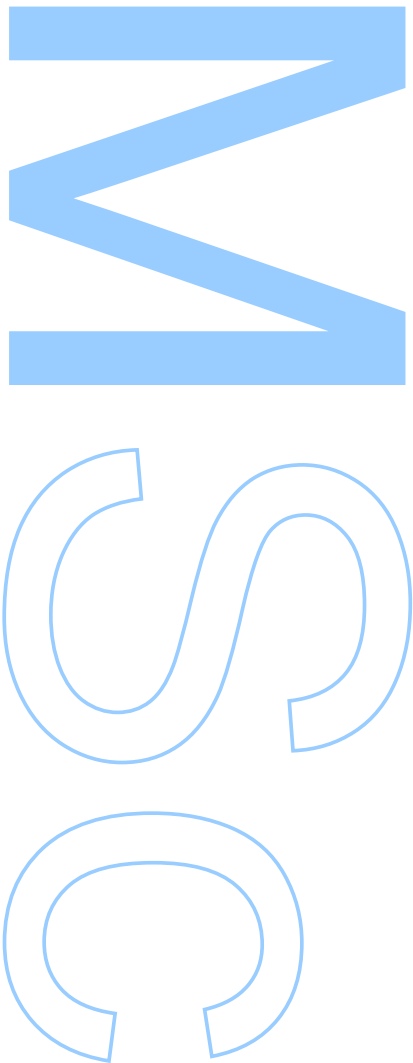
Teorema da Extensão de MacWilliams

Patrícia Reis dos Reis
2.° Ciclo
Departamento de Matemática
2018

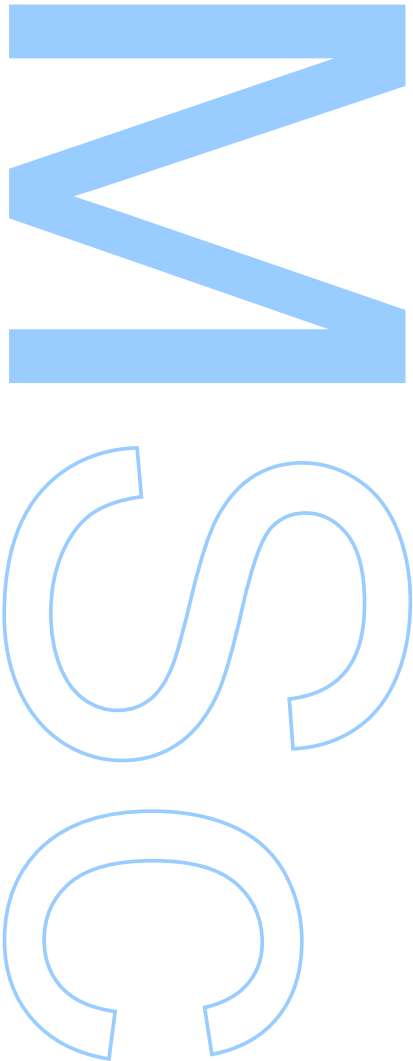
Orientador
Christian Edgar Lomp, Professor Auxiliar, FCUP



Todas as correções determinadas pelo júri, e só essas, foram efetuadas.

O Presidente do Júri,

Porto, _____/_____/_____



Agradecimentos

Em primeiro lugar gostaria de agradecer à minha irmã Magna por ser a irmã mais chata de sempre e pela maravilhosa menina que é, o que me motiva todos os dias a ser melhor. Agradeço a todos os meus amigos que me acompanharam e apoiaram nos últimos 5 anos por todo o apoio. Em especial queria agradecer à Lili pela Grande paciência, à Patrícia pelo companheirismo e bons conselhos, à São pelas risadas, ao Ricardo e à Inês por todas as ajudas, à Raquel pelas boleias, boa música e companhia em saídas, à Joana pela motivação, boa música e inspiração, à Margarida por todas as conversas de café, à Sofia pela sua autoconfiança inspiradora e ao Miguel e à Diana por tudo. De seguida, mas não menos importante quero agradecer aos dois padrinhos de faculdade incríveis que tenho, Ana e Gil, por todo o apoio, sabedoria que me tentaram incutir e pelas mil e uma coisas pelas quais tenho de agradecer. De entre os amigos não me posso esquecer também de agradecer às minhas duas grandes amigas de secundário Daniela e Xénia por todo o apoio, bons momentos e muito mais.

Falta ainda agradecer ao Professor Christian Lomp pela paciência e pelo excelente trabalho como meu orientador, bem como por toda a matemática que me ensinou. Deixo também um agradecimento especial a mais dois professores, a Professora Paula Lomp e o Professor António Machiavelo. À primeira pelas ajudas na correção da tese e por toda a álgebra que me ensinou. Ao segundo pelas incríveis aulas que me fizeram entender o que realmente quero fazer com a matemática.

Para finalizar gostaria de agradecer à minha família em especial às minhas 3 incríveis tias, Sofia, Elsa e Fernanda, pelo apoio e ajudas, e ao meu Pai por todos os sacrifícios.

Resumo

F.J. MacWilliams mostrou na sua tese de doutoramento o seu famoso Teorema da Extensão no âmbito do seu trabalho sobre teoria de códigos. Este diz que uma isometria entre dois código lineares sobre o mesmo corpo que preserva o peso de Hamming pode ser estendida a uma transformação monomial. Posteriormente alguns autores procuraram mostrar uma versão mais geral deste teorema, estudando a sua veracidade em anéis finitos. Conseguiram provar que, nessa nova versão, o Teorema da Extensão de MacWilliams se verifica apenas para anéis de Frobenius. Nesta dissertação é apresentada uma demonstração elementar da versão do teorema para corpos e duas demonstrações para a versão sobre anéis de Frobenius. Estas duas últimas provas usam duas abordagens distintas, a primeira usa elementos de combinatória como a função de Möbius e pesos homogéneos, enquanto que a segunda é baseada numa abordagem mais algébrica usando caracteres complexos.

Palavras-Chave: MacWilliams, códigos lineares, equivalência de códigos, peso de Hamming, anéis de Frobenius, peso homogéneo, função de Möbius, caracteres complexos.

Abstract

F.J. MacWilliams showed in her Ph.D. thesis her famous Extension Theorem for linear codes. Which states that an isometry between two linear codes that preserves the Hamming weight can be extended to a monomial transformation. Subsequently some authors tried to show a more general version of this theorem, for codes over finite rings. They have proved that, in this case, the extension theorem is valid only for Frobenius rings. In this dissertation we present an elementary proof of the extension theorem over fields and two proofs for the version with Frobenius rings. These last proofs use two distinct approaches, the first use combinatorial methods such as the Möbius function and homogeneous weights, while the second is based on a more algebraic approach using complex characters.

Keywords: MacWilliams, linear codes, code equivalence, Hamming weight, Frobenius rings, homogeneous weight, Möbius function, complex caracters.

Conteúdo

Introdução

Florence Jessie MacWilliams teve um importante papel na área da Teoria de Códigos, além dos seus teoremas sobre a identidade de códigos, na sua tese de doutoramento, em 1962, provou o seguinte teorema: Sejam C e D dois códigos lineares sobre o mesmo corpo, se existir um isomorfismo entre eles que preserva o peso de Hamming, então C e D são códigos equivalentes. Onde dois códigos lineares C e D, de comprimento n, são equivalentes se existe uma transformação monomial de F^n que envia um no outro. A este resultado é costume atribuir-se o nome de Teorema da Extensão, pois exposto de outra forma o que MacWilliams demonstrou foi que um isomorfismo que preserva o peso de Hamming entre dois subespaços vetoriais do mesmo espaço vetorial pode ser estendido a uma transformação monomial de todo o espaço linear. Alguns anos após a publicação dos resultados de MacWilliams, em 1994 surgiu um artigo de R. Hammons ([5]) onde é demonstrado que certos códigos não lineares apresentam grandes semelhanças com códigos lineares quando considerados como códigos sobre o anel $\mathbb{Z}_4$ (o anel dos inteiros módulo 4). Estes códigos eram chamados de código de Kerdock, código de Preparata e código de Goethals. De entre as semelhanças com os códigos lineares encontrava-se o facto de os teorema de MacWilliams serem válidos também neste códigos. Consequentemente houve um acrescido interesse sobre teoria algébrica de códigos sobre anéis finitos e em 1999 J.A. Wood publicou um artigo ([15]) onde demonstra que o teorema da extensão de MacWilliams é válido para uma certa classe de anéis finitos. Anéis estes chamados de anéis de Frobenius. Provou também, mais tarde, que não só o teorema era válido para códigos sobre estes anéis, mas também que se o teorema é válido para códigos sobre um anel finito, então este é de Frobenius.

Assim, nesta dissertação, são apresentadas três demonstrações distintas do Teorema da Extensão. A primeira é uma demonstração elementar do teorema para códigos lineares sobre corpos finitos que foi publicada por K. Bogart, D. Goldberg e J. Gordon em [1]. As restantes são demonstrações da versão do teorema para anéis de Frobenius usando duas abordagens diferentes. A primeira abordagem é a apresentada no artigo de M. Greferath e S.E. Schmidt [4] que usa elementos de combinatória como a função de Möbius sobre

conjuntos parcialmente ordenados e pesos homogéneos. A segunda abordagem é a que foi apresentada por J. A. Wood em [15] e utiliza elementos algébricos como caracteres complexos.

No primeiro capítulo (1) são expostas definições e resultados de álgebra, combinatória e teoria de códigos que serão essenciais ás demonstrações dos capítulos seguintes. Estas definições e resultados são na sua maioria baseados nos de [6], [7] e [9]. Os resultados apresentados neste capítulo, são dados sem as demonstrações, algumas destas encontram-se no Anexo e outras são remetidas para a bibliografia. No capítulo 2 é apresentada a demonstração elementar do teorema para códigos sobre corpos finitos, utilizando noções de Álgebra Linear que se assume serem conhecidas pelo leitor. No terceiro capítulo (3) são apresentados alguns resultados sobre anéis de Frobenius assim como a sua definição. No capítulo 4 são então apresentadas as duas demonstrações da versão do teorema para códigos sobre anéis de Frobenius, bem como todos os restantes resultados essenciais às provas que não foram expostos nos capítulos anteriores. Finalizamos com um pequeno capítulo, capítulo 5, onde são expostas algumas questões sobre o Teorema da Extensão que ficam por resolver nesta dissertação, bem com as referências onde se podem encontrar as suas respostas.

