A|^2}{4} \right\rfloor + 1 \geqslant p$. Feito isso, obtemos $h\hat{}A = \mathbb{Z}_p$ e o resultado está provado.

Para todo $k \in \mathbb{N}_0$, se k é par então $k^2 \equiv 0 \pmod 4$ e se k é ímpar então $k^2 \equiv 1 \pmod 4$. Assim, $4p-6$ e $4p-5$ não são quadrados e, portanto, não existe $n \in \mathbb{N}$ tal que $\sqrt{4p-7} < n < \sqrt{4p-4}$. Então,

$$\left\lfloor \sqrt{4p-7} \right\rfloor + 1 = \left\lceil \sqrt{4p-4} \right\rceil.$$

De $2\sqrt{p-1} \leqslant \lceil 2\sqrt{p-1} \rceil$ e da equação acima segue que

$$p - 1 \leqslant \frac{\left\lceil \sqrt{4p-4} \right\rceil^2}{4} = \left\lfloor \frac{\mid A \mid^2}{4} \right\rfloor,$$

como queríamos. ■

Capítulo 2

Representação de Grupos Finitos

Neste capítulo apresentamos alguns conceitos e resultados da Teoria de Representações de Grupos Finitos. Denotamos por K um corpo arbitrário e G um grupo finito com identidade e.

2.1 Representações e módulos

Uma *representação* T *de* G *sobre* K é um homomorfismo

$$T : G \to GL(M),$$

onde M é um espaço vetorial de dimensão finita sobre K e $GL(M)$ é o grupo das transformações lineares não singulares de M em M. Nestas condições, dizemos que M é o *espaço de representação* de G e a dimensão $(M : K)$ de M sobre K é o *grau* de T. Duas representações $T_1 : G \to GL(M_1)$ e $T_2 : G \to GL(M_2)$ são *equivalentes* se existe um isomorfismo $S : M_1 \to M_2$ tal que

$$T_2(g) = S^{-1}T_1(g)S, \qquad g \in G.$$

Suponhamos que $(M : K) = m$ e fixemos uma base de M. Podemos identificar M com o espaço K^m das m-uplas sobre K e considerar T como uma aplicação de G em $GL(m, K)$, o grupo das matrizes $m \times m$ não singulares sobre K. Chamamos esta nova aplicação de *representação matricial* de G correspondente a T. Apesar da representação matricial depender da base escolhida, representações matriciais obtidas por bases diferentes são *semelhantes*, donde segue que as representações são equivalentes.

Exemplo 2.1. (Representação permutacional) Seja M um espaço vetorial sobre K com base $\beta = \{u_1, \ldots, u_n\}$. Para $\sigma \in S_n$, o grupo simétrico, seja $P(\sigma) : M \to M$ o homomorfismo definido por

$$P(\sigma)(u_i) = u_{\sigma(i)}, \qquad 1 \leqslant i \leqslant n.$$

Então $P(\sigma\tau) = P(\sigma)P(\tau)$, para todos $\sigma, \tau \in S_n$, e a aplicação $\sigma \mapsto P(\sigma)$ é um homomorfismo de S_n em $GL(M)$.

Seja $[P(\sigma)]_\beta$ a matriz $n \times n$ de $P(\sigma)$ relativa à base β de M. Então $[P(\sigma)]_\beta$ é chamada *matriz permutação* e é caracterizada pela propriedade de que em cada linha e cada coluna existe somente uma entrada não nula, que é igual a 1. A aplicação $\sigma \mapsto [P(\sigma)]_\beta$ é um isomorfismo de S_n sobre o grupo das matrizes permutação em $GL(n, K)$.

Exemplo 2.2. (Representação regular) Um grupo $G = \{g_1, \ldots, g_n\}$ pode ser visto como um grupo de permutação se, para qualquer elemento $g \in G$, definirmos a aplicação $g \mapsto xg$, para todo $x \in G$ (Teorema de Cayley).

Seja agora M um espaço vetorial sobre K e $\{u_1, \ldots, u_n\}$ uma base de M. Para $g \in G$, seja π_g a transformação linear em M definida pela ação

$$\pi_g : u_i \mapsto u_j \text{ se, e somente se, } g : g_i \mapsto g_j.$$

Então a aplicação $\pi : G \to GL(M)$ definida por $\pi(g) = \pi_g$ é uma representação de G que chamamos de *representação regular* de G. Observemos que a representação matricial correspondente, com respeito à base $\{u_1, \ldots, u_n\}$, é dada por matrizes permutação.

Exemplo 2.3. (1-Representações) Seja G um grupo finito com identidade e. Vamos determinar todas as representações de G sobre K de grau 1, chamadas 1-*representações* .

Para isso, considere G' o subgrupo comutador de G. Então G' é gerado pelos elementos $\{xyx^{-1}y^{-1} : x, y \in G\}$ e G/G' é abeliano. Se $T : G \to K$ é qualquer 1-representação de G então

$$T(xyx^{-1}y^{-1}) = T(x)T(y)T(x)^{-1}T(y)^{-1} = 1,$$

ou seja, T leva todo elemento de G' sobre o elemento unidade de K. Conseqüentemente, T induz uma aplicação $\overline{T} : G/G' \to K$ dada por

$$\overline{T}(xG') = T(x), \quad x \in G, \tag{2.1}$$

que é um homomorfismo e, portanto, uma representação de G/G'.

Reciprocamente, começando com a 1-representação $\overline{T}$ de G/G' em K, a equação (2.1) define uma representação de G.

Observemos agora que duas 1-representações são equivalentes se, e somente se, são aplicações iguais. Então existe uma correspondência bijetiva, dada por (2.1), entre as distintas 1-representações T de G e as distintas 1-representações $\overline{T}$ de G/G'.

No caso de $G = S_n$ temos $G' = A_n$, o subgrupo alternado, e $[G : G'] = 2$. Então S_n possui exatamente duas 1-representações, a saber, $\sigma \mapsto 1_K$ e $\sigma \mapsto \text{sgn}\sigma \cdot 1_K$, para todo $\sigma \in S_n$.

Consideremos agora todas as somas formais

$$\sum_{g\in G}\alpha_g g, \qquad \alpha_g \in K,$$

com duas tais expressões sendo iguais se, e somente se, têm os mesmos coeficientes. Definimos operações nas somas formais pelas regras

$$\sum \alpha_g g + \sum \beta_g g = \sum (\alpha_g + \beta_g) g,$$

$$\alpha\left(\sum \alpha_g g\right) = \sum \alpha\alpha_g g, \qquad \alpha \in K, \quad \text{e}$$

$$\left(\sum_{g\in G}\alpha_g g\right)\left(\sum_{h\in G}\beta_h h\right) = \sum_{h,g\in G}\alpha_g\beta_h gh = \sum_{t\in G}\gamma_t t, \quad \text{onde } \gamma_t = \sum_{g\in G}\alpha_g\beta_{g^{-1}t}.$$

Com essas definições, podemos ver que o conjunto KG de todas somas formais é um anel, um espaço vetorial sobre K e satisfaz

$$\alpha(ab) = (\alpha a)b = a(\alpha b), \qquad \alpha \in K,\ a, b \in KG.$$

Chamamos KG de *álgebra de grupo* de G sobre K.

Seja M um espaço vetorial de dimensão finita sobre K. Dizemos que M é um *KG-módulo à esquerda* se, para cada $g \in G$ e $m \in M$, o "produto" gm está definido e satisfaz

$$\begin{gathered} gm \in M, \qquad (gh)m = g(hm), \qquad g(m+m') = gm + gm', \\ em = m, \qquad \alpha(gm) = (\alpha g)m = g(\alpha m), \end{gathered} \tag{2.2}$$

para todos $g \in G$, $m, m' \in M$ e $\alpha \in K$.

O conceito de *KG-módulo à direita* é definido de maneira análoga. Vamos trabalhar, na maioria das vezes, com KG-módulos à esquerda deixando o termo "à esquerda" subentendido, mas tomaremos o cuidado de destacá-lo quando necessário.

Seja então M um KG-módulo e, para cada $g \in G$, defina a aplicação $T(g) : M \to M$ por

$$T(g)m = gm, \qquad m \in M. \tag{2.3}$$

As condições (2.2) asseguram que, para todos $m, m' \in M$ e $\alpha \in K$, vale

$$T(g)(m+m') = T(g)m + T(g)m', \qquad T(g)(\alpha m) = \alpha T(g)m,$$

e portanto $T(g)$ é um homomorfismo. Além disso, temos

$$T(gh) = T(g)T(h), \quad T(\alpha g) = \alpha T(g), \quad T(e) = 1, \quad \text{e} \quad T(g^{-1})T(g) = T(g^{-1}g) = T(e) = 1,$$

quaisquer que sejam $g, h \in G$ e $\alpha \in K$, donde segue que $T : g \mapsto T(g)$ é uma representação de G. Chamamos T de *representação de G correspondente* a M.

Reciprocamente, se $T : G \to GL(M)$ é uma representação de G, a relação (2.3) implica que M é um KG-módulo, que chamamos de *KG-módulo correspondente* à T. Temos, então, uma correspondência bijetiva entre as representações de G (sobre K) e os KG-módulos.

Exemplo 2.4. (Módulo regular) O mais importante exemplo de KG-módulo é a própria álgebra de grupo KG. De fato, a operação

$$g(\sum_{h\in G} \lambda_h h) = \sum_{h\in G} \lambda_h gh = \sum_{t\in G} \lambda_{g^{-1}t} t$$

está bem definida e satisfaz as condições (2.2), donde se conclui que KG é um KG-módulo, que chamamos de *módulo regular*. Sua representação correspondente é, naturalmente, a representação regular definida no Exemplo 2.2.

A idéia agora é trabalharmos com KG-módulos e os resultados obtidos valerem automaticamente para as representações de G sobre K, ou vice-versa. Para isso, temos que garantir que representações equivalentes correspondem a módulos "equivalentes"no seguinte sentido.

Sejam M e M' KG-módulos. Dizemos que M e M' são *KG-isomorfos*, e denotamos por $M \simeq_{KG} M'$, se existe um isomorfismo $S : M \to M'$ tal que, para todo $g \in G$ e $m \in M$, vale

$$g(Sm) = S(gm).$$

Com isso, dois módulos são KG-isomorfos se, e somente se, suas representações correspondentes são equivalentes. Então, a partir de agora, todos os resultados e definições valem tanto para KG-módulos quanto para representações. No entanto, quando relevante, descreveremos o que os resultados e definições feitos para os módulos significam em termos de representações.

Seja M um KG-módulo. Um subespaço N de M é um *KG-submódulo* se $gn \in N$ sempre que $g \in G$ e $n \in N$. Se os únicos submódulos de M são $\{0\}$ e M dizemos que M é *irredutível* e, quando M pode ser escrito como soma direta de submódulos irredutíveis, M é *completamente redutível*. Apresentamos agora alguns resultados importantes sobre a decomposição de M em soma direta de KG-submódulos irredutíveis. As demonstrações de tais resultados podem ser encontradas em [5].

Teorema 2.5 (Maschke [5], pg. 88). *Seja G um grupo finito e K um corpo cuja característica não divide a ordem de G. Então todo KG-módulo é completamente redutível.*

Como a álgebra de grupo KG é um KG-módulo temos que, se a característica de K não

divide a ordem de G,

$$KG = U_1 \oplus \cdots \oplus U_r, \tag{2.4}$$

onde U_i é um KG-módulo irredutível, $i = 1, \ldots, r$. Um resultado ainda mais forte sobre decomposição de módulos é o seguinte.

Teorema 2.6 ([5], pg. 186). *Seja G um grupo finito, K um corpo algebricamente fechado cuja característica não divide a ordem de G e U um KG-módulo irredutível. Consideremos a decomposição de KG dada por (2.4). Então $U \simeq_{KG} U_i$, para algum $1 \leqslant i \leqslant r$, e o número de $U_i's$ com $U_i \simeq_{KG} U$ é igual a $(U : K)$.*

Sob as hipóteses do teorema acima, existe um número finito de KG-módulos irredutíveis não isomorfos que chamamos de *conjunto completo de KG-módulos irredutíveis*. Além disso, temos o seguinte resultado.

Teorema 2.7 ([5], pg. 186). *Seja G um grupo finito e K um corpo algebricamente fechado cuja característica não divide a ordem de G. Então o número de KG-módulos irredutíveis não isomorfos é igual ao número de classes de conjugação de G.*

2.2 Produto tensorial de módulos

Na seção anterior, definimos KG-módulos a partir da álgebra de grupo KG. Podemos também definir módulos sobre um anel R com identidade 1 e isso é feito de maneira análoga. Um grupo abeliano M é um *R-módulo* se, para cada $r \in R$ e $m \in M$, o produto rm está definido e satisfaz

$$r(m_1 + m_2) = rm_1 + rm_2, \quad (r_1 + r_2)m = r_1 m + r_2 m,$$

$$(r_1 r_2)m = r_1(r_2 m) \quad \text{e} \quad 1m = m,$$

para todos $r \in R$ e $m \in M$. Um subgrupo M_1 de M é chamado um *R-submódulo* se $rm_1 \in M_1$ sempre que $r \in R$ e $m_1 \in M_1$. Uma aplicação injetiva f de um R-módulo M sobre um R-módulo M' é chamado um *R-isomorfismo* se $f(m_1 + m_2) = f(m_1) + f(m_2)$ e $f(rm) = rf(m)$, para todos $m \in M$ e $r \in R$. Neste caso, dizemos que $M \simeq M'$ como R-módulos. Aqui estamos omitindo o termo "à esquerda", como convencionamos anteriormente, e de maneira análoga definimos *R-módulos à direita*.

Sejam M e N R-módulos à direita e à esquerda, respectivamente. Dizemos que uma apli-

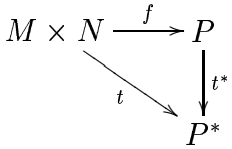
cação f do produto cartesiano $M \times N$ em um grupo abeliano P é *balanceada* se

$$\begin{aligned} f(m_1 + m_2, n) &= f(m_1, n) + f(m_2, n), \\ f(m, n_1 + n_2) &= f(m, n_1) + f(m, n_2), \\ f(m, rn) &= f(mr, n), \end{aligned}$$

para todos $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ e $r \in R$. Uma aplicação balanceada $f : M \times N \to P$ é o *produto tensorial* de M e N se

(i) os elementos $f(m, n)$ geram o grupo P,

(ii) se t é uma aplicação balanceada de $M \times N$ num grupo abeliano P^*, então existe um único homomorfismo $t^* : P \to P^*$ tal que $t = t^* f$, ou seja, tal que o diagrama abaixo comuta.



O teorema que garante a existência e a unicidade do produto tensorial pode ser encontrado em [5], pg. 61.

Denotamos o produto tensorial de M e N por $M \otimes_R N$ e escrevemos $m \otimes n$ para a imagem de (m, n) sobre a aplicação balanceada $M \times N \to M \otimes_R N$.

Vamos agora analisar sob quais condições $M \otimes_R N$ é um módulo sobre um anel. Dizemos que M é um (S, R)-*bimódulo* sobre os anéis com identidade S e R se M é um S-módulo à esquerda, um R-módulo à direita e

$$s(mr) = (sm)r, \qquad \forall\ s \in S,\ m \in M,\ r \in R.$$

Afirmamos que quando M é um (S, R)-bimódulo e N é um R-módulo à esquerda, então $M \otimes_R N$ é um S-módulo à esquerda. De fato, se $s \in S$, a aplicação $(m, n) \mapsto sm \otimes n$ de $M \times N$ em $M \otimes_R N$ é balanceada. Então existe um endomorfismo ψ_s de $M \otimes_R N$ tal que $\psi_s(m \otimes n) = sm \otimes n$. Assim, podemos definir, para cada $s \in S$,

$$s\left(\sum m_i \otimes n_i\right) = \psi_s\left(\sum m_i \otimes n_i\right) = \sum sm_i \otimes n_i$$

e concluímos que $M \otimes_R N$ é um S-módulo com respeito a essa operação.

As seguintes observações, cujas demonstrações podem ser encontradas em [5], são importantes para o estudo de módulos induzidos.

Observação 2.8 ([5], pg. 64). Sejam N um R-módulo à esquerda e M, M_1, M_2 (S,R)-bimódulos tais que $M = M_1 \oplus M_2$. Então

$$M \otimes_R N \simeq (M_1 \otimes_R N) \oplus (M_2 \otimes_R N),$$

como S-módulos à esquerda.

Como o anel R é um (R,R)-bimódulo, o produto tensorial $R \otimes_R N$ é um R-módulo à esquerda. Além disso, vale a seguinte observação.

Observação 2.9 ([5], pg. 67). Seja N um R-módulo à esquerda. Então $R \otimes_R N \simeq N$.

Utilizando os resultados acima, vamos definir o produto tensorial de dois espaços vetoriais M e N de dimensão finita sobre um corpo arbitrário K. Podemos olhar M como um (K,K)-bimódulo e portanto $M \otimes_K N$ é um espaço vetorial sobre K se definirmos

$$\alpha(\sum u_i \otimes v_i) = \sum \alpha u_i \otimes v_i, \qquad \alpha \in K, u_i \in M, v_i \in N.$$

Se $(M : K) = r$ então M é isomorfo à uma soma direta de r cópias de K. Assim, pelas Observações (2.8) e (2.9), temos que

$$M \otimes_K N \simeq N \oplus \cdots \oplus N, \qquad (r \text{ cópias})$$

como K-módulos. Isso prova que

$$(M \otimes_K N : K) = (M : K)(N : K).$$

Suponhamos agora que $\{m_1, \ldots, m_r\}$ é uma base de M e $\{n_1, \ldots, n_s\}$ é uma base de N. Usando a distributividade do produto tensorial, vemos que todo elemento de $M \otimes_K N$ é expresso como

$$\sum_{i=1}^{r} \sum_{j=1}^{s} \alpha_i \beta_j (m_i \otimes n_j), \qquad \alpha_i, \beta_j \in K.$$

Logo os elementos $\{m_i \otimes n_j \ : \ 1 \leqslant i \leqslant r, \ 1 \leqslant j \leqslant s\}$ formam uma K-base de $M \otimes_K N$, visto que a dimensão de $M \otimes_K N$ é rs.

É interessante descrevermos o que esses resultados significam em termos de representações. Sejam $T : G \to GL(M)$ e $U : G \to GL(N)$ representações de um grupo finito G. Então a *representação produto tensorial*

$$T \otimes U : G \to GL(M \otimes_K N)$$

é a aplicação que leva cada $g \in G$ na transformação linear $(T \otimes U)(g)$ definida por

$$(m \otimes n) \mapsto T(g)(m) \otimes U(g)(n), \qquad m \in M, n \in N.$$

A verificação de que $T \otimes U$ é de fato uma representação de G utiliza a expressão

$$(f \otimes g)(f' \otimes g') = ff' \otimes gg',$$

onde f, f', g, g' são homomorfismos entre espaços vetoriais sobre K.

2.3 Representações e módulos induzidos

Dado um subgrupo H de G, todo KG-módulo L é também um KH-módulo, que denotamos por $L \downarrow H$. Apesar de L e $L \downarrow H$ terem o mesmo espaço vetorial subordinado, o domínio dos operadores de $L \downarrow H$ é KH, e não KG. Nesta seção, consideraremos a situação oposta. Vamos descrever uma construção que associa a cada KH-módulo M um KG-módulo. Para tanto, seja M um KH-módulo à esquerda. Como KG é um (KG, KH)-bimódulo, podemos formar o KG-módulo à esquerda

$$M \uparrow G = KG \otimes_{KH} M,$$

que chamamos *módulo induzido* de M. Dizemos que a representação de G correspondente a $M \uparrow G$ é uma *representação induzida.*

Para descrevermos $M \uparrow G$ vamos começar com uma decomposição de G nas classes laterais de H,

$$G = g_1 H \cup \cdots \cup g_t H,$$

onde $t = [G : H]$ e $g_1 = e$. Todo elemento de G é expresso como um produto $g_i h$, com $1 \leqslant i \leqslant t$ e $h \in H$ unicamente determinados. Então, todo elemento de KG é escrito como

$$\sum_{i=1}^{t} g_i b_i, \qquad b_i \in KH,$$

de forma única, donde segue que $KG = g_1 KH \oplus \cdots \oplus g_t KH$ é um KH-módulo à direita com base $\{g_1, \ldots, g_t\}$.