Capítulo 1
Noções Básicas

Neste capítulo vão ser apresentadas definições e resultados de álgebra e combinatória que serão essenciais para o entendimento das demonstrações do teorema principal. Pressupõe-se que o leitor domine os conceitos e resultados básicos da Teoria de Grupos, estes serão usados sem serem expostos ou justificados.

Anéis

Um anel é uma estrutura algébrica $(R, +, \cdot)$, onde R é um conjunto não vazio e $+$ e $\cdot$ são operações binárias em R que satisfazem:

1. $(R, +)$ é um grupo abeliano;
2. A operação $\cdot$ é associativa;
3. Verifica-se a propriedade distrubitiva: $\forall a, b, c \in R$:
   - $a \cdot (b + c) = a \cdot b + a \cdot c$;
   - $(a + b) \cdot c = a \cdot c + b \cdot c$.

Vamos assumir que um anel R tem sempre a identidade $1 \neq 0$ e denotaremos por R^* o conjunto dos elementos invertíveis (ou unidades) do anel, que correspondem aos elementos invertíveis de $(R, \cdot)$. Tal como no caso do grupos R^* é fechado para a operação (a multiplicação do anel).

Um corpo F é um anel tal que $(F \setminus \{0\}, \cdot)$ é um grupo abeliano. Um ideal esquerdo (resp. direito) I de R é um subgrupo aditivo de R, ou seja, $(I, +) \leq (R, +)$, tal que $ri \in I, \forall r \in R, i \in I$ (resp. $ir \in I$). Um ideal bilateral é um ideal que é simultaneamente esquerdo e direito. Se I é ideal, esquerdo, direito ou bilateral usamos a notação $I \leq R$ para o indicar. Considerando $I \leq R$ bilateral, podemos definir a relação de equivalência $\forall a, b \in R, a \sim b$ se e só se $a - b \in I$, assim $R/I = \{r + I : r \in R\}$, o conjunto das classes de equivalência desta relação, tem estrutura de anel e denomina-se o anel quociente de R por I.

Um ideal próprio é um ideal, $I \leq R$, tal que $I \neq R$. Por vezes para enfatizar a desigualdade usaremos a notação $I < R$. O ideal nulo é o subconjunto $\{0\}$ e um anel que não contém ideais próprios não nulos diz-se simples.

Um ideal esquerdo (ou direito) I diz-se principal ou cíclico se existe $x \in I$ tal que $I = Rx = \{rx \ : \ r \in R\}$ (resp. xR). A este elemento x chama-se gerador de Rx. O conjunto destes ideais de um dado anel R será denotado por $I_P(R) = \{Rx \mid x \in R\}$.

Um ideal minimal é um ideal, I, não nulo, tal que, $\nexists J \leq R : \{0\} < J < I$. Analogamente, um ideal maximal , I, é um ideal próprio tal que $\nexists J \leq R : I < J < R$.

Todo o ideal minimal é principal. Suponhamos que $I \leq R$ é um ideal minimal, então seja $x \in I$ não nulo temos $\{0\} < Rx \leq I$. Logo, $Rx = I$.

Módulos

Dado um anel $(R, +', \cdot')$, um grupo abeliano $(M, +)$ diz-se um R-módulo esquerdo se existir uma função, chamada de multiplicação escalar,

$$\begin{aligned} f \colon R \times M &\to M \\ (r, m) &\mapsto r \cdot m \end{aligned}$$

que satisfaça as seguintes condições, $\forall r, s \in R, \forall m, n \in M$:

1. $r \cdot (m + n) = r \cdot m + r \cdot n$;
2. $(r +' s) \cdot m = r \cdot m + s \cdot m$;
3. $(r \cdot' s) \cdot m = r \cdot (s \cdot m)$;
4. $1 \cdot m = m$.

Analogamente podemos definir módulo direito com a multiplicação escalar definida por $f(r, m) = m \cdot r$ e as quatro condição escritas de acordo com a nova multiplicação escalar. Se M tem estrutura de R-módulo esquerdo e direito e satisfaz a seguinte condição: $\forall r, s \in R, m \in M, (r \cdot m) \cdot s = r \cdot (m \cdot s)$, diz-se um R-bimódulo.

Um R-submódulo de um R-módulo esquerdo (resp. direito) M, N, é um subgrupo aditivo de M que é também um R-módulo esquerdo (resp. direito) para a restrição da multiplicação escalar de M a N. Um submódulo bilateral de um R-bimódulo M, N, é um subgrupo aditivo de M que é também um R-módulo esquerdo e direito para a restrição da multiplicação escalar de M a N.

Analogamente ao que foi definido atrás, um submódulo próprio, $N \leq M$, é um submódulo tal que $N \neq M$. Por vezes para enfatizar a desigualdade usaremos a notação $N < M$. O

submódulo nulo é o subconjunto $\{0\}$ e um módulo que não contém submódulos próprio não nulos diz-se simples.

Podemos também aqui definir um quociente. Seja $N \leq M$ um submódulo, definimos a relação de equivalência $m \sim m'$ se e só se $m - m' \in N$, assim $M/N = \{m + N | m \in M\}$, o conjunto das classes de equivalência desta relação, tem estrutura de módulo.

Um submódulo N diz-se cíclico se existe $x \in N$ tal que $N = Rx = \{rx : r \in R\}$. A um tal elemento x chama-se gerador. Um R-módulo esquerdo (resp. direito), M diz-se finitamente gerado se existe $S \subseteq M$ finito tal que

$$M = RS = \{\sum_{i=1}^{t} r_i s_i : t \in \mathbb{N}, r_i \in R, s_i \in S\}$$

(resp. $M = SR = \{\sum_{i=1}^{t} s_i r_i : t \in \mathbb{N}, r_i \in R, s_i \in S\}$). Um submódulo maximal, N, é um submódulo próprio tal que $\nexists K \leq M : N < K < M$ e um submódulo simples, N, é um submódulo tal que $\nexists K \leq M : \{0\} < K < N$. Analogamente ao caso dos ideais minimais, os submódulos simples são cíclicos.

Seja M um módulo e $\Gamma = \{M_i : i \in I\}$ uma família de submódulos de M, a soma de Γ é dada por

$$< \bigcup_{i \in I} M_i >= \{\sum_{i=1}^{n} m_i, n \in \mathbb{N}, m_i \in M_i\}$$

se $\Gamma = \emptyset$, então $< \bigcup_{i \in I} M_i >= \{0\}$. Geralmente denota-se a soma por $\sum_{i \in I} M_i$.

Seja M um módulo e N_1 um seu submódulo. Um submódulo N_2 diz-se complemento direto de N_1 em M se $N_1 + N_2 = M$ e $N_1 \cap N_2 = \{0\}$. Denotemos por $M = N_1 \oplus N_2$. Se tal acontece todo o elemento de M pode ser escrito de forma única como a soma de um elemento de N_1 com um elemento de N_2.

O socle de um módulo M, $soc(R)$, é a soma de todos os seus submódulos simples,

$$soc(M) = \sum_{N \leq M \text{ simples}} N.$$

Com $soc(M) = \{0\}$ se M não possui submódulos simples.

Enunciaremos em seguida um resultado que será necessário para a segunda demonstração do teorema principal (Teorema da Extensão). Este está demonstrado no anexo, no subcapítulo A.2, lema A.19.

Lema 1.1. *Seja M um módulo esquerdo finito tal que* $\mathrm{soc}(M)$ *é cíclico e não nulo. Então qualquer submódulo de* $\mathrm{soc}(M)$ *é cíclico.*

O radical de um módulo M é a interseção de todos os seus submódulos maximais,

$$rad(M) = \bigcap_{N \leq M \text{ maximal}} N.$$

Com $rad(R) = M$ se M não possui submódulos maximais.

O socle e o radical de um módulo M são ambos submódulos de M.

Se virmos R como R-módulo esquerdo (resp. direito) (basta considerar a multiplicação escalar como sendo a multiplicação do anel), então os seus submódulos são os seus ideais esquerdos (resp. direitos) e o seu socle será a soma dos seus ideais esquerdos (resp. direitos) minimais. Sempre que considerarmos R como R-módulo esquerdo, este será denotado por ${}_RR$. Se considerarmos R como R-módulo direito denotaremos por R_R. Assim, existem dois socles para R, o socle direito $soc(R_R)$ e o socle esquerdo $soc({}_RR)$. Estes dois socles e o radical de um anel R são ideais bilaterais de R. Definimos ainda comprimento de um R-módulo M. Seja

$$N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_n$$

uma cadeia de submódulos de M, o comprimento desta cadeia é o seu número de submódulos, ou seja n. O comprimento de um módulo M, $l(M)$, é o maior comprimento que uma cadeia de submódulos de M, onde cada submódulo está estritamente contido no seguinte, pode ter.

Exemplo 1.2. *Seja R um anel, $n \in \mathbb{N}$, o produto cartesiano de n cópias de R, R^n, é um R-bimódulo, considerando as multiplicações escalares esquerda e direita, $f_l : R \times R^n \to R^n$ e $f_r : R^n \times R \to R^n$, respetivamente, definidas por*

$$f_l(r, (x_1, \cdots, x_n)) = (rx_1, \cdots, rx_n) \text{ e } f_r((x_1, \cdots, x_n), r) = (x_1r, \cdots, x_nr)$$

ao qual se chama o módulo livre de dimensão n.

Homomorfismos

Sejam R e S anéis, a aplicação $f : R \to S$ diz-se um homomorfismo de anéis se

- f é um homomorfismo de grupos.
- $\forall x, y \in R, f(x \cdot y) = f(x) \cdot f(y)$.
- $f(1_R) = 1_S$.