Usando a Observação 2.8 obtemos

$$M \uparrow G = (g_1 KH \otimes_{KH} M) \oplus \cdots \oplus (g_t KH \otimes_{KH} M)\,. \tag{2.5}$$

Além disso, de $g_i KH \simeq KH$ como KH-módulos à direita, este isomorfismo dado por $g_i b \mapsto b$, e da Observação 2.9, segue que

$$g_i KH \otimes_{KH} M \simeq KH \otimes_{KH} M \simeq M$$

e portanto

$$(M \uparrow G : K) = [G : H]\,(M : K)\,. \tag{2.6}$$

Como $g_i r \otimes m = g_i \otimes rm$, podemos reescrever a expressão (2.5) como

$$M \uparrow G = (g_1 \otimes_{KH} M) \oplus \cdots \oplus (g_t \otimes_{KH} M) \tag{2.7}$$

e todo elemento de $M \uparrow G$ pode ser expresso, de maneira única, como $\sum g_i \otimes u_i$, com os u_i's em M unicamente determinados. Segue disso e da equação (2.6) que se $\beta = \{m_1, \ldots, m_r\}$ é uma base de M, então

$$\beta \uparrow G = \{g_i \otimes m_j : 1 \leqslant i \leqslant t, 1 \leqslant j \leqslant r\} \tag{2.8}$$

é uma base de $M \uparrow G$.

Uma observação importante é que a construção acima independe da escolha dos representantes $g_1, \ldots, g_t$. Isso porque se $g_i h = g_{i'} h'$ para certos $h, h' \in H$, então $g_i \otimes M = g_i h \otimes M = g_{i'} h' \otimes M = g_{i'} \otimes M$.

Vamos agora determinar uma representação matricial correspondente a $M \uparrow G$, quando conhecemos uma representação matricial correspondente a M. Suponhamos que, relativo à base β, M corresponde à representação T tal que

$$hm_i = \sum_{j=1}^{r} \alpha_{ji}(h)\ m_j\ , \qquad [T(h)]_\beta = (\alpha_{ji}(h))\,, \qquad h \in H. \tag{2.9}$$

Com respeito à base $\beta \uparrow G$ de $M \uparrow G$, vamos calcular a representação $T \uparrow G$ correspondente à $M \uparrow G$. Para isso, devemos expressar $g\,(g_i \otimes m_j)$ como combinação linear dos elementos da base. Temos

$$g\,(g_i \otimes m_j) = g g_i \otimes m_j$$

e, como $g g_i \in G$, podemos escrever $g g_i = g_k h$, para certos $1 \leqslant k \leqslant t$ e $h \in H$. Então

$$\begin{aligned} g\,(g_i \otimes m_j) &= g_k h \otimes m_j = g_k \otimes h m_j \\ &= g_k \otimes (\textstyle\sum_{l=1}^{r} \alpha_{lj}(h)\ m_l) \\ &= \textstyle\sum_{l=1}^{r} \alpha_{lj}(h) g_k \otimes m_l. \end{aligned}$$

Mas $h = g_k^{-1} g g_i$ e se estendermos o domínio de definição de α_{lj} de H para G fazendo

$$\alpha_{lj}(x) = 0, \qquad \text{se} \quad x \in G \quad \text{e} \quad x \notin H,$$

podemos reescrever nossa fórmula como

$$g\,(g_i \otimes m_j) = \sum_{l=1}^{r} \sum_{k=1}^{t} \alpha_{lj}(g_k^{-1} g g_i)\ g_k \otimes m_l. \tag{2.10}$$

Ordenando os elementos da base $\beta \uparrow G$ como

$$g_1 \otimes m_1, \ldots, g_1 \otimes m_r, g_2 \otimes m_1, \ldots, g_2 \otimes m_r, \ldots, g_t \otimes m_1, \ldots, g_t \otimes m_r,$$

a equação (2.10) implica que, para cada $g \in G$, a matriz de $T \uparrow G(g)$ na base $\beta \uparrow G$ é dada por

$$\begin{pmatrix} [T(g_1^{-1}gg_1)]_\beta & \cdots & [T(g_1^{-1}gg_t)]_\beta \\ \vdots & & \vdots \\ [T(g_t^{-1}gg_1)]_\beta & \cdots & [T(g_t^{-1}gg_t)]_\beta \end{pmatrix}$$

onde $[T(x)]_\beta = 0$ se $x \in G$ e $x \notin H$.

Observação 2.10. Se T é a 1-representação *trivial* de H, ou seja, que leva todo $h \in H$ sobre o elemento identidade 1_K de K, então a representação induzida $T \uparrow G$ é uma representação permutacional das classes laterais de H em G.

A observação acima segue do fato de que, para cada i fixo, $gg_i \in g_kH$, para algum k. Logo $g_k^{-1}gg_i \in H$ e portanto

$$[T(g_k^{-1}gg_i)]_\beta = 1 \quad \text{e} \quad [T(g_j^{-1}gg_i)]_\beta = 0 \text{ se } j \neq k.$$

Observação 2.11. Se $H = \{e\}$ e T é a 1-representação trivial de H então $T \uparrow G$ é equivalente à representação regular de G.

De fato, nas condições acima, o KH-módulo M correspondente a T é isomorfo a K como K-módulos. Segue então da definição de módulo induzido e da Observação 2.9 que

$$M \uparrow G = KG \otimes_{KH} M \simeq KG \otimes_K K \simeq KG.$$

2.4 Critérios de irredutibilidade

Sejam M e N KG-módulos. Denotamos por $\mathrm{Hom}_{KG}(M, N)$ o conjunto de todas as transformações lineares f de M em N tais que $f(gm) = gf(m)$, para todo $g \in G$ e $m \in M$. Naturalmente, $\mathrm{Hom}_{KG}(M, N)$ é um espaço vetorial sobre K, cuja dimensão denotamos por

$$i(M, N).$$

Uma importante propriedade dessa dimensão ([5], pg. 320) é a sua "bilinearidade", isto é, se $M = M_1 \oplus M_2$ então

$$i(M, N) = i(M_1, N) + i(M_2, N). \tag{2.11}$$

Suponhamos agora que char$K$ não divide $|G|$. Então, pelo Teorema 2.5, M e N são completamente redutíveis. Dizemos que M e N possuem um *constituinte em comum* U se, nas decomposições de M e N em soma direta de submódulos irredutíveis, M e N possuem um somando isomorfo a U. Se N é irredutível, dizemos que $k \in \mathbb{N}$ é o *número de vezes que* N *está contido em* M se a decomposição de M contém exatamente k submódulos isomorfos a N. No caso em que K é um corpo algebricamente fechado, é possível calcular o número de constituintes comuns entre M e N através de $i(M, N)$, como diz o seguinte teorema.

Teorema 2.12. *Seja G um grupo finito e K um corpo algebricamente fechado cuja característica não divide a ordem de G. Sejam M um KG-módulo e N um KG-módulo irreduível. Então o número de vezes que N está contido em M é igual a $i(M, N)$. Além disso, M é irredutível se, e somente se, $i(M, M) = 1$.*

Demonstração. Seja $M = M_1 \oplus \cdots \oplus M_r$, onde M_j é irredutível, $j = 1, \ldots, r$. Por (2.11) temos

$$i(M, N) = i(M_1, N) + \cdots + i(M_r, N). \tag{2.12}$$

Seja $f : M_j \to N$ um KG-homomorfismo. Então f é um KG-isomorfismo ou $f \equiv 0$, pois caso contrário Ker$f$ seria um KG-submódulo de M_j. Além disso, afirmamos que se $f : N \to N$ é um KG-isomorfismo, então f é um múltiplo da identidade. De fato, f possui um autovalor $c \in K$ e portanto $\mathrm{Ker}(f - c\ \mathrm{Id}_N)$ é um KG-submódulo de N diferente de zero. Como N é irredutível, temos que $\mathrm{Ker}(f - c\ \mathrm{Id}_N) = N$, donde segue que $f = c\ \mathrm{Id}_N$. (Estes resultados são conhecidos como *Lema de Schur*.)

Com isso, obtemos

$$i(M_j, N) = \begin{cases} 0, & \text{se } M_j \not\simeq_{KG} N, \\ 1, & \text{se } M_j \simeq_{KG} N, \end{cases}$$

o que implica, juntamente com (2.12), as afirmações do teorema.

■

Seja M um KG-módulo com base $\{u_1, \ldots, u_r\}$ e suponha que L é uma extensão de K. Temos que M é um espaço vetorial sobre K que consiste de todas as K-combinações lineares dos elementos $u_1, \ldots, u_r$. Podemos considerar o conjunto de todas as L-combinações lineares dos elementos $u_1, \ldots, u_r$ como um novo espaço vetorial sobre L que contém M e possui a mesma base $\{u_1, \ldots, u_r\}$. Isso pode ser justificado como segue.

Como K é um subcorpo de L, temos L um (L, K)-bimódulo e portanto $L \otimes_K M$ é um espaço vetorial sobre L. Uma vez que M é uma soma direta de r cópias de K, segue das Observações 2.8 e 2.9 que $L \otimes_K M$ é isomorfo (como L-módulo) a uma soma de direta de r cópias de L.

Portanto $(L \otimes_K M : K) = (M : K)$, donde segue que os elementos $1 \otimes u_1, \ldots, 1 \otimes u_r$ formam uma base para $L \otimes_K M$. Temos

$$\alpha \left(\sum \alpha_i \otimes u_i \right) = \sum \alpha\alpha_i \otimes u_i = \sum \alpha\alpha_i (1 \otimes u_i),$$

para todos $\alpha, \alpha_i \in L$. Além disso, podemos identificar M com o subespaço $1 \otimes M$ de $L \otimes_K M$ e, nesse sentido, M é um subespaço de $L \otimes_K M$ e qualquer K-base de M é uma L-base de $L \otimes_K M$. Para simplificar a notação, vamos denotar $L \otimes_K M$ por M^L.

Se extendermos o domínio dos operadores do KG-módulo M para LG, M^L se torna um LG-módulo com operação definida por

$$\left(\sum \lambda_i g_i \right) \left(\sum \mu_i u_i \right) = \sum \lambda_i \mu_i (g_i u_i), \qquad \lambda_i, \mu_i \in L,\ g_i \in G,\ u_i \in M.$$

Sejam T e T^L as representações de G correspondentes a M e M^L, respectivamente. As correspondentes representações matriciais de G são idênticas com respeito às bases $\{u_1, \ldots, u_r\}$ e $\{1 \otimes u_1, \ldots, 1 \otimes u_r\}$. Então, temos T equivalente a T^L e todo esse processo é chamado de *extensão do corpo de representação*.

Seja T uma representação irredutível de G sobre K. Dizemos que T é *absolutamente irredutível* se T^L é irredutível para toda extensão L de K e que K é um *corpo de decomposição* para G se toda representação irredutível de G sobre K é absolutamente irredutível. Seguem abaixo alguns resultados importantes.

Teorema 2.13 ([5], pg. 200). *Sejam M e N KG-módulos e L uma extensão de K. Então, $i(M, N) = i(M^L, N^L)$.*

Teorema 2.14 ([5], pg. 202). *Um KG-módulo M é absolutamente irredutível se, e somente se, $i(M, M) = 1$.*

Seja K um corpo algebricamente fechado cuja característica não divide a ordem de G e M um KG-módulo irredutível. Então, pelo Teorema 2.12, $i(M, M) = 1$. Segue do teorema acima que K é um corpo de decomposição para G. Além disso, vale o seguinte resultado.

Teorema 2.15 ([5], pg. 204). *Seja K um corpo de decomposição para G e L uma extensão de K. Então L é também um corpo de decomposição para G. Se $V_1, \ldots, V_r$ formam um conjunto completo de KG-módulos irredutíveis, então $V_1^L, \ldots, V_r^L$ formam um conjunto completo de LG-módulos irredutíveis.*

Se L é uma extensão de K então char$L$=char$K$. Juntando este fato com os resultados do teorema acima e dos Teoremas 2.13 e 2.14, podemos supor apenas que K é um corpo de

decomposição cuja característica não divide a ordem de G para obtermos os resultados dos Teoremas 2.6, 2.7 e 2.12.

Um procedimento contrário ao de extensão do corpo de representação é o seguinte. Seja $T : G \to GL(n, L)$ uma representação matricial de G. Dizemos que T pode ser *realizada* sobre um subcorpo K de L se existe uma representação matricial $U : G \to GL(n, K)$ tal que U e T são representações (sobre L) equivalentes. Na terminologia de módulos, se M é um LG-módulo correspondente a T, então M pode ser realizado sobre K se, e somente se, existe um KG-módulo N tal que $M \simeq_{LG} N^L$. Uma caracterização de corpos de decomposição em termos desse conceito é a seguinte.

Teorema 2.16 ([5], pg. 465). *Seja K^* um corpo algebricamente fechado. Um subcorpo K de K^* é um corpo de decomposição para G se, e somente se, toda representação sobre K^* irredutível pode ser realizada sobre K.*

Suponhamos agora que T é uma representação de G no corpo $\mathbb{Q}$ dos números racionais. Pode-se mostrar (confira teorema abaixo), numa forma bem mais geral, que T é equivalente a uma outra representação U com a propriedade de que, para todo $g \in G$, a matriz de $T(g)$ possui suas entradas em $\mathbb{Z}$. Se cada inteiro da matriz $[T(g)]$ é trocado por sua classe módulo um primo p, obtemos uma matriz $\overline{[T(g)]}$ com coeficientes em $\mathbb{Z}_p$. Com isso, $[\overline{T}(g)] = \overline{[T(g)]}$ é uma representação de G sobre $\mathbb{Z}_p$. O teorema abaixo formaliza esse resultado.

Teorema 2.17 ([5], pg. 592). *Seja K um corpo de números algébricos e R o anel de inteiros algébricos em K. Seja P um ideal primo em R, p o único racional primo em P e $\overline{K} = K/P$ (corpo finito de característica p). Se K é um corpo de decomposição para G, então $\overline{K}$ também é um corpo de decomposição para G.*

Uma importante conseqüência dos Teoremas 2.16 e 2.17 é a seguinte.

Corolário 2.18. *Se toda representação irredutível de um grupo finito G pode ser realizada sobre $\mathbb{Q}$, então todo corpo é um corpo de decomposição para G.*

2.5 Produto tensorial externo

Sejam G_1 e G_2 grupos finitos e $P = G_1 \times G_2$ o produto direto. Seja L_i um KG_i-módulo, $i = 1, 2$. O *produto tensorial externo* $L_1 \# L_2$ de L_1 e L_2 é o KP-módulo cujo espaço vetorial subordinado é $L_1 \otimes_K L_2$ e a operação do módulo é dada por

$$(g_1, g_2)(l_1 \otimes l_2) = g_1 l_1 \otimes g_2 l_2, \quad (g_1, g_2) \in P,\ l_i \in L_i,$$

e estendida à KP e $L_1 \otimes_K L_2$ por linearidade.

Em termos de representações, se T_1 e T_2 são representações de G_1 e G_2 correspondentes aos módulos L_1 e L_2, respectivamente, então o módulo $L_1\#L_2$ corresponde à representação $T_1\#T_2$ de P, onde

$$(T_1\#T_2)(g_1, g_2) = T_1(g_1) \otimes T_2(g_2), \qquad (g_1, g_2) \in P.$$

Vamos agora relacionar os conceitos de produto tensorial (interno), que vimos na seção 2.2, e produto tensorial externo. Seja G_Δ o *subgrupo diagonal* de $G \times G$, isto é, $G_\Delta = \{(g, g) \ : \ g \in G\}$. Então $G_\Delta \simeq G$ e, se os identificarmos, temos

$$(L_1\#L_2) \downarrow G_\Delta \simeq L_1 \otimes_K L_2,$$

como KG-módulos, ou em termos de representações

$$(T_1\#T_2) \downarrow G_\Delta \sim T_1 \otimes T_2,$$

onde "$\sim$" denota equivalência.

O teorema abaixo, cuja demonstração pode ser encontrada em [5], garante a associatividade do produto tensorial externo.

Teorema 2.19 ([5], pg. 316). *Para $i = 1, 2$, seja H_i um subgrupo de G_i e L_i um KH_i-módulo à esquerda. Então,*

$$(L_1\#L_2) \uparrow (G_1 \times G_2) \simeq (L_1 \uparrow G_1) \# (L_2 \uparrow G_2).$$

2.6 O teorema do número de constituintes comuns

O objetivo desta seção é estudar a decomposição em soma direta do produto tensorial de dois módulos induzidos, $(M \uparrow G) \otimes (N \uparrow G)$ onde M e N são módulos para subgrupos de G, e achar uma fórmula para o número de constituintes comuns entre $M \uparrow G$ e $N \uparrow G$. Essa teoria é em grande parte devido a Frobenius.

Primeiramente, vamos dar uma caracterização conveniente dos módulos induzidos.

Lema 2.20. *Sejam H um subgrupo de G e M um KG-módulo tal que, para algum KH-submódulo N de $M \downarrow H$, M é uma soma direta*

$$M = \bigoplus_{i=1}^{t} g_i N,$$

onde os $\{g_i\}$ *formam um conjunto completo de representantes das classes laterais de* H *em* G. *Então,*

$$M \simeq N \uparrow G$$

como KG*-módulos.*

Demonstração. Por (2.7), temos que $N \uparrow G = (g_1 \otimes N) \oplus \cdots \oplus (g_t \otimes N)$. Este fato e a hipótese $M = \bigoplus_{i=1}^{t} g_i N$ implicam que

$$\sum g_i \otimes n_i \mapsto \sum g_i n_i$$

é um KG-isomorfismo de $N \uparrow G$ sobre N.

■

Dados S e R subgrupos de G, o conjunto $SxR = \{sxr : s \in S \text{ e } r \in R\}$ é chamado de a (S,R)-*classe dupla* de G contendo $x \in G$. Como SxR independe do representante x, G possui uma decomposição em classes laterais duplas disjuntas

$$G = Sx_1R \cup \cdots \cup Sx_tR.$$

Entretanto, diferentes classes duplas podem ter diferentes cardinalidades. Por exemplo, sejam

$$G = S_3, \quad S = \{(1),(12)\} \quad \text{e} \quad R = \{(1),(13)\}.$$

Então as (S,R)-classes duplas de G são

$$S(1)R = \{(1),(12),(13),(132)\} \quad \text{e} \quad S(23)R = \{(23),(123)\}.$$

Seja N um KR-módulo.Vamos mostrar que a estrutura do KS-módulo

$$(N \uparrow G) \downarrow S$$

é determinada pelas (S,R)-classes duplas de G. Consideremos G como a união disjunta das classes laterais $x_1R, \ldots, x_qR$. Então, por (2.7),

$$N \uparrow G = \bigoplus_{i=1}^{q} (x_i \otimes N).$$

Consideremos uma (S,R)-classe dupla SaR fixada e todas as classes laterais x_iR tais que $x_iR \subset SaR$, digamos

$$x_1R, \ldots, x_hR \subset SaR.$$

Observemos que uma classe lateral x_iR não pode interceptar duas classes duplas distintas. De fato, se $x_ir,\ x_ir' \in x_iR$ são tais que $x_ir \in SaR$ e $x_ir' \in SbR$, então $x_i \in SaR \cap SbR$ e portanto $a = b$. Seja

$$W = \bigoplus_{i=1}^{h}(x_i \otimes N).$$

Então W é um KS-submódulo de $N \uparrow G$, pois se $w = (x_1 \otimes n_1) + \cdots + (x_h \otimes n_h) \in W$, temos que $sw = (sx_1 \otimes n_1) + \cdots + (sx_h \otimes n_h) \in W$, para todo $s \in S$. De fato, $sx_i \in x_jR$, para algum j. Então $sx_iR = x_jR$ e, como $x_iR \subset SaR$, temos $x_jR = sx_iR \subset SaR$, donde segue que $sw \in W$. Além disso, W depende somente da (S, R)-classe dupla SaR e não dos representantes $\{x_i\}$ de R em G.

Para cada $x_iR \subset SaR$, existe $s_i \in S$ tal que

$$x_iR = s_iaR$$

e $s_iaR = s_jaR$ se, e somente se, $a^{-1}s_j^{-1}s_ia \in R$ ou ainda se, e somente se, $s_j^{-1}s_i \in a^{-1}Ra \cap S$. Portanto, $s_1, \ldots, s_h$ pertencem a classes laterais distintas do subgrupo

$$\widetilde{R} = a^{-1}Ra \cap S$$

de S. Além disso, para todo $s \in S$, temos que $sa \in SaR$ e $sa \in x_iR$, para algum i. Então $sa = s_iar$, para algum $r \in R$, donde segue que $s \in s_i\widetilde{R}$. Assim, $\{s_i\}_{i=1}^{h}$ forma um conjunto completo de representantes das classes laterais de $\widetilde{R}$ em S.

Voltando ao KS-módulo W, obtemos

$$W = \bigoplus_{i=1}^{h}(x_i \otimes N) = \bigoplus_{i=1}^{h}(s_ia \otimes N) = \bigoplus_{i=1}^{h} s_i(a \otimes N),$$

onde $a \otimes N$ é um $K(aRa^{-1})$-módulo. Como $\widetilde{R} \subset aRa^{-1}$, então $a \otimes N$ é um $K\widetilde{R}$-submódulo de W e, pelo Lema 2.20, obtemos

$$W \simeq \Big((a \otimes N) \downarrow \widetilde{R}\Big) \uparrow S$$

como KS-módulos. Isso prova o seguinte resultado.