O núcleo de f é o conjunto $\ker(f) = \{r \in R : f(r) = 0\}$ e a imagem o conjunto $\mathrm{Im}(f) = \{s \in S : \exists r \in R : f(r) = s\}$. Seja $I \leq R$, então $f(I) \leq \mathrm{Im}(f)$. Se $I \leq S$, então $f^{-1}(I) \leq R$, onde $f^{-1}(I)$ é a pré-imagem de I por f, em particular $\ker(f) \leq R$.

Sejam M e N R-módulos esquerdos, a aplicação $f : M \to N$ diz-se um homomorfismo de módulos, ou uma aplicação R-linear à esquerda, se

- f é um homomorfismo de grupos.
- $\forall m \in M, r \in R, f(r \cdot m) = r \cdot f(m)$

O núcleo e imagem deste homomorfismo define-se analogamente ao anterior e as mesmas propriedades verificam-se.

Um homomorfismo $f : R \to S$ de anéis (resp. módulos $f : M \to N$) é injetivo se $\ker(f) = \{0\}$, ao qual se chama monomorfismo, e é sobrejetivo se $\mathrm{Im}(f) = S$ (resp $\mathrm{Im}(f) = N$). Um isomorfismo de anéis (ou módulos) é um homomorfismo bijetivo, ou seja, injetivo e sobrejetivo. Um automorfismo de R (resp. M) é um isomorfismo $f : R \to R$ (resp. $f : M \to M$).

Os módulos sobre corpos chamam-se espaços vetoriais e são claramente bimódulos, pois os corpos são comutativos. Além disso, neste caso, os homomorfismos de módulos são as aplicações lineares.

Uma transformação monomial esquerda de R^n é uma automorfismo de módulos esquerdos da forma

$$\begin{aligned} T : R^n &\to R^n \\ (x_1, \cdots, x_n) &\mapsto (x_{\sigma(1)}u_1, \cdots, x_{\sigma(n)}u_n) \end{aligned}$$

onde, $u_1, \cdots, u_n$ são unidades de R e σ é uma permutação do grupo simétrico S_n. Analogamente se define transformação monomial direita, multiplicando as unidades do lado esquerdo.

Vamos verificar que T é de facto um automorfismo. Começamos por ver que é homomorfismo de módulos esquerdos. $\forall x = (x_1, \cdots, x_n), y = (y_1, \cdots, y_n) \in R^n$ e $\forall r \in R$,

$$\begin{aligned} T(x+y) &= ((x_{\sigma(1)} + y_{\sigma(1)})u_1, \cdots, (x_{\sigma(n)} + y_{\sigma(n)})u_n) \\ &= (x_{\sigma(1)}u_1, \cdots, x_{\sigma(n)}u_n) + (+y_{\sigma(1)}u_1, \cdots, y_{\sigma(n)}u_n) = T(x) + T(y) \end{aligned}$$

$$T(rx) = (rx_{\sigma(1)}u_1, \cdots, r(x_{\sigma(n)}u_n) = r(x_{\sigma(1)}u_1, \cdots, x_{\sigma(n)}u_n) = rT(x)$$

T é ainda isomorfismo, pois possui homomorfismo inverso $T^{-1} : R^n \to R^n$ definido por

$$T^{-1}(x_1, \cdots, x_n) = (x_{\sigma^{-1}(1)}u^{-1}_{\sigma^{-1}(1)}, \cdots, x_{\sigma^{-1}(n)}u^{-1}_{\sigma^{-1}(n)})$$

Uma transformação monomial sobre um corpo é sempre simultaneamente esquerda e direita porque os corpos são comutativos. Podemos facilmente verificar que a matriz que define esta aplicação (esquerda), Λ pode ser dada pelo produto $\Lambda = PD$. Onde D é uma matriz diagonal que na entrada D_{ii} contém u_i e P a matriz da permutação σ que permuta as entradas do vetor $(x_1, \cdots, x_n)$. Reciprocamente qualquer matriz desta forma define uma transformação monomial esquerda.

De seguida enunciaremos o teorema do isomorfismo na sua versão para anéis.

Teorema do Isomorfismo. *Sejam R e S anéis, $f : R \to S$ um homomorfismo de anéis, então*

$$\frac{R}{\ker(f)} \simeq Im(f)$$

como anéis.

De forma análoga temos o mesmo resultado para módulos. A demonstração pode ser encontrada em [3, Theorem 4.4.5].

Exemplo 1.3. *Seja R um anel e M um R-módulo direito, o conjunto dos homomorfismos direitos de M em R, é um R-módulo esquerdo. Denota-se por $Hom_R(M, R)$ e chama-se o dual do módulo M. A multiplicação escalar é dada por*

$$f\colon R \times Hom_R(M, R) \to Hom_R(M, R)$$
$$(r, f) \mapsto rf$$

onde rf é definida por $(rf)(m) = f(m)r, \forall m \in M$.

Anéis artinianos

Um módulo M diz-se artiniano se dada uma qualquer cadeia de submódulos de M

$$\cdots \leq N2 \leq N_1$$

existe $n \in \mathbb{N}$ tal que $\forall i \geq n, N_i = N_n$.

Um módulo M diz-se noetheriano se dada uma qualquer cadeia de submódulos de M

$$N_1 \leq N2 \leq \cdots$$

existe $n \in \mathbb{N}$ tal que $\forall i \geq n, N_i = N_n$.

Um anel diz-se artiniano á esquerda (resp. direita) se for artiniano como R-módulo esquerdo (resp. direito) e diz-se artiniano se o for á direita e à esquerda. Como vamos apenas lidar com anéis finitos, estes são obrigatoriamente artinianos e noetherianos.

Um módulo M diz-se semisimples se $soc(M) = M$. Assim, se virmos R como R-módulo esquerdo, este é semisimples à esquerda se $soc({}_RR) = R$.

Os dois teoremas seguintes são bastante importantes paras as demonstrações que se seguem, o primeiro é um resultado clássico sobre anéis semisimples e será importante para a demonstração do segundo que irá ter um papel importante nas duas demonstrações do teorema da extensão sobre anéis finitos. Como tal a demonstração do primeiro pode ser encontrada em [6, Theorem 3.5], enquanto que para o segundo é apresentada uma demonstração no anexo, no subcapítulo A.1.2 baseada em uma das demonstrações de [6, Theorem 20.9].

Teorema Wedderburn-Artin.

Seja R um anel semisimples á esquerda. Então $R \simeq M_{n_1}(D_1) \times \cdots \times M_{n_r}(D_r)$, para certos anéis de divisão $D_1, \cdots, D_r$ e inteiros positivos $n_1, \cdots, n_r$.

Teorema de Bass.

Seja R um anel artiniano, $a \in R$ e $\mathcal{L}$ um ideal esquerdo de R. Se $Ra + \mathcal{L} = R$, então $a + \mathcal{L}$ possui um elemento de R^*, ou seja, um elemento invertível.

Injetividade

Um R-módulo esquerdo M diz-se injetivo á esquerda se para qualquer homomorfismo injetivo $f : A \to B$ de R-módulos esquerdos e para qualquer homomorfismo de módulos $g : A \to M$, existe um homomorfismo de módulos esquerdos $\varphi : B \to M$, tal que o diagrama seguinte comuta

$$\begin{array}{ccccc} \{0\} & \longrightarrow & A & \xhookrightarrow{f} & B \\ & & \downarrow{\scriptstyle g} & \swarrow{\scriptstyle \varphi} & \\ & & M & & \end{array}$$

ou seja, $g = \varphi \circ f$. Analogamente se pode definir injetividade à direita.

As próximas definições e o próximo lema são aqui apresentados porque vão ser necessário para demonstrar uma propriedade dos anéis de Frobenius relacionada com a injetividade.

Seja R um anel e $X \subseteq R$ um subconjunto, o anulador á esquerda de X por R é o ideal

esquerdo

$$l.ann_R(X) = \{r \in R | rx = 0, \forall x \in X\}$$

O anulador à direita de X por R é o ideal direito

$$r.ann_R(X) = \{r \in R | xr = 0, \forall x \in X\}$$

O próximo lema será então necessário para a demonstração do lema 3.7 e encontra-se demonstrado no subcapítulo A.2 do anexo, lema A.20.

Lema 1.4. *Seja R um anel injetivo à esquerda, então para qualquer $a \in R$ temos*

$$r.ann_R(l.ann_R(a)) = aR$$

Códigos Lineares

Seja F um corpo finito com q elementos, um (n, k)-código linear C sobre F é um subespaço vetorial de dimensão k do espaço vetorial F^n.

Uma matriz geradora de um (n, k)-código C é qualquer matriz X cujas linhas formem uma base de C. Esta será, portanto, uma matriz $k \times n$. Ou seja, se $X_1, \cdots, X_k$ forem as linhas de X, $\forall c \in C, \exists u \in F^k : c = uX$.

Analogamente podemos definir códigos lineares sobre anéis finitos. Seja R um anel finito e R^n o módulo livre de dimensão n. Um código linear esquerdo de comprimento n, C, sobre R é um submódulo esquerdo de R^n ($C \leqslant R^n$). Analogamente se define códigos lineares direitos de comprimento n.

Ao longo do documento um código linear sobre um corpo finito, C, será simplesmente um (n, k)-código C, um código linear esquerdo sobre um anel R, $C \leq R^n$, será um R-código C esquerdo de comprimento n e analogamente um código linear direito sobre um anel R, $C \leq R^n$, será um R-código C direito de comprimento n.

Funções peso

Seja R um anel finito, uma função peso (ou apenas peso), wt, de R^n é qualquer função do forma

$$\begin{aligned} wt : R^n &\to \mathbb{R} \\ x &\mapsto \sum_{r \in R} a_r n_r(x) \end{aligned}$$

onde, para $x = (x_1, x_2, \cdots, x_n) \in R^n$ e $\forall r \in R$, $n_r(x) = |\{i : x_i = r\}|$, $a_r \in \mathbb{R}$ e $a_0 = 0$.