Teorema 2.21. (Teorema do Subgrupo) *Sejam R e S subgrupos de G e N um KR-módulo, onde K é um corpo arbitrário. Então, para cada (S, R)-classe dupla SaR, temos que $a \otimes N$ é um $K(a^{-1}Ra)$-submódulo para o subgrupo*

$$\widetilde{R} = aRa^{-1} \cap S$$

de S e

$$\left((a \otimes N) \downarrow \widetilde{R}\right) \uparrow S$$

é um KR-módulo que depende somente da classe dupla SaR. Além disso,

$$(N \uparrow G) \downarrow S = \bigoplus_{SaR} \left((a \otimes N) \downarrow \widetilde{R}\right) \uparrow S$$

como KS-módulos, onde a soma é tomada sobre todas as (S,R)-classes duplas SaR de G.

O próximo teorema é, essencialmente, um corolário do Teorema do Subgrupo. Ele nos dá uma informação sobre a decomposição em soma direta do produto tensorial $(L_1 \uparrow G) \otimes (L_2 \uparrow G)$ de dois módulos induzidos de subgrupos de G.

Teorema 2.22. (Teorema do Produto Tensorial) *Sejam H_i um subgrupo de G e L_i um KH_i-módulo, $i = 1, 2$. Para $x, y \in G$ fixados, defina*

$$H^{(x,y)} = xH_1x^{-1} \cap yH_2y^{-1},$$

$$L_1^{(x)} = x \otimes L_1 \ \subset L_1 \uparrow G,$$

$$L_2^{(y)} = y \otimes L_2 \subset L_2 \uparrow G.$$

Então $L_1^{(x)}$ e $L_2^{(y)}$ são $KH^{(x,y)}$-módulos. Além disso, o módulo induzido $(L_1^{(x)} \otimes L_2^{(y)}) \uparrow G$ depende somente da (H_1, H_2)-classe dupla D de G a qual $x^{-1}y$ pertence e

$$(L_1 \uparrow G) \otimes (L_2 \uparrow G) = \bigoplus_{\substack{D \\ x^{-1}y \in D}} \left[\left(L_1^{(x)} \otimes L_2^{(y)}\right)\right],$$

onde a soma é tomada sobre todas as (H_1, H_2)-classes duplas D de G.

Demonstração. Para mostrarmos o resultado, basta fazer o seguinte paralelo com o Teorema do Subgrupo.

Teorema do produto tensorial	Teorema do Subgrupo
$G \times G$	G
$H_1 \times H_2$	R
G_Δ (o subgrupo diagonal de $G \times G$)	S
$L_1 \# L_2$	N
$(x,y)(H_1 \times H_2)(x,y)^{-1} \cap G_\Delta$ $\simeq xH_1x^{-1} \cap yH_2y^{-1} = H^{(x,y)}$	$\widetilde{R} = aRa^{-1} \cap S$
$(x,y) \otimes (L_1 \# L_2)$ $\simeq (x \otimes L_1) \otimes (y \otimes L_2) = L_1^{(x)} \otimes L_2^{(y)}$	$a \otimes N$

Os detalhes dessa prova podem ser encontrados em [5], pg. 325.

■

Como corolário, reescrevemos o resultado correspondente ao Teorema do Produto Tensorial para representações.

Corolário 2.23. *Seja H_i um subgrupo de G e T_i uma representação de H_i, $i = 1, 2$. Então, para $x, y \in G$ fixados,*

$$T_1^{(x)} : g \mapsto T_1(x^{-1}gx) \quad e \quad T_2^{(y)} : g \mapsto T_1(y^{-1}gy)$$

são representações do subgrupo $xH_1x^{-1} \cap yH_2y^{-1}$ de G. Além disso, a representação induzida $(T_1^{(x)} \otimes T_2^{(y)}) \uparrow G$ depende somente da (H_1, H_2)-classe dupla D a qual que $x^{-1}y$ pertence e

$$(T_1 \uparrow G) \otimes (T_2 \uparrow G) = \bigoplus_{\substack{D \\ x^{-1}y \in G}} \left[\left(T_1^{(x)} \otimes T_2^{(y)} \right) \uparrow G \right],$$

onde a soma é tomada sobre todas as (H_1, H_2)-classes duplas D em G.

O próximo resultado será muito importante quando estudarmos as representações do grupo simétrico S_n. Ele é o ponto de partida para esse estudo. Sua demonstação é uma consequência do Teorema do Produto Tensorial e os detalhes podem ser encontrados em [5], pg. 327.

Teorema 2.24. (Teorema do Número de Constituintes Comuns) *Sob as mesmas hipóteses e notações do Teorema 2.22, para $x, y \in G$ fixados, temos que $i(L_1^{(x)}, L_2^{(y)})$ depende somente da (H_1, H_2)-classe dupla D em G a qual $x^{-1}y$ pertence. Além disso,*

$$i\left(L_1 \uparrow G, L_2 \uparrow G\right) = \sum_{\substack{D \\ x^{-1}y \in D}} i\left(L_1^{(x)}, L_2^{(y)}\right),$$

onde a soma é tomada sobre todas as (H_1, H_2)-classes duplas D em G.

2.7 Os caracteres de um grupo finito

A teoria de caracteres de um grupo finito é um poderoso método para o estudo de suas representações e vai muito além do que expomos aqui. Apresentamos nesta seção somente alguns resultados básicos que seguem como simples consequências do que vimos nas seções anteriores.

Seja M um KG-módulo com base $\{u_1, \ldots, u_r\}$. Então

$$gu_i = \sum_{j=1}^{r} t_{ji}(g)u_j, \qquad t_{ji}(g) \in K, \ g \in G,$$

e M corresponde a representação matricial $g \mapsto [T(g)]$ de G, onde $[T(g)] \in GL(r, K)$ e possui $t_{ij}(g)$ como a entrada (i, j).

Denotamos por tr o traço da matriz de uma tranformação linear e dizemos que a aplicação $\chi : G \mapsto K$ definida por

$$\chi(g) = tr[T(g)] = \sum_{i=1}^{r} t_{ii}(g)$$

é um *caracter* de G correspondente a M (ou a T). Se M é irredutível, então dizemos que χ é um *caracter irredutível*. Como o traço de uma transformação linear independe da escolha da base, temos que o mesmo é válido para um caracter de G. Com isso, módulos isomorfos e representações equivalentes possuem o mesmo caracter.

Observemos que

$$\chi(e) = r = (M : K).$$

Além disso, o valor $\chi(g)$ depende somente da classe de conjugação que contém g. De fato, como $tr(AB) = tr(BA)$, temos

$$\chi(g) = tr[T(g)] = tr[T(h)][T(g)][T(h)]^{-1} = tr[T(hgh^{-1})] = \chi(hgh^{-1}),$$

para todos $g, h \in G$.

Exemplo 2.25 (Caracter permutação). Seja P a representação permutacional de S_n definida no Exemplo 2.1. Então o *módulo permutação* M com base $\{u_1, \ldots, u_n\}$ correspondente à P possui a operação do módulo definida por

$$\sigma u_i = u_{\sigma(i)}, \quad i = 1, \ldots, n \text{ e } \sigma \in S_n.$$

A entrada (i, i) da matriz $[P(\sigma)]$ na base $\{u_1, \ldots, u_n\}$ é igual a 0 se $\sigma(i) = i$ e igual a 1 se $\sigma(i) \neq i$. Portanto, o *caracter permutação* ξ do módulo permutação M é dado por

$$\xi(\sigma) = |\{i \ : \ \sigma(i) = i\}|, \quad \sigma \in S_n.$$

Exemplo 2.26 (Caracter regular). Vamos calcular o caracter χ_{reg} de G correspondente ao módulo regular KG construído no Exemplo 2.4.

Consideremos $G = \{g_1, \ldots, g_n\}$ e, para cada $g \in G$, seja

$$gg_i = \sum_{j=1}^{n} t_{ji}(g) g_j, \quad t_{ji}(g) \in K.$$

Temos $\chi(e) = n = |G|$ e se $g \neq e$ então gg_i é um elemento do grupo distinto de g_i, para todo $g \in G$ e $i = 1, \ldots, n$, donde segue que $t_{ii}(g) = 0$. Portanto,

$$\chi_{\text{reg}} = \begin{cases} |G|, & g = e, \\ 0, & g \neq e. \end{cases}$$

Suponhamos que a característica de K não divide a ordem de G e seja M um KG-módulo. Pelo Teorema 2.5 temos

$$M = M_1 \oplus \cdots \oplus M_r,$$

onde M_i é um submódulo irredutível de M, para $i = 1, \ldots, r$. Seja β_i uma base de M_i e T_i a representação correspondente a M_i, $i = 1, \ldots, r$. Então $\beta = \{\beta_1, \ldots, \beta_r\}$ é uma base de M e sua correspondente representação matricial T tem a forma

$$g \mapsto [T(g)]_\beta = \begin{pmatrix} [T_1(g)]_{\beta_1} & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & [T_r(g)]_{\beta_r} \end{pmatrix}, \quad g \in G. \tag{2.13}$$

Se χ e χ_i são os caracteres de G correspondentes a M e M_i, $i = 1, \ldots, r$, respectivamente, então de (2.13) segue que

$$\chi(g) = \chi_1(g) + \cdots + \chi_r(g).$$

Se K é um corpo de decomposição para G cuja característica não divide a ordem de G, existe um conjunto completo de KG-módulos irredutíveis não isomorfos que denotamos por $\{U_1, \ldots, U_s\}$, onde s é igual ao número de classes de conjugação em G. Seja ζ_j o caracter de G correspondente a U_j, $j = 1, \ldots, s$. Abusando da notação, pelo Teorema 2.6 temos

$$KG \simeq (U_1 \oplus \cdots \oplus U_1) \oplus (U_2 \oplus \cdots \oplus U_2) \oplus \cdots \oplus (U_s \oplus \cdots \oplus U_s),$$

onde, para cada $1 \leqslant j \leqslant s$, aparecem $(U_j : K) = \zeta_j(e)$ fatores "iguais" (isomorfos) a U_j. Então,

$$|G| = \chi_{\text{reg}}(e) = (\zeta_1(e))^2 + \cdots + (\zeta_s(e))^2.$$

Consideremos agora um KG-módulo M arbitrário. Escrevemos

$$M \simeq a_1 U_1 + \cdots + a_s U_s,$$

onde os $a_j's$ são inteiros não negativos e indicam que a decomposição de M em módulos irredutíveis possui exatamente a_j submódulos isomorfos a U_j. Pelo Teorema 2.12, temos $a_j = i(M, U_j)$, $j = 1, \ldots, s$, e se χ é o caracter correspondente a M obtemos

$$\chi(g) = \sum_{j=1}^{r} i(M, U_j)\ \zeta_j(g), \quad g \in G, \tag{2.14}$$

donde concluímos que χ (e todo caracter de G) pode ser escrito como $\mathbb{Z}$-combinação linear dos caracteres $\zeta_1, \ldots, \zeta_s$.

Capítulo 3

Representações do Grupo Simétrico

No Capítulo 2, apresentamos alguns resultados e definições de representações de um grupo finito G arbitrário. Quando G é o grupo simétrico S_n, podemos descrever propriedades interessantes de suas representações. Algumas delas encontram-se neste capítulo.

A teoria que desenvolvemos aqui visa estabelecer uma fórmula para o grau das representações irredutíveis de S_n (Teorema 3.20) e uma fórmula de recursão para esses caracteres (Teorema 3.23). Denotamos a identidade de S_n por 1 e $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$.

3.1 Subgrupos de Young e suas 1-representações

Seja $n \in \mathbb{N}$. Dizemos que uma sequência de inteiros não negativos $\alpha = (\alpha_1, \ldots, \alpha_h)$, com $h \leqslant n$, é uma *composição* de n se

$$\sum_{i=1}^{h} \alpha_i = n. \tag{3.1}$$

Se, além de (3.1), temos

$$\alpha_1 \geqslant \alpha_2 \geqslant \cdots \geqslant \alpha_h \ , \tag{3.2}$$

então dizemos que α é uma *partição* de n, o que denotamos por $\alpha \vdash n$. As coordenadas de α são chamadas de *partes* de α. Usaremos, quando preciso, uma identificação da partição α com uma n-upla fazendo $\alpha_i = 0$, para $h < i \leqslant n$.

Consideremos o grupo simétrico S_n. Sabemos que cada permutação pode ser unicamente determinada como o produto de ciclos disjuntos, chamados fatores cíclicos. Com esta notação cíclica podemos estabelecer uma bijeção entre as classes de conjugação de S_n e o conjunto

$$P(n) = \{\alpha : \alpha \vdash n\},$$

considerando a aplicação

$$\pi \in S_n \mapsto c(\pi),$$

onde $c(\pi)$ representa os comprimentos dos fatores cíclicos de π ordenados.

Exemplo 3.1. Seja $\pi = (12)(345) \in S_7$. Então $\pi = (12)(345)(6)(7)$ e $\pi \mapsto (3, 2, 1, 1)$.

Como dois elementos em S_n são conjugados se, e somente se, possuem a mesma estrutura cíclica, então dois elementos em S_n possuem a mesma partição associada se, e somente se, pertencem à mesma classe de conjugação. Assim, podemos indexar as classes de conjugação de S_n por partições de n. Como o número de representações irredutíveis não equivalentes de um grupo finito G é igual ao número de classes de conjugação deste grupo, isto sugere que também relacionemos subgrupos de S_n, usados na teoria de representações, com as partições.

À uma composição $\lambda = (\lambda_1, \ldots \lambda_h)$ de n, associamos subconjuntos de $N = \{1, 2, \ldots, n\} \subset \mathbb{Z}$ dois a dois disjuntos, que denotamos por

$$N_i^\lambda \ , \quad i = 1, \ldots, h \ ,$$

e que satisfazem

$$|N_i^\lambda| = \lambda_i \ , \quad i = 1, \ldots, h \ .$$

Então temos uma *dissecção* de N, isto é, N escrito como uma *união disjunta*, dada por

$$N = \bigcup_{i=1}^{h} N_i^\lambda.$$

Se denotarmos por S_i^λ o subgrupo de S_n consistindo dos $\lambda_i!$ elementos que permutam o conjunto N_i^λ e deixam cada ponto de $N \setminus N_i^\lambda$ fixo, $i = 1, \ldots, h$, então $S_i^\lambda \cap S_k^\lambda = \{1\}$, para $i \neq k$, e $\pi\sigma = \sigma\pi$, para todos $\pi \in S_i^\lambda$, $\sigma \in S_k^\lambda$. Assim, o produto

$$S_\lambda := \prod_{i=1}^{h} S_i^\lambda$$

é um subgrupo de S_n isomorfo ao produto direto

$$S_{\lambda_1} \times S_{\lambda_2} \times \ldots \times S_{\lambda_h}.$$

Chamamos S_λ de *subgrupo de Young* correspondente à composição λ de n. Claramente, cada S_λ, onde λ é uma composição de n, é isomorfo a um S_α, onde $\alpha \vdash n$.

Seja agora K um corpo. Para cada partição λ de n, existem duas 1-representações triviais do subgrupo de Young S_λ, correspondente à λ, de S_n. Uma é a *representação identidade*

$$\begin{aligned} IS_\lambda : \ \ S_\lambda &\to GL(K^1) \\ \pi &\mapsto \mathrm{Id}_{K^1} \end{aligned}$$

onde K^1 é um espaço vetorial unidimensional sobre K, e a segunda é a que chamamos de *representação alternada*

$$\begin{aligned} AS_\lambda : \quad & S_\lambda \to GL(K^1) \\ & \pi \mapsto \mathrm{sgn}\pi \cdot \mathrm{Id}_{K^1}. \end{aligned}$$

Assim, se λ e μ são partições de n, podemos formar IS_λ, IS_μ e AS_μ e induzi-las em S_n obtendo as representações

$$IS_\lambda \uparrow S_n, \ IS_\mu \uparrow S_n \ \text{ e } \ AS_\mu \uparrow S_n$$

de S_n.

Nosso objetivo, a partir de agora, é estudar as dimensões

$$i\left(IS_\lambda \uparrow S_n, IS_\mu \uparrow S_n\right) \ \text{ e } \ i(IS_\lambda \uparrow S_n, AS_\mu \uparrow S_n)$$

para conhecermos o número de constituintes irredutíveis comuns entre essas representações induzidas.

Para isso, podemos aplicar o Teorema 2.24 e ver que

$$i\left(IS_\lambda \uparrow S_n, IS_\mu \uparrow S_n\right) = \sum_{S_\lambda \pi S_\mu} i\left(IS_\lambda \downarrow S_\lambda \cap \pi S_\mu \pi^{-1}, IS_\mu^{(\pi)} \downarrow S_\lambda \cap \pi S_\mu \pi^{-1}\right),$$

onde a soma é tomada sobre todas as classes duplas $S_\lambda \pi S_\mu$ de S_n e $IS_\mu^{(\pi)}(\pi\rho\pi^{-1}) := IS_\mu(\rho)$, para $\rho \in S_\mu$. Então

$$\begin{aligned} i\left(IS_\lambda \uparrow S_n, IS_\mu \uparrow S_n\right) &= \sum_{S_\lambda \pi S_\mu} i\left(I(S_\lambda \cap \pi S_\mu \pi^{-1}), I(S_\lambda \cap \pi S_\mu \pi^{-1})\right) \\ &= \sum_{S_\lambda \pi S_\mu} 1, \end{aligned} \tag{3.3}$$

pois $I(S_\lambda \cap \pi S_\mu \pi^{-1})$ é irredutível.

Analogamente,

$$i\left(IS_\lambda \uparrow S_n, AS_\mu \uparrow S_n\right) = \sum_{S_\lambda \pi S_\mu} i\left(I(S_\lambda \cap \pi S_\mu \pi^{-1}), A(S_\lambda \cap \pi S_\mu \pi^{-1})\right) .$$

Mas $I(S_\lambda \cap \pi S_\mu \pi^{-1})$ e $A(S_\lambda \cap \pi S_\mu \pi^{-1})$ são representações irreduíveis e $S_\lambda \cap \pi S_\mu \pi^{-1}$ é o produto direto de grupos simétricos. Portanto, tais representações irredutíveis são iguais se, e somente se, $S_\lambda \cap \pi S_\mu \pi^{-1} = \{1\}$ ou a característica de K é igual a dois. Assim,

$$i\left(IS_\lambda \uparrow S_n, AS_\mu \uparrow S_n\right) = \begin{cases} \displaystyle\sum_{S_\lambda \pi S_\mu} 1, & \text{se } \mathrm{char}K = 2 \\ \displaystyle\sum_{\substack{S_\lambda \pi S_\mu \\ S_\lambda \cap \pi S_\mu \pi^{-1} = \{1\}}} 1, & \text{caso contrário.} \end{cases} \tag{3.4}$$

Concluímos então, de (3.3) e (3.4), que as dimensões procuradas podem ser encontradas a partir do número de (S_λ, S_μ)-classes duplas de S_n. Assim, dirigiremos nossa atenção a tais classes duplas, começando com o seguinte lema.

Lema 3.2. *Sejam λ, μ partições de n, S_λ e S_μ seus correspondentes subgrupos de Young e $S_\lambda \pi S_\mu$ uma (S_λ, S_μ)-classe dupla de S_n. Então $\rho \in S_\lambda \pi S_\mu$ se, e somente se, $|N_i^\lambda \cap \pi(N_k^\mu)| = |N_i^\lambda \cap \rho(N_k^\mu)|$, para todos $1 \leqslant i, k \leqslant n$, onde $\pi(N_k^\mu)$ é a imagem do conjunto N_k^μ pela permutação π.*

Demonstração. Mostremos inicialmente que a condição é necessária. Se $\rho = \sigma\pi\tau \in S_\lambda \pi S_\mu$ então, para cada k, $\rho(N_k^\mu) = \sigma\pi\tau(N_k^\mu) = \sigma\pi(N_k^\mu)$, pois $\tau \in S_\mu$. Assim, para cada $1 \leqslant i, j \leqslant n$, temos

$$N_i^\lambda \cap \rho(N_k^\mu) = N_i^\lambda \cap \sigma\pi(N_k^\mu) = \sigma(N_i^\lambda) \cap \sigma\pi(N_k^\mu) = \sigma\left(N_i^\lambda \cap \pi(N_k^\mu)\right),$$

o que implica no resultado, pois σ é bijeção.

Reciprocamente, a hipótese $|N_i^\lambda \cap \pi(N_k^\mu)| = |N_i^\lambda \cap \rho(N_k^\mu)|$, para todos $1 \leqslant i, k \leqslant n$, implica que, se fixarmos i, os subconjuntos

$$N_i^\lambda \cap \pi(N_k\mu) \qquad \text{e} \qquad N_i^\lambda \cap \rho(N_k\mu), \qquad k = 1, \ldots, n\ ,$$

formam duas dissecções de N_i^λ em subconjuntos de ordens iguais. Conseqüentemente, para cada i, existe $\sigma_i \in S_i^\lambda$ tal que

$$\sigma_i\left(N_i^\lambda \cap \pi(N_k^\mu)\right) = N_i^\lambda \cap \rho(N_k^\mu), \qquad k = 1, \ldots, n.$$

O produto $\sigma := \sigma_1\sigma_2\cdots\sigma_n \ \in S_\lambda$ de tais permutações satisfaz as equações

$$\sigma\pi(N_k^\mu) = \rho(N_k^\mu), \qquad k = 1, \ldots, n.$$

Então, existe $\tau \in S_\mu$ tal que $\rho = \sigma\pi\tau$, como queríamos.

■

O lema acima mostra que a classe dupla $S_\lambda \pi S_\mu$ é caracterizada pelos números

$$z_{ik} := |N_i^\lambda \cap \pi(N_k^\mu)|, \qquad 1 \leqslant i, k \leqslant n.$$

Então temos uma aplicação injetiva

$$f : S_\lambda \pi S_\mu \mapsto (z_{ik})$$

do conjunto das (S_λ, S_μ)-classes duplas no conjunto das matrizes $n \times n$ (z_{ik}). Observemos que tais matrizes satisfazem

(1) $z_{ik} \in \mathbb{N}_0$, para todos $1 \leqslant i, k \leqslant n$.

(2) $\sum_{i=1}^{n} z_{ik} = \mu_k$ e $\sum_{k=1}^{n} z_{ik} = \lambda_i$.

Isto prova o seguinte teorema.

Teorema 3.3. *Sejam $\lambda = (\lambda_1, \ldots, \lambda_n)$ e $\mu = (\mu_1, \ldots, \mu_n)$ partições de n com correspondentes subgrupos de Young S_λ e S_μ, respectivamente. Então a aplicação*

$$f : S_\lambda \pi S_\mu \mapsto (z_{ik} := |N_i^\lambda \cap \pi(N_k^\mu)|)$$

estabelece uma bijeção entre o conjunto das (S_λ, S_μ)-classes duplas de S_n e o conjunto das matrizes $n \times n$ (z_{ik}) sobre $\mathbb{N}_0$ que satisfazem

$$\sum_{i=1}^{n} z_{ik} = \mu_k \quad e \quad \sum_{k=1}^{n} z_{ik} = \lambda_i.$$

Corolário 3.4. *O número de (S_λ, S_μ)-classes duplas de S_n é igual ao número de matrizes $n \times n$ com entradas em $\mathbb{N}_0$ e que possuem $\lambda = (\lambda_1, \ldots, \lambda_n)$ como vetor das somas dos elementos das linhas e $\mu = (\mu_1, \ldots, \mu_n)$ como vetor das somas dos elementos das colunas.*

Se restringirmos a função f, definida no Teorema 3.3, ao subconjunto das (S_λ, S_μ)-classes duplas $S_\lambda \pi S_\mu$ com a *propriedade de interseção trivial*

$$S_\lambda \cap \pi S_\mu \pi^{-1} = \{1\},$$

obtemos como imagem o conjunto das matrizes $n \times n$ com entradas iguais a 0 ou 1, que chamamos de *matrizes* 0-1, e que possuem λ como vetor soma dos elementos das linhas e μ como vetor soma dos elementos das colunas. De fato, se observarmos que para $\sigma = (i_1 i_2 \cdots) \cdots \in S_\mu^k$ temos $\pi\sigma\pi^{-1} = (\pi(i_1)\pi(i_2)\cdots)\cdots \in \pi S_\mu^k \pi^{-1}$, vemos que $\pi S_\mu^k \pi^{-1}$ é o subgrupo de S_n que permuta exatamente os elementos do conjunto $\pi(N_\mu^k)$, para cada $1 \leqslant k \leqslant n$. Além disso, o fato $S_\lambda \cap \pi S_\mu \pi^{-1} = \{1\}$ implica que $S_\lambda^i \cap \pi S_\mu^k \pi^{-1} = \varnothing$ ou $\{1\}$, para cada $1 \leqslant i, k \leqslant n$. Portanto $|N_i^\lambda \cap \pi(N_k^\mu)|$=0 ou 1, como queríamos.

Corolário 3.5. *O número de (S_λ, S_μ)-classes duplas de S_n com a propriedade de interseção trivial é igual ao número de matrizes 0-1 $n \times n$ com vetor soma dos elementos das linhas igual a λ e vetor soma dos elementos das colunas igual a μ.*

3.2 Representações irredutíveis ordinárias de S_n

Por uma representação irredutível ordinária de S_n entendemos uma representação de S_n sobre o corpo $\mathbb{C}$ dos números complexos. Um dos resultados que apresentaremos nesta seção diz que

cada representação irredutível ordinária de S_n pode ser realizada sobre o corpo $\mathbb{Q}$ dos números racionais. Portanto $\mathbb{Q}$ (e todo corpo) é um corpo de decomposição para S_n, o que implica que não precisamos mais assumir que a característica de K não divide $n!$, bastando simplesmente considerar as representações irredutíveis ordiárias de S_n.

Na seção anterior, consideramos as representações $IS_\alpha \uparrow S_n$ e $AS_\mu \uparrow S_n$ e expressamos o número de constituintes irredutíveis comuns entre elas,

$$i\left(IS_\alpha \uparrow S_n, AS_\mu \uparrow S_n\right),$$

em termos do número de classes duplas e matrizes 0-1. Estes resultados serão utilizados para determinarmos, nesta seção, um conjunto completo de representações irredutíveis de S_n.

Para isso, vamos em busca de pares (α, β) de partições de n com a propriedade

$$i\left(IS_\alpha \uparrow S_n, AS_\mu \uparrow S_n\right) = 1. \tag{3.5}$$

No caso em que a característica de K não divide $n!$, (3.5) nos diz que essas duas representações possuem um único constituinte irredutível em comum que aparece com multiplicidade 1 em $IS_\alpha \uparrow S_n$ e $AS_\mu \uparrow S_n$.

Os chamados *diagramas de Young*, que definiremos a seguir, nos ajudarão a determinar estes pares especiais (α, β) de partições de n.

Considere $\alpha = (\alpha_1, \ldots, \alpha_h)$ uma partição de n. À α associamos o diagrama que consiste de n símbolos $\square$ distribuídos da seguinte maneira:

$$[\alpha] := \begin{array}{ll} \square\ \square\ \cdots\cdots\ \square & \alpha_1 \text{ símbolos} \\ \square\ \square\ \cdots\ \square & \alpha_2 \text{ símbolos} \\ \vdots & \vdots \\ \square\ \cdots\ \square & \alpha_h \text{ símbolos} \end{array}$$

Chamamos $[\alpha]$ de *diagrama de Young* associado à partição α de n.

Observando $[\alpha]$, vemos que os comprimentos de suas colunas formam uma composição de n, que denotamos por

$$\alpha' := (\alpha'_1, \ldots, \alpha'_n), \qquad \text{onde } \alpha'_i = \sum_{\substack{\nu \\ \alpha_\nu \geqslant i}} 1.$$

Lembrando que para $\alpha \vdash n$ temos $\alpha_i \geqslant \alpha_{i+1}$, para todo $1 \leqslant i \leqslant h$, vemos que α' também é uma partição de n, que chamamos de *partição conjugada*. Podemos também observar que o diagrama de Young $[\alpha']$ de α' é obtido de $[\alpha]$ quando trocamos as linhas pelas colunas.

Exemplo 3.6.

$$[(3,2,1,1)] = \begin{array}{l} \square\ \square\ \square \\ \square\ \square \\ \square \\ \square \end{array} \qquad \text{e} \qquad [(3,2,1,1)'] = \begin{array}{l} \square\ \square\ \square\ \square \\ \square\ \square \\ \square \end{array} = [(4,2,1)].$$

Sabemos que

$$i\left(IS_\alpha \uparrow S_n, AS_{\alpha'} \uparrow S_n\right)$$

é igual ao número de matrizes 0-1 com soma da linha i igual a α_i e soma da coluna j igual a α'_j, $1 \leqslant i, j \leqslant h$. Mas existe somente uma matriz que satisfaz estas condições, a saber

$$\begin{pmatrix} 1\ 1\ \cdots\cdots\ 1\ 0\ \cdots\cdot\ 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ 1\ \cdots\ 1\ 0\ \cdots\cdots\cdots\ 0 \end{pmatrix}, \tag{3.6}$$

onde os 1's são colocados em cada linha o mais à esquerda possível. Portanto

$$i\left(IS_\alpha \uparrow S_n, AS_{\alpha'} \uparrow S_n\right) = 1. \tag{3.7}$$

Vamos interpretar a equação acima. Primeiro, lembremos que os resultados são válidos quando a característica de K é diferente de 2 e não divide $n!$. Portanto, podemos olhar para a equação (3.7) como um resultado de representações de S_n sobre $\mathbb{Q}$.

Como, por (2.11), $i(\cdot,\cdot)$ é "bilinear", a equação (3.7) implica que existe exatamente uma $\mathbb{Q}$-representação irredutível, digamos D, que está contida em $IS_\alpha \uparrow S_n$ e $AS_{\alpha'} \uparrow S_n$. Além disso $i(D, D) = 1$, donde segue que D está contida em $IS_\alpha \uparrow S_n$ e $AS_{\alpha'} \uparrow S_n$ com multiplicidade 1 e que D é absolutamente irredutível (Teorema 2.14).

Teorema 3.7. *Sejam α uma partição de n, α' sua partição conjugada e S_α e $S_{\alpha'}$ os subgrupos de Young de S_n correspondentes a α e α', respectivamente. Então as representações induzidas $IS_\alpha \uparrow S_n$ e $AS_{\alpha'} \uparrow S_n$ possuem exatamente um constituinte irredutível ordinário em comum. Além disso, este constituinte irredutível pode ser realizado sobre $\mathbb{Q}$ e está contido com multiplicidade 1 em $IS_\alpha \uparrow S_n$ e $AS_{\alpha'} \uparrow S_n$.*

Se observarmos o diagrama de Young $[\alpha]$ de α e a matriz 0-1 (3.6), podemos ver que apenas "trocamos" os símblos $\square$ do diagrama por 1's, "acrescentando" 0's para "completarmos" a matriz. Isso motiva a notação

$$[\alpha] := IS_\alpha \uparrow S_n \cap AS_{\alpha'} \uparrow S_n$$

para representarmos o constituinte irredutível comum, dado pelo Teorema 3.7. Mas, como a notação $[\alpha]$ indica duas situações, teremos o cuidado de especificar qual delas está sendo representada.

Nosso objetivo agora torna-se mostrar que o conjunto

$$\{[\alpha] : \alpha \text{ é partição de } n\} \tag{3.8}$$

é um conjunto completo de representações irredutíveis ordinárias de S_n. Como já sabemos que a cardinalidade de (3.8) é igual ao número de classes de conjugação de S_n, precisamos apenas mostrar que se $[\alpha] = [\beta]$ então $\alpha = \beta$. Para isto, introduziremos uma ordem parcial no conjunto

$$P(n) = \{\alpha : \alpha \text{ é partição de } n\}.$$

Sejam $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n) \in P(n)$. Dizemos que α é menor do que ou igual a β em relação às *somas parciais*, o que denotamos por $\alpha \preceq \beta$, se

$$\sum_{\nu=1}^{i} \alpha_\nu = \sum_{\nu=1}^{i} \beta_\nu, \qquad \text{para todo } 1 \leqslant i \leqslant n.$$

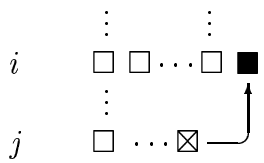
Podemos também definir uma ordem total em $P(n)$. Dizemos que α e β estão em *ordem lexicográfica*, situação que denotamos por $\alpha < \beta$, se existe $1 \leqslant i \leqslant n$ tal que

$$\alpha_1 = \beta_1, \ldots, \alpha_{i-1} = \beta_{i-1} \quad \text{e} \quad \alpha_i < \beta_i.$$

Essas duas ordens, claramente, se relacionam por

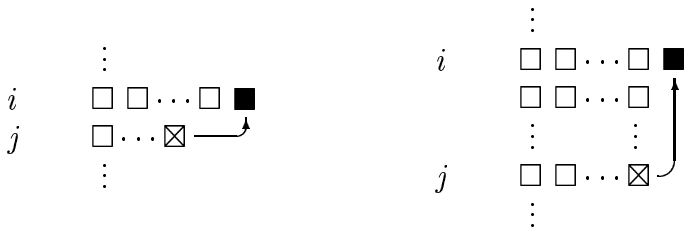
$$\alpha \preceq \beta \Rightarrow \alpha \leqslant \beta. \tag{3.9}$$

Quando $\alpha \prec \beta$ e não existe $\gamma \in P(n)$ tal que $\alpha \prec \gamma \prec \beta$, dizemos que α e β são *vizinhas* com respeito à ordem $\preceq$. Neste caso escrevemos $\alpha \prec\!\!\cdot\, \beta$. Esta situação nos dá uma importante caracterização das partições α e β. No lema abaixo provaremos que partições vizinhas podem ser facilmente expressas em termos dos correspondentes diagramas de Young, isto é, $\alpha \prec\!\!\cdot\, \beta$ se, e somente se, $[\beta]$ pode ser obtido de $[\alpha]$ ao tirarmos um símbolo $\square$ do final de uma certa linha j de $[\alpha]$ e colocarmos em outra linha $i < j$.



Depois deste procedimento precisamos garantir que o diagrama resultante corresponde a uma partição de n. Além disso, o passo acima tem que ser o mais curto possível, isto é, ou $i = j - 1$ ou $i < j - 1$ e $\alpha_i = \alpha_{i+1} = \cdots = \alpha_j$,

(3.10)



para que α e β sejam vizinhas.

Lema 3.8. *Sejam $\alpha = (\alpha_1, \ldots, \alpha_n)$ e $\beta = (\beta_1, \ldots, \beta_n)$ partições de n. Então $\alpha \prec\cdot \beta$ se, e somente se, existem i e j tais que*

(1) $1 \leqslant i < j$;

(2) $\beta_j = \alpha_j - 1$ *e* $\beta_i = \alpha_i + 1$, *enquanto* $\alpha_\nu = \beta_\nu$ *para* $\nu \neq i, j$;

(3) $i = j - 1$ *ou* $\alpha_i = \alpha_j$.

Demonstração. Assumindo $\alpha \prec \beta$, queremos mostrar que existem i, j tais que uma das situações abaixo ocorre:

(Caso 1). $\alpha = (\alpha_1, \ldots, \alpha_{i-1}, \alpha_i, \alpha_{i+1}, \alpha_{i+2}, \ldots, \alpha_h)$ e
$\beta = (\alpha_1, \ldots, \alpha_{i-1}, \alpha_i + 1, \alpha_{i+1} - 1, \alpha_{i+2}, \ldots, \alpha_h)$

(Caso 2). $\alpha = (\alpha_1, \ldots, \alpha_{i-1}, \alpha_i, \alpha_{i+1}, \ldots, \alpha_{j-1}, \alpha_j, \alpha_{j+1}, \ldots, \alpha_h)$, com $\alpha_i = \cdots = \alpha_j$ e
$\beta = (\alpha_1, \ldots, \alpha_{i-1}, \alpha_i + 1, \alpha_{i+1}, \ldots, \alpha_{j-1}, \alpha_j - 1, \alpha_{j+1}, \ldots, \alpha_h)$.

Para isso tomemos

$$i := \min\{\nu : \alpha_\nu \neq \beta_\nu\} \quad \text{e} \quad j := \min\left\{t : \sum_{\nu=1}^{t} \alpha_\nu = \sum_{\nu=1}^{t} \beta_\nu,\ i < t\right\}.$$

Claramente $i < j$ e $\alpha_j > \beta_j$. Além disso, como $\alpha \prec \beta$, temos $\beta_{j+1} \geqslant \alpha_{j+1}$. Se $i > 1$, então $\alpha_i < \beta_i \leqslant \beta_{i-1} = \alpha_{i-1}$ e $\alpha_i + 1 \leqslant \beta_i \leqslant \beta_{i-1} = \alpha_{i-1}$, situação que não precisamos considerar quando $i = 1$. Além do mais, $\alpha_j > \beta_j \geqslant \beta_{j+1} \geqslant \alpha_{j+1}$, o que implica $\alpha_j - 1 \geqslant \alpha_{j+1}$. Portanto obtemos

$$\gamma = (\alpha_1, \ldots, \alpha_{i-1}, \alpha_i + 1, \alpha_{i+1}, \ldots, \alpha_{j-1}, \alpha_j - 1, \alpha_{j+1}, \ldots, \alpha_h)$$

tal que $\alpha \prec \gamma \preceq \beta$, donde segue que $\gamma = \beta$, por hipótese.

Agora se $i \neq j - 1$ e $\alpha_i \neq \alpha_j$, então $i < j - 1$ e $\alpha_i > \alpha_j$. Podemos então tomar

$$t := 1 + \min\{\nu : \alpha_\nu > \alpha_{\nu+1},\ 1 \leqslant \nu < j\}$$

e ver que $i < t \leqslant j$. Se $t = j$, então $\alpha_i = \cdots = \alpha_{j-1} > \alpha_j > 0$ e

$$\alpha \prec (\alpha_1, \ldots, \alpha_{i-1}, \alpha_i + 1, \alpha_{i+1}, \ldots, \alpha_{j-2}, \alpha_{j-1} - 1, \alpha_j, \ldots, \alpha_h) \prec \beta$$

o que contradiz $\alpha \prec \beta$. No caso em que $t < j$ temos $\alpha_i = \cdots = \alpha_{t-1} > \alpha_t \geqslant \cdots \alpha_j > 0$. Assim

$$\alpha \prec (\alpha_1, \ldots, \alpha_{t-1}, \alpha_i + 1, \ldots, \alpha_{j-1}, \alpha_j - 1, \alpha_{j+1}, \ldots, \alpha_h) \prec \beta,$$

o que também é uma contradição. Isto mostra que as condições (1)-(3) são necessárias.

Reciprocamente, seja $\gamma = (\gamma_1, \ldots, \gamma_h) \vdash n$ tal que $\alpha \prec \gamma \preceq \beta$. Como (Caso 1) ou (Caso 2) ocorrem, temos

$$\alpha_\nu = \gamma_\nu = \beta_\nu, \quad \text{sempre que } \nu < i \text{ ou } \nu > j.$$

Segue que se $i = j - 1$, $\alpha \prec \gamma$ implica que $\gamma_i = \alpha_i + 1$ e $\gamma_{i+1} = \alpha_i - 1$. Então $\gamma = \beta$. Agora, se $i \neq j - 1$ então $\alpha_i = \cdots = \alpha_j$. Assim, de $\alpha \prec \gamma$, existem k e l tais que $1 \leqslant k < l \leqslant j$ e

$$\gamma_k = \alpha_k + 1, \quad \gamma_l = \alpha_l - 1 \quad \text{e} \quad \gamma_\nu = \alpha_\nu \ \text{ para } \ \nu \neq k, l.$$

Mas isso só pode acontecer se $k = i$ e $l = j$ pois, caso contrário, teríamos

$$\alpha_k = \gamma_k - 1 \leqslant \gamma_{k-1} - 1 = \alpha_{k-1} - 1 < \alpha_{k-1} = \alpha_i$$

ou

$$\alpha_l = \gamma_l + 1 \geqslant \gamma_{l+1} + 1 = \alpha_{l+1} + 1 > \alpha_{l+1} = \alpha_j,$$

contradizendo $\alpha_i = \cdots = \alpha_j$. Portanto $\gamma = \beta$ e o lema está provado.

■

Essa caracterização da ordem $\preceq$ nos auxilia na demonstração do seguinte resultado.

Lema 3.9. *Sejam α, β partições de n. Então $\alpha \preceq \beta$ se, e somente se, $\beta' \preceq \alpha'$.*

Demonstração. Se $\alpha \preceq \beta$ então podemos obter $[\beta]$ de $[\alpha]$ ao darmos r passos como em (3.10), ou seja, existe uma cadeia de partições $\alpha^\nu \vdash n$, $0 \leqslant \nu \leqslant r$, que satisfaz

$$\alpha = \alpha^0 \prec \alpha^1 \prec \cdots \prec \alpha^r = \beta.$$

Pelo Lema 3.8 temos que $\alpha^\nu \prec \alpha^{\nu+1}$ implica

$$(\alpha^{\nu+1})' \prec (\alpha^\nu)'.$$

Então obtemos a cadeia

$$\beta' = (\alpha^r)' \prec \cdots \prec (\alpha^0)' = \alpha'$$

donde segue que $\beta' \preceq \alpha'$. A recíproca é verdadeira por simetria.