Note-se que, para qualquer peso wt e sendo $0 = (0, \cdots, 0)$ o vetor nulo de R^n, temos $n_r(0) = 0, \forall r \in R \setminus \{0\}$ e $a_0 = 0$, logo $wt(0) = 0$.

O peso de Hamming é o peso onde $a_r = 1, \forall r \in R \setminus \{0\}$, denota-se por w_H.

Um peso wt do anel finito R diz-se homogéneo se satisfaz as seguintes propriedades:

1. Se $Rx = Ry$, então $wt(x) = wt(y), \forall x, y \in R$.

2. Existe um número real $c \geq 0$ tal que

$$\sum_{y \in Rx} wt(y) = c|Rx|, \quad \forall x \in R \setminus \{0\}.$$

Conjuntos parcialmente ordenados

Um conjunto parcialmente ordenado (c.p.o.) é um par $(P, \leq)$, onde P é um conjunto e $\leq$ é uma relação binária de ordem parcial.

Um intervalo de um c.p.o, $(P, \leq)$ é um subconjunto da forma

$$[x, y] := \{z \in P : x \leq z \wedge z \leq y\}$$

onde $x, y \in P$ são elementos tais que $x \leq y$.

O mínimo de um c.p.o. P é um elemento $i \in P : \forall a \in P, i \leq a$. O máximo de um c.p.o. P é um elemento $s \in P : \forall a \in P, a \leq s$. Por convenção denota-se o elemento mínimo de um c.p.o., caso exista, por 0 e o máximo por 1.

Seja P um c.p.o, $S \subseteq P$ um subconjunto de elementos do c.p.o., o supremo de S é o menor elemento de P, a, tal que $\forall s \in S, s \leq a$. O ínfimo de S é o maior elemento de P, a, tal que $\forall s \in S, a \leq s$.

Assim, seja P um c.p.o. com elemento mínimo 0, um átomo de P é um elemento $a \in P : \nexists b \in P : 0 < b < a$. Onde $<$ representa a ordem parcial estrita associada a $\leq$. Analogamente, seja P um c.p.o. com elemento máximo 1, um coátomo de P é um elemento $a \in P : \nexists b \in P : a < b < 1$.

Um c.p.o diz-se atomistico se todos os seus elementos forem supremos de conjuntos de átomos.

Um reticulado é um c.p.o P tal que qualquer seu conjunto de dois elementos $\{a, b\}$ possui infimo, denotando-se por $a \vee b$, e supremo, que se denota por $a \wedge b$. Sejam $a, b \in L$, onde L é um reticulado, b é uma cobertura de a se $a \leq b$ e se $\exists c \in L : a \leq c \leq b$, então $a = c$ ou $b = c$.

Se L é um reticulado onde se verifica a seguinte condição: Sejam $a, b \in L$ tais que a e b são coberturas de $a \wedge b$, então $a \vee b$ é cobertura de a e b. Diz-se que L é um reticulado semimodular.

Um reticulado diz-se modular se $\forall a, b, c \in L, a \leq b$ implica $a \vee (b \wedge c) = b \wedge (a \vee c)$.

O conjunto dos submódulos de um módulo esquerdo (ou direito), M, que se denota por $L(M)$, é um reticulado modular, onde o ínfimo de dois submódulos N_1 e N_2 é o submódulo $N_1 \cap N_2$ e o supremo o submódulo $N_1 + N_2$. Os átomos são os submódulos simples e os coatomos os maximais, além disso $L(M)$ ser atomistico significa que M é semisimples.

Temos ainda o seguinte resultado que está demonstrado no subcapítulo A.2 do anexo (lema A.21):

Lema 1.5. *Seja L um reticulado, se L é modular, então é semimodular.*

Assim, podemos concluir que o conjunto dos submódulos de um módulo esquerdo (ou direito) é também um reticulado semimodular. Facto que vai ser usado mais à frente na demonstração de uma propriedade dos reticulados atomisticos.

Caracteres

Seja G um grupo abeliano, um caractere complexo, ou caractere, de G é um homomorfismo de grupos $\pi : G \to \mathbb{C}^*$. Onde $\mathbb{C}^*$ é o grupo das unidades dos números complexos. O grupo dos caracteres do grupo G, denota-se por $\widehat{G}$, o seu elemento identidade é o caractere trivial, ou seja, o homomorfismo de G em $\mathbb{C}^*$ que envia todos os elementos de G em 1. A operação é dada por

$$\begin{aligned} \cdot : \widehat{G} \times \widehat{G} &\to \widehat{G} \\ (\pi, \chi) &\mapsto \pi \cdot \chi \end{aligned}$$

onde $\pi \cdot \chi$ é definida por $(\pi \cdot \chi)(g) = \pi(g)\chi(g), \forall g \in G$.

Seja R um anel e M um R-módulo esquerdo, o R-módulo de caracteres $\widehat{M}$ associado a M é o grupo dos caracteres de M, visto como grupo abeliano aditivo $(M, +)$, junto com a multiplicação escalar dada por

$$\begin{aligned} \cdot : R \times \widehat{M} &\to \widehat{M} \\ (r, \pi) &\mapsto \pi^r \end{aligned}$$

onde $\pi^r(x) = \pi(rx), \forall x \in M$. Ou seja, $\widehat{M}$ é um R-módulo direito.

Seja R um anel finito, um caractere χ de R é um caractere gerador direito se a aplicação $\phi : R \to \widehat{R}$, dada por $\phi(r) = \chi^r$ é um isomorfismo de R-módulos direitos.

Temos ainda demonstrado no subcapítulo A.4 do anexo, lema A.22, o seguinte resultado que será importante para um resultado intermédio necessário á 3ª demonstração do teorema principal.

Lema 1.6. *Seja G um grupo abeliano e $\widehat{G}$ o seu grupo de caracteres, então $|G| = \left|\widehat{G}\right|$.*

Os dois seguintes resultados serão também importantes para a última demonstração do teorema principal e é possível encontrar a demonstração do primeiro em [10, Lemma 76] e a demonstração do segundo em [13, Corolary pág. 63].

Proposição 1.7. *Seja G um grupo abeliano finito e considere-se o conjunto das funções de G com valores em $\mathbb{C}$, $\mathcal{F}(G, \mathbb{C})$. Este conjunto é um grupo abeliano para a soma de funções, onde o elemento neutro é dado pela função que envia todos os elementos de G em 0. Se considerarmos a multiplicação escalar,*

$$f \colon \mathbb{C} \times \mathcal{F}(G, \mathbb{C}) \to \mathcal{F}(G, \mathbb{C})$$
$$(z, f) \mapsto zf$$

onde zf é definida por $(zf)(x) = z \cdot f(x), \forall x \in G$, temos que $\mathcal{F}(G, \mathbb{C})$ é um espaço vetorial sobre o corpo dos complexos, $\mathbb{C}$

Claramente o grupo dos caracteres complexos de G é um subconjunto de $\mathcal{F}(G, \mathbb{C})$. Seja $\{\pi_1, \cdots, \pi_n\}$ um conjunto finito de caracteres de G, este diz-se independente se $\pi_1, \cdots, \pi_n$ forem linearmente independentes como elementos do espaço vetorial $\mathcal{F}(G, \mathbb{C})$.

Qualquer conjunto finito de caracteres de G é independente.

Proposição 1.8. *Seja G um grupo abeliano finito e $\widehat{G}$ o seu grupo de caracteres, então:*

$$\sum_{\pi \in \widehat{G}} \pi(x) = \begin{cases} |G|, & se \quad x = 0 \\ 0, & se \quad x \neq 0 \end{cases}$$

Capítulo 2
Teorema da Extensão de MacWilliams

Neste capítulo irá ser demonstrada a versão do teorema da extensão de MacWilliams para corpos finitos de forma análoga ao que é feito em [1]. De seguida é apresentado a versão do teorema que irá ser considerada,

Teorema de MacWilliams. *Sejam C e D dois (n,k)-códigos lineares sobre um corpo F, e $\psi : C \to D$, um isomorfismo que preserva o peso de Hamming. Então existe uma transformação monomial $\varphi : F^n \to F^n$ tal que $\varphi|_C = \psi$.*

Para demonstrar o teorema vamos provar que se X é uma matriz geradora de C e Y é uma matriz geradora de D então Y pode ser obtida de X permutando as suas colunas e multiplicando cada uma delas por um escalar adequado.

Tendo em conta que diferentes autores optam por diferentes definições de matriz de uma aplicação linear, vamos expor a definição que irá ser adotada.

Definição 2.1. *Seja $f : F^k \to F^n$, uma aplicação linear entre dois espaços vetoriais sobre um corpo F. Considere-se a base canónica de F^k, $B_k = (e_1, \cdots, e_k)$ e a base canónica de F^n, $B_n = (e_1, \cdots, e_n)$, então a matriz de f relativamente às bases canónicas de F^k e F^n é a matriz cujas linhas são os vetores $f(e_1), \cdots, f(e_n)$, ou seja, é a matriz $M = \begin{pmatrix} f(e_1) \\ \vdots \\ f(e_n) \end{pmatrix}$. Assim é possível definir a aplicação f da seguinte forma:*

$$\begin{aligned} f : F^k &\to F^n \\ v &\mapsto vM \end{aligned}$$

O objetivo deste subcapítulo é demonstrar que a matriz de ortogonalidade, definida mais abaixo é invertível em $\mathbb{Q}$. Este facto irá ser crucial para a demonstração do teorema principal.