■

Lembremos que nosso objetivo é mostrar que as representações irredutíveis ordinárias $[\alpha]$ de S_n formam um conjunto completo. Mas $[\alpha]$ "corresponde" ao diagrama de Young $[\alpha]$ e portanto à matriz 0-1 dada por (3.6). Vamos ver então o que a ordem parcial $\preceq$ do conjunto $P(n)$ representa em termos das matrizes 0-1.

Teorema 3.10. *Sejam $\alpha = (\alpha_1, \ldots, \alpha_n)$ e $\beta = (\beta_1, \ldots, \beta_n)$ partições de n. Se existe uma matriz 0-1 cuja soma da linha i é igual a α_i e a soma da coluna j é igual a β'_j, para todos $1 \leqslant i \leqslant j \leqslant n$, então $\alpha \preceq \beta$.*

Demonstração. Seja A uma matriz como na hipótese do teorema e $\overline{A}$ a matriz 0-1 dada por (3.6). Então A e $\overline{A}$ possuem α como vetor soma dos elementos de cada linha. Além disso temos

$$\sum_{j=1}^{n} \beta'_j = \sum_{j=1}^{n} \alpha'_j = n.$$

Portanto podemos obter A de $\overline{A}$ ao mudarmos de posição, dentro de uma mesma linha, os 1's das linhas de $\overline{A}$. Segue que

$$\sum_{\nu=1}^{i} \beta'_\nu \leqslant \sum_{\nu=1}^{n} \alpha'_\nu,$$

para todo $i = 1, \ldots, n$, ou seja, $\beta' \preceq \alpha'$. Aplicando agora o Lema 3.9 obtemos $\alpha \preceq \beta$.

■

Pode-se mostrar que a recíproca do teorema acima é também válida. Essa caracterização da ordem $\preceq$ em termos de matrizes 0-1 é conhecida como *Teorema de Gale e Ryser* e é um dos resultados mais importante em combinatória. A demonstração da recíproca pode ser encontrada em [19].

Aplicando (3.4) e o Corolário 3.5, obtemos uma caracterização do Teorema 3.10 em termos de representações.

Teorema 3.11. *Sejam α e β partições de n e S_α e $S_{\beta'}$ os subgrupos de Young correspondentes a α e β', respectivamente. Se* char$K \neq 2$ *e $i(IS_\alpha \uparrow S_n, AS_{\beta'} \uparrow S_n) \neq 0$, então $\alpha \preceq \beta$.*

Corolário 3.12. *Sejam α e β partições de n. Se a multiplicidade $i(IS_\alpha \uparrow S_n, [\beta])$ é não nula, então $\alpha \preceq \beta$.*

Demonstração. Pelo Teorema 3.7, temos $i(AS_{\beta'} \uparrow S_n, [\beta]) = 1$. Este fato e a hipótese $i(IS_\alpha \uparrow S_n, [\beta]) \neq 0$ implicam que $i(IS_\alpha \uparrow S_n, AS_{\beta'} \uparrow S_n) \neq 0$. O resultado segue agora do último teorema.

■

Teorema 3.13. *$\{[\alpha] : \alpha$ é partição de $n\}$ é um conjunto completo de classes de equivalência das representações irredutíveis ordinárias de S_n.*

Demonstração. Como já observamos anteriormente, precisamos somente mostrar que se $[\alpha] = [\beta]$ então $\alpha = \beta$. Suponhamos então que $[\alpha] = [\beta]$. Assim

$$i(IS_\alpha \uparrow S_n, [\beta]) = i(IS_\alpha \uparrow S_n, [\alpha]) = 1 \quad \text{e} \quad i(IS_\beta \uparrow S_n, [\alpha]) = i(IS_\beta \uparrow S_n, [\beta]) = 1.$$

Aplicando o Corolário 3.12, concluímos que $\alpha \preceq \beta$ e $\beta \preceq \alpha$, donde segue que $\alpha = \beta$.

■

Como cada $[\alpha]$ pode ser realizada sobre $\mathbb{Q}$, o teorema acima nos diz que $\mathbb{Q}$ é um corpo de decomposição para S_n (Teorema 2.16). Logo, pelo Corolário 2.18, vale o seguinte resultado.

Teorema 3.14. *Todo corpo é um corpo de decomposição para S_n.*

3.3 Os caracteres irredutíveis ordinários de S_n

Na seção anterior construímos um conjunto completo de representações irredutíveis ordinárias de S_n. Agora vamos ver como se comportam os caracteres dessas representações.

Seja $p(n) := |P(n)|$ o número de partições de n e consideremos essas particões em ordem lexicográfica

$$\alpha^1 = (1, \ldots, 1) < \alpha^2 < \cdots < \alpha^{p(n)} = (n).$$

Definamos a matriz

$$M_n = (m_{kj}), \quad 1 \leqslant k, j \leqslant p(n)$$

com as seguintes multiplicidades como entrada

$$m_{kj} = i(IS_{\alpha^k} \uparrow S_n, [\alpha^j]).$$

Pelo Teorema 3.7, Lema 3.9 e Corolário 3.12, temos que $m_{kk} = 1$ e $m_{kj} \neq 0$ somente se $\alpha^k \leqslant \alpha^j$. Portanto

$$M_n = \begin{pmatrix} 1 & & * \\ & \ddots & \\ \mathbf{0} & & 1 \end{pmatrix} \tag{3.11}$$

Uma outra observação a respeito de M_n é que o produto escalar da linha i com a linha j satisfaz

$$\sum_{l=1}^{p(n)} m_{kj} m_{jl} = i(IS_{\alpha^k} \uparrow S_n, IS_{\alpha^j} \uparrow S_n) = \sum_{S_{\alpha^i} \pi S_{\alpha^j}} 1.$$

Exemplo 3.15. Consideremos as particões de $n = 3$ em ordem lexicográfica

$$\alpha^1 = (1,1,1) < \alpha^2 = (2,1) < \alpha^3 = (3).$$

Então

$$M_3 = \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix}$$

e sabemos que

$$i(IS_{\alpha^k} \uparrow S_3, IS_{(3)} \uparrow S_3) = \sum_{S_{\alpha^k} \pi S_{(3)}} 1 = 1, \qquad k = 1, 2$$

e

$$i(IS_{(1,1,1)} \uparrow S_3, IS_{(2,1)} \uparrow S_3) = \sum_{S_{(1,1,1)} \pi S_{(2,1)}} 1 = [S_3 : S_{(2,1)}],$$

pois $S_{(3)} = S_3$ e $S_{(1,1,1)} = \{1\}$. Com isso,

$$1 = \sum_{l=1}^{3} m_{kl} m_{3l} = m_{k3}, \qquad k = 1, 2$$

e

$$3 = [S_3 : S_{(2,1)}] = \sum_{l=1}^{3} m_{1l} m_{2l} = m_{12} + 1.$$

Portanto

$$M_3 = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

A expressão (3.11) tem consequências importantes. Denotemos por

$$\zeta^{\alpha}$$

o caracter da representação irredutível ordinária $[\alpha]$ e por

$$\xi^{\alpha}$$

o caracter da *representação permutacional* $IS_{\alpha} \uparrow S_n$ (veja observação 2.9). Como $\{[\alpha] : \alpha \vdash n\}$ é um conjunto completo de representações irredutíveis de S_n, por (2.14), temos que todo caracter de S_n pode ser escrito como combinação linear dos caracteres ζ^{α}, ou seja,

$$\xi^{\alpha^k} = \sum_{j=1}^{p(n)} i(IS_{\alpha^k} \uparrow S_n, [\alpha^j]) \cdot \zeta^{\alpha^j} = \sum_{j=1}^{p(n)} m_{kj} \zeta^{\alpha^j},$$

para todo $1 \leqslant k \leqslant p(n)$. Se representarmos por ζ^{α}_{β} o valor do caracter ζ^{α} na classe β e por ξ^{α}_{β} o valor do caracter permutação ξ^{α} nesta mesma classe então

$$\xi^{\alpha^k}_{\beta^l} = \sum_{j=1}^{p(n)} m_{kj} \zeta^{\alpha^j}_{\beta^l}, \qquad 1 \leqslant l \leqslant p(n), \tag{3.12}$$

onde estamos ordenando as classes de conjugação β^l através de suas partições associadas. Além disso, se colocarmos ζ^{α}_{β} e ξ^{α}_{β} em matrizes

$$Z_n := (\zeta^{\alpha^k}_{\beta^k}) \quad \text{e} \quad P_n := (\xi^{\alpha^k}_{\beta^k}), \qquad 1 \leqslant k, l \leqslant p(n),$$

então Z_n é a tabela de caracteres de S_n e P_n satisfaz

$$P_n = M_n Z_n,$$

como podemos ver por (3.12). Uma vez que $\det M_n \neq 0$, temos

$$Z_n = M_n^{-1} P_n. \tag{3.13}$$

Como M_n é uma matriz com entradas em $\mathbb{N}_0$ e determinante igual a 1, segue que M_n^{-1} é uma matriz sobre $\mathbb{Z}$. Portanto, cada caracter irredutível ordinário ζ^α de S_n é uma $\mathbb{Z}$-combinação linear dos caracteres permutação ξ^α e, como existem exatamente $p(n)$ destes caracteres, esta $\mathbb{Z}$-combinação linear está unicamente determinada.

Para determinarmos esta $\mathbb{Z}$-combinação linear, vamos primeiro introduzir uma multiplicação nas representações $[\alpha]$ de S_n. Se $m, k \in \mathbb{N}$ e S_k é o grupo simétrico que permuta os elementos do conjunto $\{m+1, \ldots, m+k\}$, então $S_m \times S_k$ pode ser mergulhado em S_{m+k} de forma natural

$$S_m \times S_k \hookrightarrow S_{m+k}.$$

Portanto, se $\gamma \vdash n$ e $\delta \vdash k$ então a representação $[\gamma]\#[\delta]$ de $S_m \times S_k$ define uma representação de um subgrupo de S_{m+k} que é isomorfo a $S_m \times S_k$. Podemos então induzir $[\gamma]\#[\delta]$ em S_{m+k}, denotar a representação resultante por $[\gamma][\delta]$ e chamar de *produto externo* de $[\gamma]$ e $[\delta]$,

$$[\gamma][\delta] := [\gamma]\#[\delta] \uparrow S_{m+k}.$$

Essa multiplicação é associativa, pelo Teorema 2.19, e comutativa. Portanto, para uma partição $\alpha = (\alpha_1, \ldots, \alpha_h)$ de n temos

$$IS_\alpha \uparrow S_n = ([\alpha_1]\# \cdots \#[\alpha_h]) \uparrow S_n = [\alpha_1] \ldots [\alpha_h]. \tag{3.14}$$

Com a ajuda dessa multiplicação vamos definir um determinante que corresponde à partição $\alpha = (\alpha_1, \ldots, \alpha_h)$ de n, onde $\alpha_{h+1} = 0$, pondo

$$|[\alpha_i + j - i]| := \begin{vmatrix} [\alpha_1] & [\alpha_1+1] & [\alpha_1+2] & \cdots & [\alpha_1+h-1] \\ [\alpha_2-1] & [\alpha_2] & [\alpha_2+1] & \cdots & [\alpha_2+h-2] \\ & & \vdots & & \\ [\alpha_h-h+1] & [\alpha_h-h+2] & [\alpha_h-h+3] & \cdots & [\alpha_h] \end{vmatrix} \tag{3.15}$$

e

$$[r] := \begin{cases} 1, & \text{se } r = 0 \\ 0, & \text{se } r < 0 \end{cases}, \quad 1 \cdot [r] := [r] \quad \text{e} \quad 0 \cdot [r] := 0, \tag{3.16}$$

o que é consistente com (3.14). Notemos que (3.15), quando aplicamos a definição de determinante, não depende da escolha de h, apenas da condição $\alpha_{h+1} = 0$.

Exemplo 3.16. Seja $\alpha = (3,1,1,0,0) \vdash 5$. Então o determinante dado por (3.15) é igual a

$$\begin{vmatrix} [3] & [4] & [5] \\ 1 & [1] & [2] \\ 0 & 1 & [1] \end{vmatrix} = [3][1][1] - [3][2] - [4][1] + [5]$$

$$= \begin{vmatrix} [3] & [4] & [5] & [6] \\ 1 & [1] & [2] & [3] \\ 0 & 1 & [1] & [2] \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

o que ilustra a nossa observação de que (3.15) independe da escolha de h.

Exemplo 3.17. Seja $\alpha = (2,1) \vdash 3$. Então

$$\begin{vmatrix} [2] & [3] \\ 1 & [1] \end{vmatrix} = [2][1] - [3],$$

que corresponde à representação $IS_{(2,1)} \uparrow S_3 - IS_{(3)} \uparrow S_3$. O caracter dessa representação é igual a

$$\xi^{(2,1)} - \xi^{(3)}.$$

Olhando agora para a matriz M_3 do Exemplo 3.15 obtemos

$$M_3^{-1} = \begin{pmatrix} 1 & -2 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Segue então de (3.13) que

$$\zeta^{(2,1)} = \xi^{(2,1)} - \xi^{(3)}.$$

No exemplo acima, com M_3 em mãos, vimos que o determinante dado por (3.15) correspondente à $\alpha = (2,1) \vdash 3$ dá a expressão desejada para $\zeta^{(2,1)}$ como $\mathbb{Z}$-combinação linear dos caracteres permutação. Na verdade, este fato vale para qualquer partição α.

Para $\pi \in S_n$ e $\alpha = (\alpha_1, \ldots, \alpha_n)$ partição de n, definamos

$$\alpha - \mathrm{id} + \pi = (\alpha_1 - 1 + \pi(1), \ldots, \alpha_n - n + \pi(n))$$

e

$$\xi^{\lambda} = \begin{cases} \text{o caracter de } IS_\lambda \uparrow S_n, & \text{se } \lambda \text{ é composição de } n, \\ \text{a função que leva } S_n \text{ no } 0, & \text{caso contrário.} \end{cases} \tag{3.17}$$

No caso em que λ não é uma composição de n, dizemos que ξ^λ é o "caracter zero". Por definição, temos as seguintes propriedades:

(1) (o caracter zero de S_m) # (um caracter de S_k) = (o caracter zero de S_{m+k});

(2) induzir ou restringir um caracter zero resulta no caracter zero.

Aplicando a definição de determinante temos

$$||[\alpha_i - i + j]|| = \sum_{\pi \in S_n} \text{sgn}\pi \prod_{i=1}^{n} [\alpha_i - i + \pi(i)].$$

Logo, se o determinante $||[\alpha_i - i + j]||$ dá a expressão de ζ^α como $\mathbb{Z}$-combinação linear dos caracteres de permutação, então (com a notação acima)

$$\zeta^\alpha = \sum_{\pi \in S_n} \text{sgn}\pi \ \xi^{\alpha - \text{id} + \pi}.$$

Teorema 3.18 ([15], pg. 53). *Para cada α partição de n temos que*

$$\zeta^\alpha = \sum_{\pi \in S_n} \text{sgn}\pi \ \xi^{\alpha - id + \pi},$$

isto é, o caracter da representação irredutível ordinária $[\alpha]$ de S_n pode ser escrito como combinação linear dos caracteres permutação ξ^λ, λ partição de n, com coeficientes 0,1,-1. Podemos, portanto, expressar $[\alpha]$ na forma determinante

$$[\alpha] = ||[\alpha_i - i + j]||,$$

sujeita às condições $[r] := 1$ se $r = 0$ e $[r] := 0$ se $r < 0$.

Vamos agora obter, com a ajuda do Teorema 3.18, uma fórmula para os graus das representações irredutíveis ordinárias $[\alpha]$ de S_n. Para isso considere o diagrama de Young de α.

$$[\alpha] = \begin{array}{l} \square\ \square\ \cdots\cdots\ \square \\ \square\ \square\ \cdots\ \square \\ \vdots \\ \square\ \cdots\ \square \end{array}$$

Denotamos por *símbolo* (i, j) de $[\alpha]$ o símbolo $\square$ que está na linha i e na coluna j do diagrama. Denotemos por

$$H_{ij}^\alpha$$

o gancho (i, j) de $[\alpha]$, que consiste do símbolo (i, j) junto com todos os símbolos $\square$ à direita na mesma linha e os símbolos $\square$ abaixo na mesma coluna.

$$H_{ij}^\alpha = \begin{array}{l} \square\ \square\ \cdots\ \square\ \square \ \rightarrow i \\ \square \\ \vdots \\ \square \\ \downarrow \\ j \end{array}$$

Denotamos o número de símbolos de H_{ij}^{α} por h_{ij}^{α}, isto é,

$$h_{ij}^{\alpha} := \alpha_i - j + \alpha'_j - i + 1.$$

Exemplo 3.19. Seja $\alpha = (3,2,1,1) \vdash 7$. O diagrama de Young correspondente a $(3,2,1,1)$ é igual a

$$[(3,2,1,1)] \;=\; \begin{array}{l}\square\,\square\,\square\\ \square\,\square\\ \square\\ \square\end{array}$$

Então

$$H_{11}^{\alpha} \;=\; \begin{array}{l}\blacksquare\,\blacksquare\,\blacksquare\\ \blacksquare\,\square\\ \blacksquare\\ \blacksquare\end{array} \qquad h_{11}^{\alpha} = 6$$

$$H_{12}^{\alpha} \;=\; \begin{array}{l}\square\,\blacksquare\,\blacksquare\\ \square\,\blacksquare\\ \square\\ \square\end{array} \qquad h_{12}^{\alpha} = 3$$

$$H_{13}^{\alpha} \;=\; \begin{array}{l}\square\,\square\,\blacksquare\\ \square\,\square\\ \square\\ \square\end{array} \qquad h_{13}^{\alpha} = 1$$

$$H_{21}^{\alpha} \;=\; \begin{array}{l}\square\,\square\,\square\\ \blacksquare\,\blacksquare\\ \blacksquare\\ \blacksquare\end{array} \qquad h_{21}^{\alpha} = 4$$

$$H_{22}^{\alpha} \;=\; \begin{array}{l}\square\,\square\,\square\\ \square\,\blacksquare\\ \square\\ \square\end{array} \qquad h_{22}^{\alpha} = 1$$

$$H_{31}^{\alpha} \;=\; \begin{array}{l}\square\,\square\,\square\\ \square\,\square\\ \blacksquare\\ \blacksquare\end{array} \qquad h_{31}^{\alpha} = 2$$

$$H_{41}^{\alpha} \;=\; \begin{array}{l}\square\,\square\,\square\\ \square\,\square\\ \square\\ \blacksquare\end{array} \qquad h_{41}^{\alpha} = 1.$$

Teorema 3.20. *Seja α partição de n e ζ^{α} o caracter irredutível associado a α. Então*

$$\zeta^{\alpha}(1) = \frac{n!}{\prod_{i,j} h_{ij}^{\alpha}}.$$

Demonstração. Assumindo que $\alpha = (\alpha_1, \ldots, \alpha_h) \vdash n$ possui exatamente h partes não nulas, segue de (2.6) que

$$\xi^{\alpha}(1) = [S_n : S_{\alpha}] = \frac{n!}{\alpha_1! \cdots \alpha_h!}.$$

Então pelo Teorema 3.18, temos

$$\begin{aligned}\zeta^\alpha(1) &= \sum_{\pi\in S_n} \operatorname{sgn}\pi\ \xi^{\alpha-\mathrm{id}+\pi}(1) = \sum_{\pi\in S_n} \operatorname{sgn}\pi\ \frac{n!}{\prod_i (\alpha_i - i + \pi(i))!} \\ &= n!\left|\frac{1}{(\alpha_i - i + j)!}\right|,\end{aligned}$$

onde $\frac{1}{r!} = 0$ se $r < 0$ (veja (3.16)).

Mas $H^\alpha_{i1} = \alpha_i + \alpha'_1 - i = \alpha_i - i + h$, já que α possui h partes não nulas, e quando $j < h$

$$\frac{h^\alpha_{i1}!}{(\alpha_i + j - i)!} = \frac{(\alpha_i - i + h \pm j)!}{(\alpha_i + j - i)!} = \prod_{r=1}^{h-j} \alpha_i - i + j + r = \prod_{r=1}^{h-j} h^\alpha_{i1} - h + j + r.$$

Quando $j = h$, temos $\frac{h^\alpha_{i1}!}{(\alpha_i+j-i)!} = 1$. Então

$$\left|\frac{1}{(\alpha_i + j - i)!}\right| = \frac{1}{\prod_i h^\alpha_{i1}!}\left|\frac{h^\alpha_{i1}!}{(\alpha_i + j - i)!}\right| = \frac{1}{\prod_i h^\alpha_{i1}!}\left|\prod_{r=1}^{h-j} h^\alpha_{i1} - h + j + r\right|$$

(onde estamos convencionando o produtório como igual a 1 na coluna $j = h$).