Notação. *Denota-se por $\mu(n)$ o número de subespaços de dimensão 1 do espaço vetorial F^n, por $L_1, \ldots, L_{\mu(n)}$ os $\mu(n)$ subespaços distintos de dimensão 1 e por $u_1, \cdots, u_{\mu(n)}$ os gerados de cada um destes subespaços.*

Proposição 2.2. *Seja F um corpo com q elementos, o número de subespaços vetoriais de dimensão 1 de F^n é*

$$\mu(n) = \frac{q^n - 1}{q - 1}.$$

Demonstração. Comecemos por notar que como cada L_i tem dimensão 1 é gerado por um único elemento. Assim, seja $u \in L_i$ gerador, os restantes elementos do subespaço são os q múltiplos possíveis de u, ou seja os elementos $0, u, \ldots, (q-1)u$. Além disso F^n tem $q^n - 1$ elementos não nulos. Logo o número de subespaços é dado por:

$$\mu(n) = \frac{q^n - 1}{q - 1}.$$

□

Definição 2.3. *Dois subespaços, L_i e L_j, dizem-se ortogonais se $\forall u \in L_i$, $\forall u' \in L_j$, $u \cdot u' = 0$, onde $\cdot$ é o produto interno usual de F^n. Denotamos por $L_i \perp L_j$.*

Proposição 2.4. *Sejam L_i e L_j dois subespaços de dimensão 1 e $u \in L_i, u' \in L_j$ não nulos, tais que $u \cdot u' = 0$ então $L_i \perp L_j$. Assim para ver se dois subespaços são ortogonais basta pegar em quaisquer dois elementos não nulos, um elemento de cada subespaço, e verificar se o seu produto interno dá 0.*

Demonstração. A função do produto interno é bilinear como é sabido e todos os elementos de L_i e L_j são da forma λu_i e μu_j, respetivamente, para algum $\lambda, \mu \in F$.

Assim, sejam $u \in L_i$ e $u' \in L_j$ não nulos tais que $u \cdot u' = 0$ temos

$$u \cdot u' = (\lambda u_i) \cdot (\mu u_j) = \lambda\mu(u_i \cdot u_j) = 0 \Rightarrow u_i \cdot u_j = 0$$

para alguns $\lambda, \mu \in F$. Como o produto dos geradores é nulo, então $\forall \lambda, \mu \in F$ temos $\lambda u_i \cdot \mu u_j = 0$. Ou seja $L_i \perp L_j$.

□

Definição 2.5. *Seja V um espaço vetorial sobre um corpo F, o peso de Hamming de um seu subespaço de dimensão 1, L_i é o peso de Hamming de um seu gerador. Ou seja, $wt(L_i) := wt(u_i)$, com $u_i \in L_i$, gerador.*

Notação. *Chamamos "Matriz de Ortogonalidade"dos subespaços de dimensão 1 de* F^n *à matriz* $T = (t_{ij})$ *de* $\mu(n) \times \mu(n)$ *de 0's e 1's onde:*

$$t_{ij} = \begin{cases} 0, & se \quad L_i \perp L_j \\ 1, & caso\ contrário. \end{cases}$$

Teorema 2.6. *A matriz* T *é invertível sobre o corpo dos números racionais,* $\mathbb{Q}$.

Para conseguirmos provar o resultado anterior é necessário provar primeiro a seguinte proposição:

Proposição 2.7. *As seguintes afirmações são verdadeiras para um corpo* F *com* q *elementos,* $n \geq 2$ *e* $1 \leq i, j \leq \mu(n)$ *com* $i \neq j$*:*

1. *O número de subespaços de dimensão 1 de* F^n *que são ortogonais ao subespaço* L_i *é* $\mu(n-1)$*, ou seja,* $|\{L_j | L_j \perp L_i\}| = \mu(n-1)$.

2. *O número de subespaços de dimensão 1 de* F^n *que são simultaneamente ortogonais ao subespaço* L_i *e a* L_j *é* $\mu(n-2)$*. Ou seja,* $|\{L_k | L_k \perp L_i \wedge L_k \perp L_j\}| = \mu(n-2)$.

3. *Se virmos as linhas de* T *como vetores de* F^n*, a soma das linhas de* T *é o vetor constante,* $x = (x_1, \ldots, x_{\mu(n)})$*, onde* $x_i = q^{n-1}$ *para todo o* $i \in \{1, \ldots, \mu(n)\}$.

4. *Se virmos as linhas de* T *como vetores de* F^n*, a soma das linhas de* T *que têm entrada 0 na coluna* j *é o vetor,* $y(j) = (y_1, \ldots, y_{\mu(n)})$*, onde* $y_j = 0$ *e* $y_i = q^{n-2}$ *para todo o* $i \neq j$.

Demonstração.

1. Comecemos por considerar a seguinte aplicação, para um dado $u_i \in L_i$ não nulo:

$$\begin{aligned} f \colon F^n &\to F \\ u &\mapsto u \cdot u_i \end{aligned}$$

Como o produto interno é uma aplicação bilinear, se fixarmos uma das variáveis passamos a ter uma aplicação linear, portanto f é de facto uma aplicação linear.

Notemos que $\ker(f) = \{u \in F^n | u \cdot u_i = 0\} \Leftrightarrow \ker(f) = \{u \in F^n | u \in L_j : L_j \perp L_i\}$. Assim $\{L_j | L_j \perp L_i\}$ é o conjunto dos subespaços de dimensão 1 de $\ker(f)$. Logo falta apenas ver qual é a dimensão de $\ker(f)$.

A matriz de f é o vetor u_i, como este é não nulo temos que $\text{car}(M_f) = 1$, onde M_f é a matriz da aplicação linear f. Logo $dim(\text{Im}(f))$ =$\text{car}(M_f) = 1$. Assim, como

$dim(F^n) = dim(\ker(f)) + dim(\mathrm{Im}(f))$, temos $dim(\ker(f)) = n - dim(\mathrm{Im}(f)) = n - 1$ e portanto o número de subespaços de dimensão 1 de $\ker(f)$ é $\mu(n-1)$. Ou seja

$$|\{L_j | L_j \perp L_i\}| = \mu(n-1).$$

2.

Comecemos por considerar a seguinte aplicação, para um dado $u_i \in L_i$ e $u_j \in L_j$:

$$\begin{aligned} f\colon F^n &\to F^2 \\ u &\mapsto (u \cdot u_i, u \cdot u_j) \end{aligned}$$

Da mesma forma que anteriormente, como o produto interno é uma aplicação bilinear, a linearidade é preservada em cada componente da função f e como tal a aplicação é linear.

Temos $\ker(f) = \{u \in F^n | (u \cdot u_i, u \cdot u_j) = (0,0)\}$ que é equivalente a $\ker(f) = \{u \in F^n | u \in L_k : L_k \perp L_i \wedge L_k \perp L_j\}$. Assim $\{L_k | L_k \perp L_i \wedge L_k \perp L_j\}$ é o conjunto dos subespaços de dimensão 1 de $\ker(f)$. Logo falta apenas ver qual é a dimensão de $\ker(f)$.

Novamente temos que $dim(F^n) = dim(\ker(f)) + dim(\mathrm{Im}(f))$. A matriz de f é dada por $M_f = (u_i, u_j)$, como $i \neq j$, as duas colunas u_i e u_j são linearmente independentes e por isso $\mathrm{car}(M_f) = 2$. Logo $dim(\mathrm{Im}(f)) = 2$ e $dim(\ker(f)) = n - dim(\mathrm{Im}(f)) = n - 2$. Portanto o número de subespaços de dimensão 1 de $\ker(f)$ é $\mu(n-2)$. Ou seja

$$|\{L_j | L_j \perp L_i\}| = \mu(n-2)$$

3.

Seja x o vetor que corresponde á soma de todas as linhas da matriz T e x_i as suas coordenadas para $i \in \{1, \ldots, \mu(n)\}$. Então:

$$\begin{aligned} x_i &= |\{L_j | L_j \not\perp L_i\}| = |\{L_j : 1 \leq j \leq \mu(n)\} \setminus \{L_j | L_j \perp L_i\}| \\ &= |\{L_j : 1 \leq j \leq \mu(n)\}| - |\{L_j | L_j \perp L_i\}| = \mu(n) - \mu(n-1) \qquad \text{(por 1)} \\ &= \frac{q^n - 1 - q^{n-1} + 1}{q-1} = q^{n-1} \end{aligned}$$

4.

Seja $y(j)$ o vetor que corresponde á soma de todas as linhas da matriz T que têm entrada

0 na coluna j e y_i as suas coordenadas para $i \in \{1, \ldots, \mu(n)\}$. Então, $y_j = 0$ e para $i \neq j$:

$$\begin{aligned} y_i &= |\{L_k | L_k \not\perp L_i \wedge L_k \perp L_j\}| \\ &= |\{L_k | L_k \perp L_j\} \setminus \{L_k | L_k \perp L_i \wedge L_k \perp L_j\}| \\ &= |\{L_k | L_k \perp L_j\}| - |\{L_k | L_k \perp L_i \wedge L_k \perp L_j\}| \\ &= \mu(n-1) - \mu(n-2) \\ &= \frac{q^{n-1} - 1 - q^{n-2} + 1}{q-1} = q^{n-2} \qquad \text{(por 1 e 2)} \end{aligned}$$

□

Demonstração Teorema 2.6.
Notemos que podemos escrever os vertores $\{e_1, \ldots, e_{\mu(n)}\}$ da base canónica de $\mathbb{Q}^{\mu(n)}$ como combinação linear das linhas de T:

$$e_j = \frac{x}{q^{n-1}} - \frac{y(j)}{q^{n-2}}.$$

Podemos então concluir que o espaço vetorial gerado pelas linhas de T é $\mathbb{Q}^{\mu(n)}$ e portanto a característica de T é $\mu(n)$ (porque $\mathbb{Q}^{\mu(n)}$ tem dimensão $\mu(n)$, logo como T tem $\mu(n)$ linhas que geram o espaço, então essas linhas têm de ser linearmente independentes).
Logo T é invertível sobre $\mathbb{Q}$. □

Podemos agora demonstrar o teorema principal, para isso suponhamos que temos dois (n, k)-códigos, C e D, tais que existe um isomorfismo $\psi : C \to D$ que preserva o peso de Hamming.

Notação 2.8. *Seja X uma matriz geradora de C, $(k \times n)$ considere-se o isomorfismo $f : F^k \to C$ definido por $f(u) = uX$. f é um isomorfismo pois por definição de matriz geradora é sobrejetivo e como as linhas de X são linearmente independentes é injetivo.*

Nota 2.9. *Observemos que, por definição, X é a matriz de f relativamente á base canónica de F^k e de F^n. Além disso, como $f(Fu) = Ff(u), \forall u \in F^k$, então $f(L_i) = f(Fu_i) = Ff(u_i) =< f(u_i) >$, ou seja, f envia os subespaços unidimensionais de F^k em subespaços unidimensionais de C.*

Notação 2.10. *Considere-se $g : F^k \to D$ definida como $g = \psi \circ f$. E, por último, sejam $c_1, \cdots, c_n$ as colunas de X, denotemos por r o vetor coluna $r = (r_1, \ldots, r_{\mu(k)})^t$, com entradas:*

$$r_i = |\{j : c_j \neq 0 \wedge c_j^t \in L_i\}|$$

Nota 2.11.

1. *g é um isomorfismo porque é a composição de dois isomorfismos.*
2. *Se Y for a matriz do isomorfismo g relativamente á base canónica de F^k e de F^n, então $g(u) = uY, \forall u \in F^k$, logo, como g é isomorfismo, é sobrejetiva, e por isso todos os elementos de D se escrevem da forma uY. Ou seja, Y é uma matriz geradora de D.*
3. *Notemos que r nos indica a quantidade de colunas não nulas de X, pois podemos escrever o número de colunas nulas de X como $n - \sum_{i=1}^{\mu(k)} r_i$.*

Lema 2.12. *Seja T a matriz de ortogonalidade dos subespaços de dimensão 1 de F^k, podemos interpretar Tr como o vetor coluna da lista dos pesos de Hamming dos subespaços unidimensionais de C. Ou seja $(Tr)_i = w_H(f[L_i])$.*

Demonstração. Considere-se então a matriz de ortogonalidade mencionada no enunciado e o vetor r já definido. Temos:

$$Tr = \begin{pmatrix} t_{11} & t_{12} & \cdots & t_{1\mu(k)} \\ t_{21} & t_{22} & \cdots & t_{2\mu(k)} \\ \vdots & \vdots & \ddots & \vdots \\ t_{\mu(k)1} & t_{\mu(k)2} & \cdots & t_{\mu(k)\mu(k)} \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_{\mu(k)} \end{pmatrix} = \begin{pmatrix} \sum_{i=1}^{\mu(k)} t_{1i} r_i \\ \sum_{i=1}^{\mu(k)} t_{2i} r_i \\ \vdots \\ \sum_{i=1}^{\mu(k)} t_{\mu(k)i} r_i \end{pmatrix}$$

Sejam $c_1, \cdots, c_n$ as colunas de X, então

$$\begin{aligned} (Tr)_i &= \sum_{j=1}^{\mu(k)} t_{ij} r_j = \sum_{j:L_j \not\perp L_i} 1 \cdot r_j + \sum_{j:L_j \perp L_i} 0 \cdot r_j = \sum_{j:L_j \not\perp L_i} r_j \\ &= \sum_{j:L_j \not\perp L_i} |\{c_k : c_k \neq 0 \wedge c_k^t \in L_j\}| = |\{c_k : c_k \neq 0 \wedge c_k^t \in L_j \wedge u_i \cdot c_k^t \neq 0\}| \\ &= |\{c_k : c_k \neq 0 \wedge u_i \cdot c_k^t \neq 0\}| = w_H(u_i X) \\ &= w_H(f(u_i)) = w_H(f[L_i]) \end{aligned}$$

□

Nota 2.13. *Se considerarmos o vetor r' definido da mesma forma que o vetor r, mas considerando agora as colunas em Y, temos $(Tr')_i = w_H(g[L_i])$. A demonstração é idêntica à do caso anterior, bastando substituir r por r' e X por Y até ao penúltimo passo onde teremos então:*

$$(Tr)_i = w_H(u_i Y) = w_H(g(u_i)) = w_H(g[L_i])$$

Teorema 2.14. *Existe uma matriz $\Lambda = DP$, onde D é uma matriz diagonal e P uma matriz de permutação, tal que, $X\Lambda = Y$.*

Demonstração. Começamos por mostrar que $(Tr)_i = (Tr')_i$, $\forall i \in \{1, \cdots, \mu(k)\}$

$$(Tr')_i = w_H(g[L_i]) = w_H(g(u_i)) = w_H(\psi \circ f(u_i)) = w_H(f(u_i)) = w_H(f[L_i]) = (Tr)_i$$

Logo $Tr = Tr'$. Mas como T tem matriz inversa em $\mathbb{Q}$, aplicando a matriz inversa em ambos os lados da equação obtemos, $r = r'$. Como r especifica o número de colunas não nulas, podemos concluir que X e Y têm o mesmo número de colunas não nulas. Além disso, o número de colunas de X que pertencem a um dado subespaço unidimensional é o mesmo que o número de colunas de Y que pertencem ao mesmo espaço. Mas, como os subespaços unidimensionais são gerados por um único elemento, ou seja todos os elementos de um dado L_i são múltiplos escalares de um seu gerador, temos que as colunas de Y que pertencem a um dado L_i são múltiplos escalares das colunas de X que pertencem a esse mesmo subespaço. Como r e r' não especificam a ordem das colunas, nenhuma informação mais podemos retirar da igualdade. Concluímos assim que a matriz Y pode ser obtida da matriz X reordenando as colunas da última e multiplicando cada uma destas por um escalar adequado, escalar este que será uma unidade, pois F é corpo.
Em linguagem matemática temos então:

$$\begin{aligned} Y &= X(DP) && \text{(D matriz diagonal } n \times n \text{ e P matriz de permutação } n \times n) \\ &= X\Lambda && (\Lambda = DP) \end{aligned}$$

□

Assim esta matriz $\Lambda = DP = PD$ (pois estamos a trabalhar em corpos) define uma transformação monomial $\varphi : F^n \to F^n$, como visto no capítulo 1 na página 8. Falta apenas verificar que quando restrita a C é igual á isometria de que partimos.

Seja então $c \in C$, $\varphi(c) = c\Lambda$, mas por definição de matriz geradora temos, $\varphi(c) = uX\Lambda$, para algum $u \in F^k$. Vamos ter então

$$\varphi(c) = uX\Lambda = uY = g(u) = \psi(f(u)) = \psi(c)$$

E temos, assim, o pretendido.

Capítulo 3
Anéis de Frobenius

Neste capítulo além da definição de anel de Frobenius são apresentadas algumas das suas propriedades. Propriedades estas responsáveis pelo facto de a versão do Teorema da Extensão para códigos sobre anéis finitos ser válida apenas nestes anéis.

Teorema 3.1. *Seja R um anel as seguintes condições são equivalentes:*

1. *R é Noetheriano à direita e injetivo como R-módulo à direita.*
2. *R é Noetheriano à esquerda e injetivo como R-módulo à direita.*
3. *R é Noetheriano à direita e satisfaz as seguintes condições:*
   (a) *$r.ann_R(l.ann_R(A)) = A, \forall A \leq R$ direito.*
   (b) *$l.ann_R(r.ann_R(A)) = A, \forall A \leq R$ esquerdo.*
4. *R é artiniano dos dois lados e satisfaz 3a e 3b.*

Demonstração. Ver [7, Theorem 15.1]. □

Definição 3.2. *Um anel que satisfaz alguma das condições do teorema 3.1 diz-se um anel Quase Frobenius, QF.*

Nota 3.3. *Os anéis QF podem ser também definidos como anéis que são simultaneamente noetherianos á esquerda (resp. direita) e injetivos á esquerda ([7, pág. 409]).*

Teorema 3.4. *Seja R um anel artiniano, então as seguintes condições são equivalentes, para $\overline{R} = R/rad(R)$:*

1. *R é QF e $soc({}_RR) \simeq {}_R\overline{R}$.*
2. *R é QF e $soc(R_R) \simeq \overline{R}_R$.*
3. *$soc({}_RR) \simeq {}_R\overline{R}$ e $soc(R_R) \simeq \overline{R}_R$.*

Demonstração. Ver [7, Theorem 16.14]. □

Definição 3.5. *Um anel que satisfaz alguma das condições do teorema 3.4 diz-se um anel de Frobenius.*

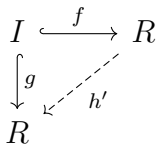
Corolário 3.6. *Seja R um anel de Frobenius, então os seus socles á esquerda e à direita ($soc({}_RR)$ e $soc(R_R)$) são principais.*

Demonstração. Por definição temos $soc({}_RR) \simeq {}_R\overline{R}$ e $soc(R_R) \simeq \overline{R}_R$, mas ${}_R\overline{R}$ e $\overline{R}_R$ são R-módulos cíclicos, gerados por $1 + rad$. □

A seguinte propriedade dos anéis de Frobenius finitos vai ser necessária na 2ª demonstração do teorema principal.

Lema 3.7. *Seja R um anel finito de Frobenius, $I \leq R$ um ideal esquerdo e $f, g : I \to R$ dois homomorfismos injetivos de módulos esquerdos. Então, existe um automorfismo de módulos esquerdos $h : R \to R$ tal que $f = h \circ g$.*

Demonstração. Como R é de Frobenius, é injetivo como R-módulo á esquerda. Pela definição de injetividade e nas condições do enunciado temos que existe um homomorfismo $h' : R \to R$ tal que $h' \circ f = g$.



Como h' é um homomorfismo de R-módulos á esquerda, vamos ter $h'(r) = rh'(1)$, $\forall r \in R$. Ou seja, h' fica determinado pelo valor de $a = h'(1) \in R$.

Mas então, $g(x) = h'(f(x)) = f(x)a$ e como g é uma função injetiva,

$$\{0\} = \ker(g) = \{x \in I : f(x)a = 0\}$$

Assim, se $y \in Im(f) \cap l.ann_R(a)$, então $\exists x \in I : y = f(x) \wedge f(x)a = 0$, logo $x \in \ker(g)$, ou seja, $x = 0$ e $Im(f) \cap l.ann_R(a) = \{0\}$.

Podemos então, tomando $B = Im(f) \oplus l.ann_R(a)$, considerar o homomorfismo

$$\pi : B \to R$$
$$f(x) + y \mapsto y$$

que está bem definido, pois por estarmos a trabalhar com uma soma direta os elementos de B escrevem-se de forma única como soma de elementos de $Im(f)$ e de $l.ann_R(a)$.