Transformações elementares aplicadas no determinante do lado direito da igualdade acima implicam no determinante de Vandermonde

$$\left|(h^\alpha_{i1})^{h-j}\right| = \prod_{1\leqslant i<j\leqslant h} \left(h^\alpha_{i1} - h^\alpha_{j1}\right).$$

Portanto

$$\zeta^\alpha(1) = n!\ \frac{\prod_{i<j}\left(h^\alpha_{i1} - h^\alpha_{j1}\right)}{\prod_i h^\alpha_{i1}!}.$$

Para completar a prova, mostraremos que para $1 \leqslant i \leqslant h$ temos

$$\prod_{j=i+1}^{h} \left(h^\alpha_{i1} - h^\alpha_{j1}\right) \prod_{\nu=1}^{\alpha_i} h^\alpha_{i\nu} = h^\alpha_{i1}! \tag{3.18}$$

Feito isso,

$$\zeta^\alpha(1) = n!\ \frac{\prod_{i<j}\left(h^\alpha_{i1} - h^\alpha_{j1}\right)}{\prod_{i=1}^{h}\prod_{j=i+1}^{h}\left(h^\alpha_{i1} - h^\alpha_{j1}\right)\prod_{\nu=1}^{\alpha_i} h^\alpha_{i\nu}} = n!\ \frac{\prod_{i<j}\left(h^\alpha_{i1} - h^\alpha_{j1}\right)}{\prod_{i<j}\left(h^\alpha_{i1} - h^\alpha_{j1}\right)\prod_{\nu=1}^{\alpha_i} h^\alpha_{i\nu}} = \frac{n!}{\prod_{i,j} h^\alpha_{ij}},$$

como queríamos.

Agora, em cada um dos lados da equação (3.18) existem exatamente h^α_{i1} fatores. Os fatores $h^\alpha_{i1} - h^\alpha_{j1}$ estão crescendo (estritamente) quando j cresce, enquanto os $h^\alpha_{j\nu}$ são estritamente crescentes quando ν cresce. Além disso, os fatores do lado esquerdo são todos menores ou

iguais a h^α_{i1}. Portanto é suficiente provarmos que os fatores do lado esquerdo são dois a dois distintos, ou ainda, que

$$h^\alpha_{i1} - h^\alpha_{j1} < h^\alpha_{i\nu} < h^\alpha_{i1} - h^\alpha_{j+1,1} \tag{3.19}$$

para um $1 \leqslant j \leqslant h$ adequado, que depende de ν.

Tomemos então $j = \alpha'_\nu$ tal que $\alpha_j \geqslant \nu$ e $\alpha_{j+1} < \nu$. Assim,

$$h^\alpha_{i1} - h^\alpha_{j1} = \alpha_i - i - \alpha_j + j \leqslant \alpha_i - i - \nu + j < \alpha_i - i - \nu + j + 1 = h^\alpha_{i\nu}$$

e

$$h^\alpha_{i1} - h^\alpha_{j+1,1} = \alpha_i - i - \alpha_{j+1} + j + 1 > \alpha_i - i - \nu + j + 1 = h^\alpha_{i\nu},$$

o que prova (3.19) e completa a demonstração.

■

Exemplo 3.21. Vamos determinar os graus de todas as representações irredutíveis ordinárias de S_4. Para isso, considere a seguinte tabela:

$[(1,1,1,1)]$	$=$	□ □ □ □	$h_{11} = 4,\ h_{21} = 3,\ h_{31} = 2,\ h_{41} = 1$
$[(2,1,1)]$	$=$	□ □ □ □	$h_{11} = 4,\ h_{12} = 1,\ h_{21} = 2,\ h_{22} = 1$
$[(2,2)]$	$=$	□ □ □ □	$h_{11} = 3,\ h_{12} = 2,\ h_{21} = 2,\ h_{22} = 1$
$[(3,1)]$	$=$	□ □ □ □	$h_{11} = 4,\ h_{12} = 2,\ h_{13} = 1,\ h_{21} = 1$
$[(4)]$	$=$	□ □ □ □	$h_{11} = 4,\ h_{12} = 3,\ h_{13} = 2,\ h_{14} = 1$

Então, pelo Teorema 3.20, os grau das representações irredutíveis ordinárias de S_4 são

α	$(1,1,1,1)$	$(2,1,1)$	$(2,2)$	$(3,1)$	(4)
$\zeta^\alpha(1)$	1	3	2	3	1

3.4 Fórmulas de recursão

Dizemos que uma partição $\lambda = (\lambda_1, \ldots, \lambda_n)$ de n tem *comprimento* h se λ possui exatamente h partes não nulas e denotamos por $P_h(n)$ o conjunto das partições de n de comprimento menor do que ou igual a h.

Sejam $\lambda \in P_h(n+1)$ e $\mu \in P_h(n)$. Escrevemos $\mu \to \lambda$ se existe $1 \leqslant j \leqslant h$ tal que $\lambda_i = \mu_i + \delta_{ij}$, para todo $1 \leqslant i \leqslant j$, onde δ_{ij} é o delta de Kronecker.

Lema 3.22. *Seja $\lambda \in P_h(n)$. Então*

$$\xi^\lambda \downarrow S_{n-1} = \sum_{\substack{\mu \in P_h(n-1) \\ \mu \to \lambda}} \xi^\mu,$$

onde S_{n-1} é o subgrupo de S_n que fixa o ponto n.

Demonstração. O Teorema do Subgrupo (Teorema 2.21) diz que

$$\begin{aligned}(IS_\lambda \uparrow S_n) \downarrow S_{n-1} &= \sum_{S_{n-1}\pi S_\lambda} \left[IS_\lambda^{(\pi)} \downarrow \left(S_{n-1} \cap \pi S_\lambda \pi^{-1} \right) \right] \uparrow S_n \\ &= \sum_{S_{n-1}\pi S_\lambda} I\left(S_{n-1} \cap \pi S_\lambda \pi^{-1} \right) \uparrow S_n.\end{aligned}$$

Pelo Teorema 3.5, a (S_{n-1}, S_λ)-classe dupla $S_{n-1}\pi S_\lambda$ é caracterizada pela matriz $2 \times n$

$$\begin{pmatrix} \cdots & \left| N \setminus \{n\} \cap \pi\left(N_j^\lambda\right)\right| & \cdots \\ \cdots & \left| \{n\} \cap \pi\left(N_j^\lambda\right)\right| & \cdots \end{pmatrix}, \quad 1 \leqslant j \leqslant n,$$

pois podemos considerar S_{n-1} como o subgrupo de Young de S_n associado à partição $(n-1, 1)$ de n.

Esta classe dupla está, portanto, unicamente determinada por

$$\delta_j = \left(\cdots, \left| \{n\} \cap \pi\left(N_j^\lambda\right)\right|, \cdots \right),$$

isto é, um vetor com coordenadas todas nulas exceto a j-ésima, onde $1 \leqslant j \leqslant n$ é tal que $n \in \pi\left(N_j^\lambda\right)$, que é igual a 1.

Como $\pi S_\lambda^j \pi^{-1}$ é o grupo simétrico que permuta exatamente os elementos de $\pi(N_j^\lambda)$, vemos que $S_{n-1} \cap \pi S_\lambda \pi^{-1} \simeq S_{\lambda - \delta_j}$, onde $\lambda - \delta_j = (\lambda_1, \ldots, \lambda_{j-1}, \lambda_j - 1, \lambda_{j+1}, \ldots, \lambda_h)$. Portanto,

$$(IS_\lambda \uparrow S_n) \downarrow S_{n-1} = \sum_{j=1}^{h} IS_{\lambda - \delta_j} \uparrow S_n = \sum_{\substack{\mu \in P_h(n-1) \\ \mu \to \lambda}} IS_\mu \uparrow S_n$$

o que implica

$$\xi^\lambda \downarrow S_{n-1} = \sum_{\substack{\mu \in P_h(n-1) \\ \mu \to \lambda}} \xi^\mu.$$

■

Aplicando este lema na forma determinante de ζ^α dada pelo Teorema 3.18, obtemos

$$\begin{aligned}\zeta^\alpha \downarrow S_{n-1} &= \sum_{\pi\in S_n} \operatorname{sgn}\,\pi \left(\xi^{\alpha-\mathrm{id}+\pi}\downarrow S_{n-1}\right) = \sum_{\pi\in S_n} \operatorname{sgn}\,\pi \sum_{\substack{\mu\in P_h(n-1)\\ \mu\to\alpha-\mathrm{id}+\pi}} \xi^\mu \\ &= \sum_{\substack{\mu\in P_h(n-1)\\ \mu\to\alpha-\mathrm{id}+\pi}} \sum_{\pi\in S_n} \operatorname{sgn}\,\pi\cdot\xi^\mu = \sum_{\substack{\mu\in P_h(n-1)\\ \mu\to\alpha}} \zeta^\mu,\end{aligned}$$

o que prova a seguinte fórmula de recursão para caracteres irredutíveis.

Teorema 3.23. *Seja $\lambda \in P_h(n)$. Então*

$$\zeta^\lambda \downarrow S_{n-1} = \sum_{\{\mu\in P_h(n-1):\mu\to\lambda\}} \zeta^\mu.$$

Corolário 3.24. *Seja $\lambda \in P_h(n+1)$. Então*

$$\frac{n+1}{\prod_{i,j} h_{ij}^\lambda} = \sum_{\mu\to\lambda} \frac{1}{\prod_{i,j} h_{ij}^\mu}.$$

Demonstração. Podemos assumir $n > 0$, visto que para $n = 0$ o resultado é obviamente verdadeiro. Pelos Teoremas 3.20 e 3.23, temos

$$\frac{(n+1)!}{\prod_{i,j} h_{ij}^\lambda} = \zeta^\lambda(1) = \left(\zeta^\lambda \downarrow S_n\right)(1) = \sum_{\mu\to\lambda} \frac{n!}{\prod_{i,j} h_{ij}^\mu},$$

donde segue o resultado.

■

Capítulo 4

Espaços de Grassmann

Neste capítulo apresentamos os resultados de álgebra multilinear que Dias da Silva e Hamidoune utilizaram para provar a conjectura de Erdős e Heilbronn. A prova da conjectura segue como um caso particular do Teorema 1.1, que apresentamos na seção 4.3.

4.1 Definições e exemplos

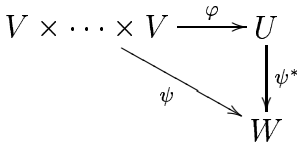
Sejam V e U espaços vetoriais de dimensão finita sobre um corpo K. Dizemos que uma aplicação h-linear $\varphi : \underbrace{V \times \cdots \times V}_{h} \to U$ é *anti-simétrica* se, para cada $\pi \in S_h$, temos

$$\varphi(v_{\pi(1)}, \ldots, v_{\pi(h)}) = \operatorname{sgn}\pi \ \varphi(v_1, \ldots, v_h), \qquad v_1, \ldots, v_h \in V.$$

Consideremos, então, uma aplicação $\varphi : V \times \cdots \times V \to U$ h-linear e anti-simétrica. O par (φ, U) é um *espaço de Grassmann* de grau h associado a V se

(i) U é gerado pelos elementos $\varphi(v_1, \ldots, v_h)$, onde $v_1, \ldots, v_h \in V$;

(ii) Se W é um espaço vetorial sobre K e $\psi : V \times \cdots \times V \to W$ é uma aplicação h-linear anti-simétrica, então existe uma única aplicação linear $\psi^* : U \to W$ tal que $\psi^*\varphi = \psi$, isto é, tal que o diagrama abaixo comuta



Nessas condições, denotamos φ por $\wedge$, U por $\bigwedge^h V$ e $\varphi(v_1, \ldots, v_h)$ por $v_1 \wedge \cdots \wedge v_h$.

Utilizando a multilinearidade e a anti-simetria de $\wedge$ obtemos as seguintes propriedades:

(1) $v_1 \wedge \cdots \wedge (v_i + v_i') \wedge \cdots \wedge v_h = (v_1 \wedge \cdots \wedge v_i \wedge \cdots \wedge v_h) + (v_1 \wedge \cdots \wedge v_i' \wedge \cdots \wedge v_h)$,

(2) $a(v_1 \wedge \cdots \wedge v_h) = (av_1) \wedge \cdots \wedge v_h = \cdots = v_1 \wedge \cdots \wedge (av_h)$,

(3) se $\pi \in S_h$, então $v_{\pi(1)} \wedge \cdots \wedge v_{\pi(h)} = \mathrm{sgn}\pi \ (v_1 \wedge \cdots \wedge v_h)$,

(4) se $\mathrm{char}K \neq 2$ e $v_i = v_j$, para algum $i \neq j$, então $v_1 \wedge \cdots \wedge v_h = 0$.

para todos $v_i \in V$, $i = 1, \ldots, h$ e $a \in K$.

As três primeiras propriedades são imediatas e, aplicando **(3)** para $\pi = (ij) \in S_h$, vemos que

$$v_1 \wedge \cdots \wedge v_i \wedge \cdots \wedge v_j \wedge \cdots \wedge v_h = -(v_1 \wedge \cdots \wedge v_j \wedge \cdots \wedge v_i \wedge \cdots \wedge v_h),$$

donde segue **(4)**.

Exemplo 4.1. Seja $V = \mathbb{R}^2$ e U o conjunto das matrizes reais anti-simétricas de ordem 2. Consideremos $\varphi : \mathbb{R}^2 \times \mathbb{R}^2 \to U$ definida por

$$\varphi\left((a_1, a_2), (b_1, b_2)\right) = (a_i b_j - a_j b_i)_{1 \leqslant i,j \leqslant 2} = \begin{pmatrix} 0 & a_1 b_2 - a_2 b_1 \\ a_2 b_1 - a_1 b_2 & 0 \end{pmatrix},$$

$(a_1, a_2),\ (b_1, b_2) \in \mathbb{R}^2$. Claramente φ é bilinear e anti-simétrica. Para mostrar que (φ, U) é um espaço de Grassmann, fixemos a base $\{e_1 = (1, 0),\ e_2 = (0, 1)\}$ de $\mathbb{R}^2$. Então

$$\varphi(e_1, e_2) = -\varphi(e_2, e_1) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

e, como U é gerado exatamente por essa matriz, temos que a imagem de φ gera U.

Consideremos agora $\psi : \mathbb{R}^2 \times \mathbb{R}^2 \to W$ uma aplicação bilinear anti-simétrica. Definamos $\psi^* : U \to W$ por

$$\psi^*(\varphi(e_i, e_j)) = \psi(e_i, e_j), \qquad 1 \leqslant i, j \leqslant 2.$$

Então ψ^* é linear e, portanto, $\psi^*\varphi = \psi$. Suponhamos que exista outra aplicação linear ψ^{**} tal que $\psi^{**}\varphi = \psi$. Então

$$\psi^*(\varphi(e_1, e_2)) = \psi(e_1, e_2) = \psi^{**}(\varphi(e_1, e_2))$$

e como $\varphi(e_1, e_2)$ gera U, obtemos $\psi^* = \psi^{**}$.

Vamos agora ver como a base do espaço de Grassmann $\bigwedge^h V$ se comporta em relação a uma base fixada $\{e_0, \ldots, e_{k-1}\}$ de V. Como $\bigwedge^h V$ é gerado pelas imagens da aplicação $\wedge$ as propriedades **(1)** e **(2)** implicam que os elementos $e_{i_1} \wedge \cdots \wedge e_{i_h}$, com $i_j \in \{0, \ldots, k-1\}$ para $1 \leqslant j \leqslant h$, geram $\bigwedge^h V$. Além disso, as propriedades **(3)** e **(4)** garantem que precisamos apenas considerar os elementos $e_{i_1} \wedge \cdots \wedge e_{i_h}$ com índices $k - 1 \geqslant i_1 > i_2 > \cdots > i_h \geqslant 0$.

Vamos mostrar que o conjunto

$$\mathcal{I} = \{e_{i_1} \wedge \cdots \wedge e_{i_h} \ : \ k-1 \geqslant i_1 > i_2 > \cdots > i_h \geqslant 0\} \tag{4.1}$$

é linearmente independente. Suponhamos que existe $e_{j_1} \wedge \cdots \wedge e_{j_h} \in \mathcal{I}$ tal que

$$e_{j_1} \wedge \cdots \wedge e_{j_h} = \sum a_{i_1,\cdots,i_h}\ e_{i_1} \wedge \cdots \wedge e_{i_h},$$

onde a soma é tomada sobre todas as h-uplas $(i_1, \ldots, i_h) \neq (j_1, \ldots, j_h)$ com $k-1 \geqslant i_1 > \cdots > i_h \geqslant 0$ e $a_{i_1,\ldots,i_h} \in K$. Consideremos ψ uma aplicação h-linear e anti-simétrica definida por $\psi(e_{j_1}, \ldots, e_{j_h}) = 1$ e $\psi(e_{i_1}, \ldots, e_{i_h}) = 0$, se $(i_1, \ldots, i_h) \neq (j_{\pi(1)}, \ldots, j_{\pi(h)})$, para todo $\pi \in S_h$. Então, por definição, existe uma única aplicação linear θ satisfazendo $\theta\wedge = \psi$. Mas

$$\begin{aligned} 1 &= \psi(e_{j_1}, \ldots, e_{j_h}) \\ &= \theta(e_{j_1} \wedge \cdots \wedge e_{j_h}) \\ &= \sum a_{i_1,\ldots,i_h}\ \theta(e_{i_1} \wedge \cdots \wedge e_{i_h}) \\ &= \sum a_{i_1,\ldots,i_h}\ \psi(e_{i_1}, \ldots, e_{i_h}) \\ &= 0, \end{aligned}$$

um absurdo.

Com isso, temos que $\mathcal{I}$ é um conjunto linearmente independente e que gera $\bigwedge^h V$, sendo portanto uma base de $\bigwedge^h V$. Dizemos que $\mathcal{I}$ é a *base de* $\bigwedge^h V$ *induzida pela base* $\{e_0, \ldots, e_{k-1}\}$ *de* V.

4.2 Alguns resultados de álgebra linear

Seja V um espaço vetorial de dimensão finita sobre um corpo K e $T : V \to V$ um operador linear. Denotamos por $I : V \to V$ o operador identidade e definimos $T^i : V \to V$, $i = 0, 1, \ldots$, por

$$T^0(v) = \mathrm{Id}(v) = v \quad \text{e} \quad T^i(v) = T(T^{i-1}(v)), \quad i \geqslant 1,$$

para todo $v \in V$. Indicamos o *polinômio minimal* de T sobre V por $p_{T,V}(x)$.

Dizemos que um subespaço W de V é *T-invariante* se $T(W) \subset W$. Neste caso, T restrito a W é um operador linear em W com polinômio minimal $p_{T,W}(x)$. Como $p_{T,V}(T)(w) = 0$, para todo $w \in W$, segue que $p_{T,W}(x)$ divide $p_{T,V}(x)$. Assim o *grau* de $p_{T,W}(x)$, que denotamos por $\partial p_{T,W}$, é menor ou igual a $\partial p_{T,V}$.

O *subespaço cíclico* com respeito a T gerado por $v \in V$ é o menor subespaço de V que contém v e é T-invariante, ou seja, o subespaço gerado pelos elementos $v, T(v), T^2(v), \ldots$ Denotamos por $C_T(v)$ tal subespaço. Naturalmente $C_T(v)$ tem dimensão finita. Além disso, valem os seguintes resultados.

Proposição 4.2. *Seja $C = C_T(v)$. Então a dimensão $(C : K)$ de C sobre K é igual a $\partial p_{T,C}$.*

Demonstração. Seja $l = (C : K)$. Então C é gerado pelos elementos $v, T(v), \ldots, T^{l-1}(v)$ e existem constantes $a_0, a_1, \ldots, a_{l-1} \in K$ tais que

$$T^l(v) = -a_{l-1}T^{l-1}(v) - \cdots - a_1T(v) - a_0v.$$

Seja $p(x) = x^l + a_{l-1}x^{l-1} + \cdots + a_1x + a_0$. Então $p(T) = 0$ em C pois a equação acima implica que $p(T)(v) = 0$ e

$$p(T)(T^i(v)) = T^i(p(T)(v)) = T^i(0) = 0, \quad i \geqslant 1.$$

Portanto, $p_{T,C}(x)$ divide $p(x)$, donde segue que $\partial p_{T,C} \leqslant l$.

Por outro lado, seja $\partial p_{T,C} = m$. Temos que $p_{T,C}(T)(v) = 0$, donde segue que os vetores $v, T(v), \ldots, T^m(v)$ são linearmente dependentes. Assim $l \leqslant m$, ou seja, $l = \partial p_{T,C}$.