Novamente pela injetividade de R e considerando a inclusão $i : B \to R$, temos que existe $\pi' : R \to R$ tal que $\pi = \pi' \circ i$.

Assim, dado $y \in l.ann_R(a)$ qualquer, $y = \pi(y) = \pi'(y) = y\pi'(1)$. Da mesma forma, dado $x \in I, 0 = \pi(f(x)) = \pi'(f(x)) = f(x)\pi'(1)$.

Ou seja, denotando $s = \pi'(1)$ e fazendo uso do lema 1.4, temos que

$$y = ys \Leftrightarrow y(1-s) = 0 \Rightarrow 1 - s \in r.ann_R(l.ann_R(a)) = aR.$$

No entanto, $s = \pi'(1) \in r.ann_R(Im(f))$. Logo

$$R = aR + r.ann_R(Im(f))$$

Assim, pelo Teorema de Bass (nota A.17), temos que $\exists u \in R^* : u \in a + r.ann_R(Im(f))$.

Finalmente considere-se o homomorfismo de R-módulos á esquerda $h : R \to R$, definido por $h(x) = xu$, que é claramente um automorfismo, pois possui homomorfismo inverso $h^{-1} : R \to R$, dado por $h^{-1}(x) = xu^{-1}$. Vamos então ter $h(f(x)) = f(x)a + f(x)b$, com $b \in r.ann_R(Im(f))$. Logo ficamos com $h(f(x)) = f(x)a = g(x)$ e temos o automorfismo pretendido. □

Nota 3.8. *Seja R um anel e $h : R \to R$ um automorfismo de R-módulos esquerdos, então $h(r) = ru$ para alguma unidade u de R.*

O próximo teorema dá-nos uma propriedade dos anéis de Frobenius que será fundamental para podermos concluir que qualquer anel de Frobenius possui um caractere gerador direito. Facto este que será fundamental par a 3ª demonstração do teorema principal.

Teorema 3.9. *Seja R um anel finito, $\widehat{R}_R$ o R-módulo de caracteres associado a R_R e ${}_R\widehat{R}$ o R-módulo de caracteres associado a ${}_RR$. Então as seguintes condições são equivalentes:*

- *R é anel de Frobenius.*
- *Como R-módulos à esquerda, $\widehat{R}_R \simeq {}_RR$.*
- *Como R-módulos à direita, ${}_R\widehat{R} \simeq R_R$.*

Demonstração. Ver [15, Theorem 3.10]. □

Corolário 3.10. *Seja R um anel finito, R é um anel de Frobenius se e só se admite um caractere gerador direito.*

Demonstração. Suponhamos que R admite um caractere gerador direito ou esquerdo, então $\widehat{R} \simeq {}_RR$ ou $\widehat{R} \simeq R_R$, logo pelo teorema 3.9, R é de Frobenius.

Reciprocamente, suponhamos que R é de Frobenius, então $\widehat{R} \simeq R_R$ pelo teorema 3.9, seja $\psi : R \to R_R$ um isomorfismo. Como ψ é um isomorfismo de R-módulos direitos, então $\psi(r) = \psi(1)r = \chi^r, \forall r \in R$. Ou seja, χ é um caractere gerador direito. □

De seguida iremos demonstrar uma outra propriedade, exposta na proposição 4.14 que será necessária á 3ª demonstração do teorema principal.

Lema 3.11. *Seja χ um caracter de um anel finito R. Então χ é um caracter gerador direito se e só se* $\ker \chi$ *não possui ideais direitos diferentes de* $\{0\}$.

Demonstração. Dado χ um caractere direito de R e $\phi : R \to \widehat{R}$ o homomorfismo de R-módulos direitos definido por $\phi(r) = \chi^r$, começamos por mostrar que $x \in \ker(\phi)$ se e só se $xR \in \ker(\chi)$.

Tem-se que $x \in \ker(\phi)$ se e só se $\chi^x(r) = 1, \forall r \in R$, o que é equivalente a $xR \subseteq \ker(\chi)$.

Suponhamos agora que χ é um caractere gerador, então ϕ é um isomorfismo, ou seja, é injetiva. Logo $\ker(\phi) = \{0\}$ e pelo que vimos $\forall x \in R \setminus \{0\}, xR \nsubseteq \ker(\chi)$. Vamos supor que existe um ideal direito, $J \neq \{0\}$, em $\ker(\chi)$, então para algum $x \in J$ vamos ter $xR \subseteq J \subseteq \ker(\chi)$. Absurdo, logo $\ker(\chi)$ não possui ideais direitos diferentes de $\{0\}$.

Reciprocamente suponhamos que $\ker(\chi)$ não possui ideais direitos diferentes de $\{0\}$. Logo, pelo que foi visto no início da demonstração, o único elemento de $\ker(\phi)$ é 0. Pelo lema 1.6 $|R| = \left|\widehat{R}\right|$. Logo ϕ é também sobrejetiva e por isso é um isomorfismo, ou seja, χ é um caractere gerador direito. □

Proposição 3.12. *Seja R um anel finito de Frobenius, com caractere gerador direito χ, seja M um R-módulo direito finitamente gerado e $Hom_R(M, R)$ o grupo dos homomorfismos de M em R. Então a aplicação $f : Hom_R(M, R) \to \widehat{M}$, dada por $f(\lambda) = \chi \circ \lambda$ é um homomorfismo injetivo de grupos abelianos.*

Demonstração. Começamos por ver que é de facto um homomorfismo. Sejam λ_1, λ_2 elementos de $Hom_R(M, R)$, $f(\lambda_1 + \lambda_2)(x) = \chi(\lambda_1(x) + \lambda_2(x)) = \chi(\lambda_1(x)) \cdot \chi(\lambda_2(x))$, $\forall x \in R$, porque χ é homomorfismo de $(M, +)$ para $(\mathbb{C}, \cdot)$.

Vamos agora ver que $\ker(f) = \{0\}$. Se $\lambda \in \ker(f)$, então $\chi(\lambda(M)) = 1$, logo $\lambda(M)$ está contido em $\ker(\chi)$. Mas $\lambda(M)$ é um ideal direito de R (pelas propriedades dos homomorfismos vistas no capítulo 1), logo pelo lema 3.11 $\lambda(M) = \{0\}$. Ou seja, $\lambda = 0_{Hom_R(M,R)}$. □

Capítulo 4

Teorema da Extensão em Anéis Finitos

Neste capítulo vais ser então feita a prova do seguinte teorema,

Teorema da Extensão para Anéis Finitos. *Seja R um anel de Frobenius finito, $C \leq R^n$ um R-código esquerdo (ou direito) e $\varphi : C \to R^n$ um homomorfismo linear esquerdo (ou direito) que preserva o peso de Hamming. Então φ pode ser estendido a uma transformação monomial esquerda (ou direita) de R^n.*

A ideia da primeira demonstração, de abordagem combinatória, é provar um teorema semelhante, mas utilizando pesos homogéneos. No entanto, é possível demonstrar que para um dado peso homogéneo, os monomorfismos que o preservam são exatamente os homomorfismos que preservam o peso de Hamming. Estabelecendo assim uma relação entre estes dois pesos e consequentemente entre os homomorfismos que os preservam podemos demonstrar o teorema da extensão, demonstrando uma versão sua para os pesos homogéneos. Para isso vai ser necessário alguns resultados sobre a função de Möbius para c.p.o.'s finitos. Esta função vai ser essencial para a demonstração. A segunda demonstração baseia-se essencialmente na propriedade dos anéis de Frobenius, que está exposta no corolário 3.10, de que todo o anel de Frobenius possui um caractere gerador.

O objetivo das duas provas será mostrar que o homomorfismo linear que preserva os pesos $\varphi : C \to R^n$ satisfaz

$$\varphi(x) = \varphi(x_1, \cdots, x_n) = (x_{\sigma(1)}u_1, \cdots, x_{\sigma(n)}u_n)$$

ou o análogo para o lado direito, para $u_1, \cdots, u_n$ unidades de R e $\sigma \in S_n$. Se conseguirmos provar que φ satisfaz esta condição, podemos claramente concluir que é restrição de uma transformação monomial, esquerda ou direita de R^n.

4.1 Função de Möbius e peso homogéneo

Começamos então por ver como podemos relacionar a função de Möbius com pesos homogéneos.

Definição 4.1. *Seja P um c.p.o. finito, $Int(P)$ o conjunto dos intervalos de P e $\mathcal{A} = \mathcal{F}(Int(P), \mathbb{R})$ a Álgebra Incidente de P sobre o anel dos números reais $\mathbb{R}$ (a definição pode ser encontrada no subcapítulo A.4 do anexo). Então a função de Möbius, $\mu : Int(P) \to \mathbb{R}$ é a função inversa, em $\mathcal{A}$, da função zeta, $\zeta : Int(P) \to \mathbb{R}$ definida por $\zeta([x, y]) = 1$. Esta função pode ser definida recursivamente de duas formas, onde $\mu(x, y) := \mu([x, y])$ para $x \leq y$:*

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

e

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

Como pode ser verificado no início do subcapítulo A.4 do anexo Álgebra Incidente.

Teorema (Fórmula da Inversão de Möbius)**.** *Seja P um c.p.o finito e $g, f : P \to \mathbb{R}$ duas funções. Então as seguinte condições são equivalentes:*

$$g(x) = \sum_{y \leq x} f(y), \quad \forall x \in P$$

se e só se

$$f(x) = \sum_{y \leq x} g(y)\mu(y, x), \quad \forall x \in P.$$

Este teorema está demonstrado no subcapítulo A.4 do anexo Álgebra Incidente e corresponde ao teorema A.23.

O próximo lema é um resultado intermédio que vai ser usado na demonstração do teorema 4.7.