■

Proposição 4.3. *Seja T um operador linear diagonalizável sobre V e $\sigma(T)$ o conjunto dos autovalores de T. Então $(C_T(v) : K) \leqslant |\sigma(T)| = \partial p_{T,V}$, para todo $v \in V$.*

Demonstração. Seja $c \in \sigma(T)$, f um autovetor associado a c e consideremos W o subespaço gerado por f. Então W é T-invariante e $p_{T,W}(x) = x - c$. Portanto $(x - c)$ divide $p_{T,V}(x)$, para todo $c \in \sigma(T)$, donde segue que $\prod_{c\in\sigma(T)}(x - c)$ divide $p_{T,V}(x)$.

Por outro lado, como T é diagonalizável, V possui uma base $\{f_0, f_1, \ldots, f_{k-1}\}$ de autovetores e

$$\prod_{c\in\sigma(T)} (T - cI)(f_i) = 0, \quad i = 0, \ldots, k - 1.$$

Então $\prod_{c\in\sigma(T)}(T - cI)(v) = 0$, para todo $v \in V$, donde segue que $p_{T,V}(x)$ divide $\prod_{c\in\sigma(T)}(x - c)$.

Portanto, $p_{T,V}(x) = \prod_{c\in\sigma(T)}(x - c)$ e $\partial p_{T,V} = |\sigma(T)|$. Lembrando que $\partial p_{T,C} \leqslant \partial p_{T,V}$, onde $C = C_T(v)$, podemos aplicar a proposição anterior e concluir que $(C_T(v) : K) \leqslant |\sigma(T)|$.

■

Proposição 4.4. *Seja $T : V \to V$ um operador linear. Se $f_0, f_1, \ldots, f_{k-1}$ são autovetores de T com autovalores distintos e $v = f_0 + f_1 + \cdots + f_{k-1}$, então $(C_T(v) : K) = k$. Se $(V : K) = k$ então $C_T(v) = V$.*

Demonstração. Mostraremos inicialmente que $f_0, f_1, \ldots, f_{k-1}$ são linearmente independentes. Suponha que não. Então existe um subconjunto mínimo de vetores que é linearmente dependente, digamos $\{f_0, f_1, \ldots, f_{l-1}\}$. Temos $l \geqslant 2$, pois $f_i \neq 0$, $i = 0, \ldots, k - 1$, e existem $a_0, a_1, \ldots, a_{l-1} \in K$ tais que $\sum_{i=0}^{l-1} a_i f_i = 0$.

Seja c_i o autovalor associado a f_i. Então

$$0 = T\left(\sum_{i=0}^{l-1} a_i(f_i)\right) = \sum_{i=0}^{l-1} a_i T(f_i) = \sum_{i=0}^{l-1} a_i c_i f_i,$$

o que implica

$$0 = \sum_{i=0}^{l-1} a_i c_i f_i - c_{l-1} \sum_{i=0}^{l-1} a_i f_i = \sum_{i=0}^{l-1} a_i (c_i - c_{l-1}) f_i = \sum_{i=0}^{l-2} a_i (c_i - c_{l-1}) f_i,$$

contradizendo a minimalidade de l.

Seja agora W o subespaço T-invariante gerado por $f_0, f_1, \ldots, f_{k-1}$. Como $v = f_0 + f_1 + \cdots + f_{k-1} \in W$, temos $C_T(v) \subset W$. Assim

$$(C_T(v) : K) \leqslant (W : K) = k.$$

Por outro lado,

$$\begin{aligned} T^i(v) &= T^i(f_0 + f_1 + \cdots + f_{k-1}) \\ &= T^i(f_0) + T^i(f_1) + \cdots + T^i(f_{k-1}) \\ &= c_0^i f_0 + c_1^i f_1 + \cdots + c_{k-1}^i f_{k-1} \end{aligned}$$

e a matriz dos vetores $\{v, T(v), \ldots, T^{k-1}(v)\}$ na base $\{f_0, \ldots, f_{k-1}\}$ é a matriz de Vandermonde

$$\begin{pmatrix} 1 & c_0 & c_0^2 & \cdots & c_0^{k-1} \\ 1 & c_1 & c_1^2 & & c_1^{k-1} \\ \vdots & & \vdots & & \vdots \\ 1 & c_{k-1} & c_{k-1}^2 & \cdots & c_{k-1}^{k-1} \end{pmatrix}.$$

Como $c_0, \ldots, c_{k-1}$ são autovalores distintos, o determinante $\prod_{0 \leqslant i < j \leqslant k-1} (c_j - c_i)$ da matriz acima é diferente de zero, o que implica que o conjunto $\{v, T(v), \ldots, T^{k-1}(v)\}$ é linearmente independente. Assim,

$$(C_T(v) : K) \geqslant k,$$

o que conclui a demonstração da proposição.

■

Para a próxima seção é importante também destacarmos o seguinte resultado.

Lema 4.5. *Seja $\{e_0, e_1, \ldots, e_{k-1}\}$ uma base de V. Se $v_i = \sum_{j=0}^{k-1} a_{ij} e_j$, $i = 0, 1, \ldots, l-1$, com $l \leqslant k$, são vetores de V tais que , para $i \in \{0, 1, \ldots, l-1\}$ fixado,*

(1) *$a_{ii} \neq 0$, e*

(2) *$a_{ij} = 0$, se $l > j > i$,*

então $v_0, v_1, \ldots, v_{l-1}$ são linearmente independentes.

Demonstração. Claramente o resultado é verdadeiro quando $l = 1$. Então, seja $1 < l \leqslant k-1$ e suponhamos que para $l-1$ vale o resultado.

De (1) e (2) segue que

$$v_i = \sum_{j=0}^{i} a_{ij}e_j \; + \; \sum_{j=l+1}^{k} a_{ij}e_j, \quad \text{com } a_{ii} \neq 0, \qquad i = 0, \ldots, l-1, l.$$

Como $a_{ll} \neq 0$ e $a_{il} = 0$ quando $i < l$, temos que $\sum_{i=0}^{l} c_i v_i$ implica em $c_l = 0$. Assim, $\sum_{i=0}^{l-1} c_i v_i = 0$ e aplicando a hipótese de indução obtemos $c_0 = \cdots = c_{l-1} = 0$.

■

4.3 Operadores derivativos

Seja K um corpo arbitrário. Nesta seção vamos assumir que p é um primo se a característica de K é finita igual a p e $p = +\infty$ se char$K$=0.

Seja V um espaço vetorial de dimensão finita sobre K. Todo operador linear $T : V \to V$ induz um operador linear $DT : \bigwedge^h V \to \bigwedge^h V$ definido por

$$DT(v_0 \wedge \cdots \wedge v_{h-1}) = \sum_{i=0}^{h-1} v_0 \wedge \cdots \wedge v_{i-1} \wedge T(v_i) \wedge v_{i+1} \wedge \cdots \wedge v_{h-1}$$

que chamamos de *operador derivativo* de T.

Nosso objetivo é mostrar que existe um subespaço cíclico com respeito a DT com dimensão maior ou igual a $\min\{p, (k-h)h+1\}$, onde k é a dimensão de um certo subespaço cíclico com respeito a T. Para isso precisamos saber como se comportam as potências $(DT)^n$ do operador derivativo.

Vamos ver primeiro o que acontece com DT no caso particular em que T é diagonalizável e possui $(V : K)$ autovalores distintos. Denotemos por $h^\wedge A$ o conjunto das somas de h elementos distintos de um conjunto A, assim

$$h^\wedge A = \{a_0 + a_1 + \cdots + a_{h-1} \; : \; a_i \in A \text{ e } a_i \neq a_j \text{ para todo } i \neq j\}.$$

Denotemos ainda por $\sigma(DT)$ o conjunto dos autovalores de DT e $C_{DT}(w)$ o subespaço cíclico com respeito a DT gerado por $w \in \bigwedge^h V$.

Proposição 4.6. *Seja $T : V \to V$ um operador diagonalizável. Então DT é diagonalizável. Além disso, se T possui $(V : K)$ autovalores distintos, então*

$$\sigma(DT) = h^\wedge\sigma(T) \quad e \quad |h^\wedge\sigma(T)| \geqslant (C_{DT}(w) : K),$$

para todo $w \in \bigwedge^h V$.

Demonstração. Seja $k = (V : K)$, $\sigma(T) = \{a_0, a_1, \ldots, a_{k-1}\}$ e $\{f_0, f_1, \ldots, f_{k-1}\}$ base de autovetores de V tal que $T(f_i) = a_i f_i$, $i = 0, 1, \ldots, k-1$. Então

$$\mathcal{I} = \{f_{i_1} \wedge \cdots \wedge f_{i_h} : k-1 \geqslant i_1 > \ldots > i_h \geqslant 0\}$$

é a base de $\bigwedge^h V$ induzida pela base de autovetores de V. Além disso,

$$\begin{aligned} DT(f_{i_1} \wedge \cdots \wedge f_{i_h}) &= \sum_{j=1}^{h} f_{i_1} \wedge \cdots \wedge T(f_{i_j}) \wedge \cdots \wedge f_{i_h} \\ &= \sum_{j=1}^{h} f_{i_1} \wedge \cdots \wedge a_{i_j} f_{i_j} \wedge \cdots \wedge f_{i_h} \\ &= \sum_{j=1}^{h} a_{i_j} \left(f_{i_1} \wedge \cdots \wedge f_{i_h}\right) \\ &= \left(a_{i_1} + \cdots + a_{i_h}\right) f_{i_1} \wedge \cdots \wedge f_{i_h}, \end{aligned}$$

para todo $f_{i_1} \wedge \cdots \wedge f_{i_h} \in \mathcal{I}$. Portanto DT é diagonalizável e, se $a_i \neq a_j$ para todo $i \neq j$, temos $\sigma(DT) = h^{\wedge}\sigma(DT)$. A outra afirmação é consequência imediata da Proposição 4.3.

■

Proposição 4.7. *Seja* $T : V \to V$ *um operador linear. Então, para todo* $v \in V$,

$$(DT)^n \left(T^{h-1}(v) \wedge \cdots \wedge T(v) \wedge v\right) = \sum_{\lambda \in P_h(n)} \frac{n!}{\prod_{i,j} h_{ij}^{\lambda}} \bigwedge \left(T(v)^{\lambda}\right),$$

onde $\bigwedge \left(T(v)^{\lambda}\right) = T^{\lambda_1+h-1}(v) \wedge T^{\lambda_2+h-2}(v) \wedge \cdots \wedge T^{\lambda_{h-1}+1}(v) \wedge T^{\lambda_h}(v)$.

Demonstração. Usaremos indução sobre n. Quando $n = 1$, aplicando a definição de DT obtemos

$$(DT)\left(T^{h-1}(v) \wedge \cdots \wedge T(v) \wedge v\right) = T^h(v) \wedge T^{h-2} \wedge \cdots \wedge T(v) \wedge v = \bigwedge \left(T(v)^{(1,0,\ldots,0)}\right).$$

Suponhamos então que o resultado é válido para n. Então

$$\begin{aligned} (DT)^{n+1}\left(T^{h-1}(v) \wedge \cdots \wedge T(v) \wedge v\right) &= DT\left((DT)^n \left(T^{h-1}(v) \wedge \cdots \wedge T(v) \wedge v\right)\right) \\ &= DT\left(\sum_{\lambda \in P_h(n)} \frac{n!}{\prod_{i,j} h_{ij}^{\lambda}} \bigwedge \left(T(v)^{\lambda}\right)\right) \\ &= \sum_{\lambda \in P_h(n)} \frac{n!}{\prod_{i,j} h_{ij}^{\lambda}} DT\left(\bigwedge_{i=1}^{h} T^{\lambda_i+h-i}(v)\right) \\ &= \sum_{\lambda \in P_h(n)} \frac{n!}{\prod_{i,j} h_{ij}^{\lambda}} \sum_{t=1}^{h} \bigwedge_{i=1}^{h} T^{\lambda_i+h-i+\delta_{it}}(v). \end{aligned}$$

Como $x_1 \wedge \cdots \wedge x_h = 0$ se existe $i \neq j$ tal que $x_i = x_j$, temos

$$(DT)^{n+1}\left(T^{h-1}(v) \wedge \cdots \wedge T(v) \wedge v\right) = \sum_{\lambda \in P_h(n)} \frac{n!}{\prod_{i,j} h_{ij}^{\lambda}} \sum_{t \notin \{i:\lambda_i = \lambda_{i+1}\}}^{h} \bigwedge_{i=1}^{h} T^{\lambda_i + h - i + \delta_{it}}(v).$$

Fixemos agora $\lambda \in P_h(n)$. Para cada $t \in \{1, \ldots, h\}$ tal que $\lambda_t \neq \lambda_{t+1}$, seja $\chi = (\chi_1, \ldots, \chi_h)$ dado por

$$\chi_i = \lambda_i + \delta_{it}, \qquad i = 1, \ldots, h.$$

Então $\chi \in P_h(n+1)$ e $\lambda \to \chi$. Reciprocamente, seja $\chi \in P_h(n+1)$ tal que $\lambda \to \chi$. Por definição, existe $j \in \{1, \ldots, h\}$ tal que

$$\chi_i = \lambda_i + \delta_{ij}, \qquad i = 1, \ldots, h.$$

Seja $t = j$. Então $\lambda_t = \chi_j - 1 < \chi_{j+1} = \lambda_{t+1}$.

Estabelecemos portanto um bijeção entre

$$\{t \in \{1, \ldots, h\} : \lambda_t \neq \lambda_{t+1}\} \quad \text{e} \quad \{\chi \in P_h(n+1) : \lambda \to \chi\},$$

donde segue que

$$\begin{aligned}(DT)^{n+1}\left(T^{h-1}(v) \wedge \cdots \wedge T(v) \wedge v\right) &= \sum_{\lambda \in P_h(n)} \frac{n!}{\prod_{i,j} h_{ij}^{\lambda}} \sum_{\substack{\chi \in P_h(n+1) \\ \lambda \to \chi}} \bigwedge_{i=1}^{h} T^{\chi_i + h - i}(v) \\ &= \sum_{\chi \in P_h(n+1)} \left(\sum_{\substack{\lambda \in P_h(n) \\ \lambda \to \chi}} \frac{n!}{\prod_{i,j} h_{ij}^{\lambda}} \right) \bigwedge_{i=1}^{h} T^{\chi_i + h - i}(v).\end{aligned}$$

Aplicando o Corolário 3.24, obtemos

$$(DT)^{n+1}\left(T^{h-1}(v) \wedge \cdots \wedge T(v) \wedge v\right) = \sum_{\chi \in P_h(n+1)} \frac{(n+1)!}{\prod_{i,j} h_{ij}^{\chi}} \bigwedge \left(T(v)^{\chi}\right).$$

■

O próximo passo é mostrar que a dimensão do subespaço cíclico com respeito a DT gerado por $T^{h-1}(v) \wedge \cdots \wedge T(v) \wedge v \in \bigwedge^h V$ é maior ou igual a $\min\{p, (k-h)h+1\}$, onde $k = (C_T(v) : K)$. Para isso, precisamos do seguinte resultado.

Lema 4.8. *Seja $\{e_0, e_1, \ldots, e_{k-1}\}$ uma base de V e suponhamos que $k \geqslant h$. Então*

$$\left\{ e_{\lambda_1 + h - 1} \wedge \cdots \wedge e_{\lambda_{h-1}+1} \wedge e_{\lambda_h} \ : \ \lambda \in \bigcup_{n \in \mathbb{N}_0} P_h(n) \text{ e } \lambda_1 \leqslant k - h \right\}$$

é uma base de $\bigwedge^h V$.

Demonstração. Consideremos a aplicação

$$g : (\lambda_1, \ldots, \lambda_h) \mapsto (\lambda_1 + h - 1, \ldots, \lambda_{h-1} + 1, \lambda_h)$$

do conjunto $\{\lambda : \lambda \in \bigcup_{n\in\mathbb{N}_0} P_h(n) \text{ e } \lambda_1 \leqslant k - h\}$ em $\{(i_1, \ldots, i_h) : k - 1 \geqslant i_1 > \cdots > i_h \geqslant 0\}$.

Afirmamos que g é bijeção. De fato, para $(i_1, \ldots, i_h)$ com $k - 1 \geqslant i_1 > \cdots > i_h \geqslant 0$, seja

$$\lambda_j = i_j - h + j, \quad j = 1, \ldots, h.$$

Então

$$\begin{aligned}
&\lambda_j = i_j - h + j \geqslant i_{j+1} - h + j + 1 = \lambda_{j+1}, \quad j = 1, \ldots, h-1\\
&\lambda_1 = i_1 - h + 1 \leqslant k - h\\
&\lambda_h = i_h \geqslant 0,
\end{aligned}$$

donde segue que g é sobrejetiva. Além disso, se $g(\lambda) = g(\mu)$ então $\lambda_i + h - i = \mu_i + h - i$, para todo $i \in \{1, \ldots, h\}$, e portanto $\lambda = \mu$.

Como g é bijeção e $\{e_{i_1} \wedge \cdots \wedge e_{i_h} : k - 1 \geqslant i_1 > \cdots > i_h \geqslant 0\}$ é base de $\bigwedge^h V$, temos o resultado desejado.

■

Teorema 4.9 (Dias da Silva-Hamidoune). *Seja $T : V \to V$ um operador linear, $v \in V$, $k = (C_T(v) : K)$ e $w = T^{h-1}(v) \wedge \cdots \wedge T(v) \wedge v \in \bigwedge^h V$. Então*

$$(C_{DT}(w) : K) \geqslant \min\{p, (k - h)h + 1\}.$$

Demonstração. Se $k < h$ o resultado é óbvio. Suponhamos, então, que $k \geqslant h$. Vamos mostrar que $w, (DT)(w), \ldots, (DT)^r(w)$, onde $0 \leqslant r \leqslant \min\{p - 1, (k - h)h\}$, são linearmente independentes.

Como $\{v, T(v), \ldots, T^{k-1}(v)\}$ é uma base de $C_T(v)$, do Lema 4.8 segue que

$$\mathcal{I} = \left\{ \bigwedge (T(v)^\lambda) \ : \ \lambda \in \bigcup_{n\in\mathbb{N}_0} P_h(n) \text{ e } \lambda_1 \leqslant k - h \right\}$$

é uma base de $\bigwedge^h C_T(v)$. Seja $\mathcal{B}$ uma base de $\bigwedge^h V$ contendo $\mathcal{I}$.

Vamos agora construir partições de $P_h(n)$, $n = 0, 1, \ldots, \min\{p-1, (k-h)h\}$, que denotamos por $\lambda^{(n)}$, satisfazendo

(1) $\bigwedge (T(v)^{\lambda^{(n)}}) \in \mathcal{I}$,

(2) na expressão de $(DT)^n(w)$ na base $\mathcal{B}$, o coeficiente de $\bigwedge (T(v)^{\lambda^{(n)}})$ é não nulo,

(3) se $l \in \{0, 1, \ldots, \min\{p-1, (k-h)h\}\}$ e $l > n$, então o coeficiente de $\bigwedge(T(v)^{\lambda^{(l)}})$ é igual a zero na expressão de $(DT)^n(w)$ na base $\mathcal{B}$.

Feito isso, o Lema 4.5 nos diz que

$$\{\ (DT)^n(w) : 0 \leqslant n \leqslant \min\{p-1, (k-h)h\}\ \}$$

é um conjunto linearmente independente, como queríamos.

Seja $n \in \{0, 1, \ldots, \min\{p-1, (k-h)h\}\}$ e escrevamos $n = rh + t$, com $0 \leqslant t \leqslant h-1$ e $r \geqslant 0$. Temos

$$\lambda^{(n)} := (\ \underbrace{r+1, \ldots, r+1}_{t}\ ,\ \underbrace{r, \ldots, r}_{h-t}\ )\ \in P_h(n).$$

Se $t = 0$, então $rh = n \leqslant (k-h)h$ e portanto $\lambda_1^{(n)} = r \leqslant k-h$. Se $t > 0$, segue que $rh < n \leqslant (k-h)h$ e também $\lambda_1^{(n)} = r+1 \leqslant k-h$. Assim, obtemos **(1)**.

Pela Proposição 4.7,

$$(DT)^n(w) = \frac{n!}{\prod_{i,j} h_{ij}^{\lambda^{(n)}}} \bigwedge(T(v)^{\lambda^{(n)}}) + \sum_{\substack{\lambda \in P_h(n) \\ \lambda \neq \lambda^{(n)}}} \frac{n!}{\prod_{i,j} h_{ij}^{\lambda}} \bigwedge(T(v)^{\lambda}).$$

Fixemos $\lambda \in P_h(n) - \{\lambda^{(n)}\}$. Se $\lambda_1 \leqslant k-h$, $\bigwedge(T(v)^{\lambda}) \in \mathcal{I}$. Suponhamos que $\lambda_1 > k-h$ e

$$T^{\lambda_i + h - i}(v) = \sum_{j=0}^{k-1} a_{ij} T^j(v), \qquad i = 1, 2, \ldots, h. \tag{4.2}$$

Então,

$$\begin{aligned} \bigwedge(T(v)^{\lambda}) &= \left(\sum_{j_1=0}^{k-1} a_{1,j_1} T^{j_1}(v)\right) \wedge \cdots \wedge \left(\sum_{j_h=0}^{k-1} a_{h,j_h} T^{j_h}(v)\right) \\ &= \sum_{j_1=0}^{k-1} \cdots \sum_{j_h=0}^{k-1} \left(\prod_{i=1}^{h} a_{i,j_i}\right) \bigwedge_{i=1}^{h} T^{j_i}(v). \end{aligned} \tag{4.3}$$

Observemos em (4.2) que, se $\lambda_i + h - i \leqslant k-1$, temos $a_{ij} = \delta_{\lambda_i + h - i, j}$. Consideremos $(j_1, \ldots, j_h)$ tal que $\prod_{i=1}^{h} a_{i,j_i} \neq 0$. Então, para cada $i = 2, \ldots, h$,

$$\lambda_i + h - i > k-1 \quad \text{ou} \quad j_i = \lambda_i + h - i,$$

donde segue que

$$j_i \leqslant \lambda_i + h - i, \qquad i = 2, \ldots, h, \quad \text{e} \quad j_1 \leqslant k-1 < \lambda_1 + h - 1. \tag{4.4}$$

Ordenando $j_1, \ldots, j_h$ de forma decrescente obtemos a sequência

$$k-1 \geqslant l_1 \geqslant \cdots \geqslant l_h \geqslant 0$$

e

$$\bigwedge_{i=1}^{h} T^{j_i}(v) = \pm \bigwedge_{i=1}^{h} T^{l_i}(v).$$

Se $l_i = l_{i'}$, para $i \neq i'$, então $\bigwedge_{i=1}^{h} T^{j_i}(v) = 0$. Suponhamos que

$$k - 1 \geqslant l_1 > \cdots > l_h \geqslant 0.$$

Seja $\gamma = (\gamma_1, \ldots, \gamma_h)$, com $\gamma_i = l_i - h + i$, para $i = 1, \ldots, h$. Então $k - h \geqslant \gamma_1 \geqslant \cdots \geqslant \gamma_h \geqslant 0$ e

$$\sum_{i=1}^{h} \gamma_i = \sum_{i=1}^{h} l_i + \sum_{i=1}^{h} (-h + i) = \sum_{i=1}^{h} j_i + \sum_{i=1}^{h} (-h + i).$$

Segue agora de (4.4) que $\sum_{i=1}^{h} \gamma_i < \sum_{i=1}^{h} \lambda_i = n$ e portanto

$$\gamma \in \bigcup_{0 \leqslant m < n} P_h(m).$$

Provamos então que, para cada $(j_1, \ldots, j_h)$ tal que $\prod_{i=1}^{h} a_{i,j_i} \neq 0$, temos $\bigwedge_{i=0}^{h-1} T^{j_i}(v) = 0$ ou $\bigwedge_{i=0}^{h-1} T^{j_i}(v) = \pm \bigwedge(T(v)^{\gamma})$, com $\gamma \in \bigcup_{0 \leqslant m < n} P_h(m)$ e $\gamma_1 \leqslant k - h$. Com isso e (4.3) obtemos

$$(DT)^n(w) = \frac{n!}{\prod_{i,j} h_{ij}^{\lambda^{(n)}}} \bigwedge \left(T(v)^{\lambda^{(n)}} \right) + \sum_{\substack{\lambda \in P_h(n) \\ \lambda \neq \lambda^{(n)} \\ \lambda_1 \leqslant k-h}} \frac{n!}{\prod_{i,j} h_{ij}^{\lambda}} \bigwedge \left(T(v)^{\lambda} \right) + \sum_{\substack{\gamma \in \bigcup_m P_h(m) \\ 0 \leqslant m < n \\ \lambda_1 \leqslant k-h}} b_\gamma \bigwedge \left(T(v)^{\gamma} \right),$$

onde $b_\gamma \in K$, para cada γ.

Na expressão acima, escrevemos $(DT)^k(w)$ como combinação linear dos elementos de $\mathcal{I} \subset \mathcal{B}$. Como $n \leqslant p - 1$, o coeficiente de $\bigwedge \left(T(v)^{\lambda^{(n)}} \right)$ é não-nulo, valendo portanto **(2)**. Além disso, se $l, n \in \{0, 1, \ldots, \min\{p - 1, (k - h)h\}\}$, com $l > n$, então $\lambda^{(l)} \notin P_h(n)$ e $\lambda^{(l)} \notin \bigcup_{0 \leqslant m < n} P_h(m)$. Isso verifica **(3)** e conclui a demonstração.

■

4.4 Demonstração do Teorema 1.1

Nas seções anteriores obtemos todos os resultados necessários para a demonstração do Teorema de Dias da Silva e Hamidoune, que prova a conjectura de Erdős e Heilbronn.

Teorema (Dias da Silva-Hamidoune). *Seja K um corpo, p a característica de K, se ela é finita, e $p = \infty$ se a característica de K é igual a 0. Seja A um subconjunto finito de K e h um inteiro positivo. Então,*

$$|h^{\wedge}A| \geqslant \min\{p, h|A| - h^2 + 1\},$$

onde $h^{\wedge}A$ é o conjunto das somas de h elementos distintos de A.

Demonstração. Se $h > |A|$, o resultado é óbvio. Suponhamos então que $h \leqslant |A| = k$ e consideremos um operador linear $T : K^k \to K^k$ tal que $\sigma(T) = A$. Da Proposição 4.6 segue que $\sigma(DT) = h^{\wedge}A$ e $|h^{\wedge}A| \geqslant (C_{DT}(w) : K)$, para todo $w \in \bigwedge^h(K^k)$. Então, aplicando a Proposição 4.4 e o Teorema 4.9 obtemos $|h^{\wedge}A| \geqslant \min\{p, h|A| - h^2 + 1\}$.

■

Por fim, vamos fazer uma observação sobre o coeficiente que aparece na expressão dada pela Proposição 4.7 das potências do operador DT.

Sejam $a = (a_1, a_2, \ldots, a_h)$ e $b = (b_1, b_2, \ldots, b_h) \in \mathbb{Z}^h$. Dizemos que uma seqüência de vetores

$$a = v_1,\ v_2, \ldots,\ v_m = b$$

é um *caminho* em $\mathbb{Z}^h$ se $v_j - v_{j-1} \in \{e_1, e_2, \ldots, e_h\}$, $j = 2, \ldots, m$, onde $e_i = (0, \ldots, 0, 1, 0 \ldots, 0)$ é o vetor com coordenada i igual a 1 e as demais iguais a 0. Um vetor $w = (w_1, w_2, \ldots, w_h) \in \mathbb{Z}^h$ é *estritamente decrescente* se $w_1 > w_2 > \cdots > w_h$ e uma seqüência $a = v_1,\ v_2, \ldots,\ v_m = b$ é um *caminho estritamente decrescente* se cada v_i é estritamente decrescente, $i = 1, 2, \ldots h$.

Sejam $a = (h-1, h-2, \ldots, 1, 0)$ e $b = (b_1, b_2, \ldots, b_h)$ um vetor em $\mathbb{Z}^h$ estritamente decrescente. Pode-se mostrar [18] que o número de caminhos estritamente decrescentes de a até b é dado por

$$\frac{\left[b_1 + b_2 + \cdots + b_h - \binom{h}{2}\right]!}{b_1!\ b_2!\ \cdots\ b_h!} \prod_{1 \leqslant i < j \leqslant h} (b_i - b_j), \qquad h \geqslant 2.$$

Vamos agora observar as potências de DT aplicadas no vetor $w = T(v) \wedge v$.

$$\begin{aligned}
(DT)(T(v) \wedge v) &= T^2(v) \wedge v \\
(DT)^2(T(v) \wedge v) &= T^3(v) \wedge v + T^2(v) \wedge T(v) \\
(DT)^3(T(v) \wedge v) &= T^4(v) \wedge v + 2\,[T^3(v) \wedge T(v)]
\end{aligned}$$

Se representarmos por $(1, 0)$ o vetor $T(v) \wedge v$, onde o 1 indica a potência de T em $T(v)$ e o 0 a potência de T em $v = T^0(v)$, vemos que na expressão de $(DT)^3(w)$ aparece o vetor $(3, 1)$ com coeficiente igual a 2. Isso porque, partindo de $(1, 0)$, temos dois caminhos estritamente decrescentes para chegar em (3,1), que são

$$v_1 = (1, 0),\ v_2 = (2, 0),\ v_3 = (3, 0),\ v_4 = (3, 1)$$

e

$$v_1 = (1, 0),\ v_2 = (2, 0),\ v_3 = (2, 1),\ v_4 = (3, 1).$$

O que vamos mostrar então é que, na expressão de $(DT)^n(T^{h-1} \wedge \cdots \wedge T(v) \wedge v)$ dada pela Proposição 4.7, o coeficiente do vetor $\bigwedge(T(v)^{\lambda})$ pode ser representado pelo número de caminhos

estritamente decrescentes de $(h-1,\ldots,1,0)$ até $(l_1,l_2,\ldots,l_h)=(\lambda_1+h-1,\lambda_2+h-2,\ldots,\lambda_h)$, onde $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_h)\in P_h(n)$, ou seja,

$$\frac{n!}{\prod_{i,j}h_{ij}^{\lambda}}=\frac{\left[l_1+l_2+\cdots+l_h-\binom{h}{2}\right]!}{l_1!\;l_2!\;\cdots\;l_h!}\prod_{1\leqslant i<j\leqslant h}(l_i-l_j)=\frac{n!}{l_1!\;l_2!\;\cdots\;l_h!}\prod_{1\leqslant i<j\leqslant h}(l_i-l_j).$$

Precisamos então mostrar que

$$\prod_{i,j}h_{ij}^{\lambda}\prod_{1\leqslant i<j\leqslant h}(l_i-l_j)=l_1!\;l_2!\;\cdots\;l_h!. \tag{4.5}$$

Exemplo 4.10. Seja $\lambda=(5,3,1,1)\in P_4(10)$. Então,

Diagrama de λ	Comprimentos dos ganchos	$l_i=\lambda_i+4-i$
λ_1 □ □ □ □ □ λ_2 □ □ □ λ_3 □ λ_4 □	$h_{11}=8\;\; h_{12}=5\;\; h_{13}=4\;\; h_{14}=2\;\; h_{15}=1$ $h_{21}=5\;\; h_{22}=2\;\; h_{23}=1$ $h_{31}=2$ $h_{41}=1$	$l_1=8$ $l_2=5$ $l_3=2$ $l_4=1$

Podemos observar que $l_i=h_{i1}$, para todo $i=1,2,3,4$. Isso é de fato verdade para toda partição $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_h)$, pois

$$h_{i1}=\lambda_i-1+\lambda'_1-i+1=\lambda_i+h-i=l_i,\qquad i=1,2,\ldots,h,$$

onde $\lambda'=(\lambda'_1,\lambda'_2,\ldots,\lambda'_h)$ é a partição conjugada de λ.

Representando $(l_1,l_2,\ldots,l_h)$ pelo diagrama de Young, obtemos

Diagrama de $(l_1,l_2,\ldots,l_h)$	Diferenças (l_i-l_j) com $i<j$
l_1 □ □ □ □ □ □ □ □ l_2 □ □ □ □ □ l_3 □ □ l_4 □	$l_1-l_4=7\;\; l_1-l_3=6\;\; l_1-l_2=3$ $l_2-l_4=4\;\; l_2-l_3=3$ $l_3-l_4=1$

Com as tabelas acima, vemos que

$$\begin{aligned}
&h_{11}\cdot(l_1-l_4)\cdot(l_1-l_3)\cdot h_{12}\cdot h_{13}\cdot(l_1-l_2)\cdot h_{14}\cdot h_{15} \;=\; l_1!\\
&h_{21}\cdot(l_2-l_4)\cdot(l_2-l_3)\cdot h_{22}\cdot h_{23} \;=\; l_2!\\
&h_{31}\cdot(l_3-l_4) \;=\; l_3!\\
&h_{41} \;=\; l_4!
\end{aligned}$$

e, neste caso paticular, (4.5) se verifica.

Para mostrar (4.5) vamos usar indução sobre λ_1, onde $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_h)$. Se $\lambda_1 = 1$, então $\lambda = (1, 1, \ldots, 1)$ e

Diagrama de λ		Diagrama de $(l_1, l_2, \ldots, l_h)$	
λ_1	$\square$	$l_1 = h$	$\square\ \square\ \cdots\ \square\ \square$
λ_2	$\square$	$l_2 = h-1$	$\square\ \square\ \cdots\ \square$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
λ_{h-1}	$\square$	$l_{h-1} = 2$	$\square\ \square$
λ_h	$\square$	$l_h = 1$	$\square$

donde segue que $\prod_i h_{i1} \prod_{i<j}(l_i - l_j) = l_1! \cdots l_h!$. Suponhamos então que o resultado seja válido para toda partição $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_h)$, com $\lambda_1 < k$.

Seja $\lambda = (k, \lambda_2, \ldots, \lambda_h)$ e $[\lambda]$ o Diagrama de Young de λ. Vimos no Exemplo 4.10 que $h_{i1} = l_i$, para todo $i = 1, 2, \ldots, h$. Consideremos então a partição $\overline{\lambda} = (k-1, \lambda_2 - 1, \ldots, \lambda_h - 1)$ obtida ao retirarmos a primeira coluna de $[\lambda]$. Então $\overline{\lambda}$ possui exatamente λ'_2 partes não nulas e, aplicando a hipótese de indução, temos

$$\prod_{i,j} h_{ij}^{\overline{\lambda}} \prod_{1 \leqslant i < j \leqslant \lambda'_2} (\overline{l_i} - \overline{l_j}) = \overline{l_1}!\ \overline{l_2}!\ \cdots\ \overline{l_{\lambda'_2}}!. \tag{4.6}$$

Mas como o diagrama de $\overline{\lambda}$ é igual a $[\lambda]$ sem a primeira coluna, temos

$$\prod_{i,j} h_{ij}^{\overline{\lambda}} = \frac{\prod_{i,j} h_{ij}^{\lambda}}{h_{11} h_{21} \cdots h_{h1}} = \frac{\prod_{i,j} h_{ij}^{\lambda}}{l_1 l_2 \cdots l_h}. \tag{4.7}$$

Além disso, para $1 \leqslant i < j \leqslant \lambda'_2$, temos

$$\begin{aligned} &\overline{l_i} - \overline{l_j} = [\lambda_i - 1 + \lambda'_2 - i - (\lambda_j - 1 + \lambda'_2 - j)] = \lambda_i - i - \lambda_j + j = l_i - l_j, \\ &\overline{l_i} = (\lambda_i - 1) + \lambda'_2 - i = \lambda_i + r - i - (r - \lambda'_2 + 1) = l_i - (h - \lambda'_2 + 1). \end{aligned} \tag{4.8}$$

Assim, substituindo (4.7) e (4.8) em (4.6), obtemos

$$\frac{\prod_{i,j} h_{ij}^{\lambda}}{l_1 l_2 \cdots l_h} \frac{\displaystyle\prod_{1 \leqslant i < j \leqslant h} (l_i - l_j)}{\displaystyle\prod_{\substack{\lambda'_2 < j \leqslant h \\ 1 \leqslant i < j}} (l_i - l_j)} = (l_1 - h + \lambda'_2 - 1)!\ (l_2 - h + \lambda'_2 - 1)!\ \cdots\ (l_{\lambda'_2} - h + \lambda'_2 - 1)!.$$

Mas, para $1 \leqslant i \leqslant \lambda'_2$, temos

$$\begin{aligned} l_i - l_h &= l_i - \underbrace{\lambda_h}_{=1} = l_i - 1 \\ l_i - l_{h-1} &= l_i - (\underbrace{\lambda_{h-1}}_{=1} + h - h + 1) = l_i - 2 \\ &\vdots \\ l_i - l_{\lambda'_2+1} &= l_i - (\underbrace{\lambda_{\lambda'_2+1}}_{=1} + h - \lambda'_2 - 1) = l_i - h + \lambda'_2 \end{aligned}$$

e, para $\lambda'_2 < i < j \leqslant h$, temos

$$\begin{aligned} l_i - l_h &= l_i - 1 \\ l_i - l_{h-1} &= l_i - 2 \\ &\vdots \\ l_i - l_{i+1} &= 1, \end{aligned}$$

o que implica que a equação (4.5) também vale quando $\lambda_1 = k$, como queríamos.

Bibliografia

[1] N. Alon, M. B. Nathanson & I.Z. Ruza — *Adding distinct congruence classes modulo a prime.* Am. Math. Monthly, 102: 250-255, 1995.

[2] M. Burrow — *Representation theory of finite groups.* New York: Academic Pres s, 1965.

[3] Cristina Caldeira — *Alguns resultados em teoria aditiva linear.* Dissertação de Doutorado em Matemática, Faculdade de Ciências e Tecnologia da Universidade de Coimbra, 1998.

[4] A. Cauchy — *Recherches sur les nombres.* J. École Polytech, 9: 99-116, 1813.

[5] C.W. Curtis & I. Reiner — *Representation theory of finite groups and associative algebras.* New York: Interscience Publishers, 1962.

[6] H. Davenport — *On the addition of residue classes.* J. London Math. Soc., 10: 30-32, 1935.

[7] H. Davenport — *A historical note.* J. London Math. Soc., 22: 100-101, 1947.

[8] J.A. Dias da Silva & Y.O. Hamidoune — *A note on the minimal polynomial of the Kronecker sum of two linear operators* . Linear Algebra Appl., 141: 283-287, 1990.

[9] J.A. Dias da Silva & Y.O. Hamidoune — *Cyclic Spaces for a Grassmann Derivatives and Additive Theory* . Bull. London Math. Soc., 26: 140-146, 1994.

[10] J.A. Dias da Silva & H. Godinho — *Generalized derivations and additive theory.* J. Linear Algebra and Appl., 342: 1-15, 2002.

[11] P. Erdős — *On the addition of residue classes (*mod *p).* In Proceedings of the 1963 Number Theory Conference at the University of Colorado, pages 16-17, Boulder, 1963. University of Colorado.

[12] P. Erdős & H. Heilbronn — *On the addition of residue classes* mod *p.* Acta Arith., 9: 149-159, 1964.

[13] H. Godinho — *Linear algebraic techniques in additive theory and a generalization of the Cauchy-Davenport theorem.* Mat. Contemporânea, 21: 105-115, 2002.

[14] G. James & M. Liebeck — *Representations and characters of groups.* London: Cambridge University Press, 1993.

[15] G. James & A. Kerber — *The representation theory of the symmetric group.* London: Addison-Wesley Publishing Company, 1981.

[16] V.F. Lev — *Restricted set addition in groups I: the classical setting.* J. London Math. Soc. (2), 62: 27-40, 2000.

[17] M. B. Nathanson — *An inverse theorem for sums of sets of lattice points.* J. Number Theory, 46: 29-59, 1994.

[18] M. B. Nathanson — *Additive Number Theory.* New York: Springer, 1996.

[19] H.J. Ryser — *Combinatorial mathematics.* New Jersey: John Wiley and sons, 1963.

Índice Remissivo

KG-módulo
- KG-isomorfismo, 17
- KG-submódulo, 17
- à direita, 16
- à esquerda, 16
- completamente irredutível, 17
- conjunto completo , 18
- irredutível, 17
- regular, 17
- representação correspondente a , 17

R-isomorfismo, 18
R-módulo, 18
R-submódulo, 18
álgebra de grupo, 16

aplicação anti-simétrica, 55
aplicação balanceada, 19

bimódulo , 19

caracter
- definição, 32
- irredutível, 32
- permutação, 32

classe dupla, 28
composição, 34
conjunto crítico, 9
constituinte comum, 24
corpo de decomposição, 25

dissecção, 35

espaço de Grassmann
- base induzida, 57
- definição, 55

lema de Schur, 24

módulo induzido, 21
módulo permutação, 32
matriz permutação, 15
matrizes 0-1, 38

operador derivativo, 60
ordem lexicográfica, 41
ordem sobre as somas parciais, 41

partes de uma partição, 34
partição
- comprimento de , 52
- conjugada, 39
- definição, 34

partições vizinhas, 41
produto tensorial
- definição, 19
- representação, 20

produto tensorial externo, 26
propriedade de interseção trivial, 38

representação
- 1-representações, 15
- 1-representações de S_n, 35
- absolutamente irredutível, 25

definição, 14
espaço de , 14
extensão do corpo de, 25
grau de, 14
induzida, 21
módulo correspondente a , 17
matricial, 14
realizada, 26
regular, 15
trivial, 23
representações equivalentes, 14

subgrupo diagonal, 27

teorema
do número de constituintes comuns, 31
do produto tensorial, 30
do subgrupo, 29
Gale e Ryser, 44

Young
diagrama de, 39
subgrupo de , 35