Lema 4.2. *Seja R um anel finito, $L(R)$ o reticulado dos seus ideias esquerdos e $I \in L(R)$. Se o intervalo $[\{0\}, I]$ é atomístico, então $\mu(\{0\}, I) \neq 0$.*

Demonstração.
Para podermos fazer esta prova precisamos de um resultado de [14, Equation 3.33] (pág. 317) que nos diz: Seja L um reticulado semimodular finito com minimo 0, máximo 1 e

átomo a, então

$$\mu(0,1) = -\sum_{\substack{t \text{ coatomo} \\ a \not\leq t}} \mu(0,t) \tag{4.1}$$

Porém este resultado, quando exposto em [14] refere-se a reticulados semimodulares finitos, que é o caso, pois R é finito e $[\{0\}, I]$ é um reticulado de submódulos de R como R-módulo e por isso é modular, logo semimodular pelo lema 1.5.

Note-se que seja $A \leq I$, o intervalo $[\{0\}, A]$ continua a ser um reticulado semimodular finito atomistic com minimo $\{0\}$ e máximo A. Assim a equação 4.1 pode ser aplicada em cada um desses intervalos.

Vamos então provar por indução que para qualquer $A \leq I$ de comprimento n temos $\mu(\{0\}, A) = (-1)^n \cdot c_n(A)$, onde $c_n(A)$ é um número inteiro positivo.

Suponhamos que $A \leq I$ é um submódulo simples, ou seja, tem comprimento 1, $l(A) = 1$. Então por definição de função de Möbius,

$$\mu(\{0\}, A) = -\mu(\{0\}, \{0\}) = -1.$$

Se $l(A) = 2$ e considere-se $S \leq A$ minimal, ou seja, átomo. Então

$$\mu(\{0\}, A) = -\sum_{\substack{T \text{ coatomo} \\ S \not\leq T}} \mu(0,T).$$

Mas $l(T) = 1$, logo ficamos com,

$$\mu(\{0\}, A) = -(-1) \cdot |\{T \leq A : S \not\leq A\}| = (-1)^2 \cdot c_2(A).$$

onde temos, claramente, $c_2(A) > 0$.

Supomos agora que o que pretendemos demonstrar é válido para qualquer $A \leq I$ com $l(A) = n$. Seja então $A \leq I$ e $S \leq A$ simples, tal que $l(A) = n + 1$, temos $\mu(\{0\}, A) = -\sum_{\substack{T \text{ coatomo} \\ S \not\leq T}} \mu(0,T)$. Por hipótese ficamos com:

$$\mu(\{0\}, A) = -\sum_{\substack{T \text{ coatomo} \\ S \not\leq T}} (-1)^n c_n(T) = (-1)^{n+1} \cdot \sum_{\substack{T \text{ coatomo} \\ S \not\leq T}} c_n(T) = (-1)^{n+1} \cdot c_{n+1}(A).$$

Como $c_{n+1}(A)$, por hipótese é a soma de números naturais não nulos, então é também um número natural não nulo. Como I é submódulo dele próprio, temos assim o pretendido.

□

De seguida vamos definir uma relação de equivalência e provar um resultado intermédio que nos vai ajudar em alguns cálculos intermédios nas futuras provas.

Seja R um anel finito, considere-se o conjunto parcialmente ordenado pela inclusão $I_P(R) = \{Rx \mid x \in R\}$.

Lema 4.3. *Para $x \in R$, o conjuto $R^*x = \{rx \mid r \in R^*\}$ é o conjunto de todos os geradores de Rx e temos ainda,*

$$|R^*x| = \sum_{Ry \leq Rx} |Ry|\mu(Ry, Rx).$$

Demonstração.
Vamos começar por provar a primeira afirmação.

Seja $G_x = \{\text{Geradores de } Rx\}$. O objetivo é provar que $R^*x = G_x$. Seja então, $u \in R^*$, claramente $Rux \subseteq Rx$. Seja agora $rx \in Rx$, $rx = ru^{-1}ux \in Rux$, logo também $Rx \subseteq Rux$. Assim, $Rux = Rx$. Logo ux é gerador de Rx.

Temos então $R^*x \subseteq G_x$.

Seja agora $y \in G_x$, então $Rx = Ry$. Além disso $\exists a \in R : y = ax$. Considere-se agora o epimorfismo de R-módulos á esquerda,

$$\varphi : R \to Rx$$
$$r \mapsto rx$$

Assim, $y = \varphi(a)$. Mas, como φ é um homomorfismo, temos,

$$\varphi(Ra) = R\varphi(a) = Ry = Rx = \varphi(R).$$

Seja agora $r \in R$, então existe $r' \in R$ tal que $\varphi(r) = \varphi(r'a) \Rightarrow r - r'a \in \ker(\varphi)$, logo $\exists k \in \ker(\varphi) : r - r'a = k \Leftrightarrow r = r'a + k$. Logo $R \subseteq Ra + \ker(\varphi)$, como, claramente também temos $Ra + \ker(\varphi) \subseteq R$, ficamos com $R = Ra + \ker(\varphi)$.

Podemos então usar o Teorema de Bass para concluir que $a+\ker(\varphi)$ possui uma unidade de R. Seja $u \in R^*$ essa unidade, temos que $u = a + b$, para $b \in \ker(\varphi)$. Mas então

$$ux = ax + bx = ax = y.$$

Logo $y \in R^*x$ e, finalmente, $R^*x = G_x$.

Para a segunda parte da lema iremos usar fórmula da inversão de Möbius (teorema 4.1) no c.p.o. $I_P(R)$. Comecemos por demonstrar que $|Rx| = \sum_{Ry \leq Rx} |R^*y|$.

A relação binária em $R \times R$, definida por $x \sim y$ se e só se $Rx = Ry$, para $x, y \in R$ é uma relação de equivalência: Note-se agora que as classes de equivalência desta relação são precisamente os conjuntos R^*x, pois dois elementos são equivalentes se e só se são geradores de um mesmo ideal principal. Como $\sim$ é uma relação de equivalência, a união das suas classes formam uma partição de todo o conjunto. Assim, considere-se a relação apenas no ideal Rx, as classes de equivalência dos elementos deste conjunto formam uma partição dele, ou seja,

$$Rx = \dot{\bigcup_{y \in Rx}} R^*y$$

Logo $|Rx| = |\dot{\bigcup_{y \in Rx}} R^*y| = \sum_{Ry \leq Rx} |R^*y|$.

Tomando agora, $f(Rx) = \sum_{Ry \leq Rx} |R^*x|$ e $g(Rx) = |Rx|$, que são funções de $I_P(R)$ em $\mathbb{R}$ e que por isso satisfazem as condições necessárias para podermos aplicar a inversão de Möbius, obtemos o resultado desejado se o fizermos. □

Nota 4.4. *Usando a primeira condição do lema anterior temos que, se $Rx = Ry$, então $|R^*x| = |R^*y|$.*

Podemos assim provar o seguinte teorema que nos dá uma definição alternativa de peso homogéneo

Teorema 4.5. *Uma função peso num anel finito R é homogéneo se e só se existe um número real $c \geq 0$ tal que*

$$wt(x) = c\left(1 - \frac{\mu(0, Rx)}{|R^*x|}\right), \quad \forall x \in R \setminus \{0\}$$

Demonstração. Começamos por provar a primeira implicação. Suponhamos então que temos um peso homogêneo, wt, ou seja, um peso que satisfaz:

1. Se $Rx = Ry$, então $wt(x) = wt(y), \forall x, y \in R$.
2. Existe um número real $c \geq 0$ tal que

$$\sum_{y \in Rx} wt(y) = c|Rx|, \quad \forall x \in R \setminus \{0\}.$$

e consideremos a função $f : I_P(R) \to \mathbb{R}$ definida por

$$f(Rx) = (c - wt(x))|R^*x|.$$

Esta função está bem definida pela condição 1 e pela nota 4.4, ou seja, se $Rx = Ry$, então $wt(x) = wt(y)$ e $|R^*x| = |R^*y|$, assim $f(Rx) = f(Ry)$. Além disso temos

$$\sum_{Ry \subseteq Rx} f(Ry) = \sum_{y \in Rx} (c - wt(y)). \tag{4.2}$$

Porque,

$$\sum_{Ry \subseteq Rx} f(Ry) = \sum_{Ry \subseteq Rx} (c - wt(y))|R^*y| = \sum_{Ry \subseteq Rx} \sum_{y' \in R^*y} (c - wt(y))$$

e considerando agora a relação de equivalência, $\sim$, definida na prova do lema 4.3, R^*y são as suas classes de equivalência e por isso ficamos com

$$\sum_{Ry \subseteq Rx} \sum_{y' \in R^*y} (c - wt(y)) = \sum_{y \in Rx} (c - wt(y)).$$

Usando agora a condição 2 da definição de peso homogéneo, podemos concluir que

$$\sum_{y \in Rx} (c - wt(y)) = \sum_{y \in Rx} c - \sum_{y \in Rx} wt(y) = c|Rx| - \sum_{y \in Rx} wt(y) = 0, \quad \forall x \in R \setminus \{0\}$$

Ficamos então com

$$\sum_{Ry \subseteq Rx} f(Ry) = 0, \quad \forall x \in R \setminus \{0\}.$$

Tomemos agora a função $g : I_P(R) \to \mathbb{R}$ definida por

$$g(Rx) = \begin{cases} 0, & \text{se} \quad x \in R \setminus \{0\} \\ c, & \text{se} \quad x = 0 \end{cases}$$

Como $f(\{0\}) = c$, podemos ver a igualdade obtida anteriormente como

$$\sum_{Ry \subseteq Rx} f(Ry) = g(Rx).$$

Aplicando a inversão de Möbius obtemos,

$$f(Rx) = \sum_{Ry \subseteq Rx} g(Ry)\mu(Ry, Rx) = c\mu(0, Rx)$$

Resolvendo a equação ficamos com:

$$(c - wt(x))|R^*x| = c\mu(0, Rx) \;\Leftrightarrow\; wt(x) = c(1 - \frac{\mu(0, Rx)}{|R^*x|}), \quad \forall x \in R$$

Reciprocamente, seja wt um peso e suponhamos que existe um número real positivo, c

tal que

$$wt(x) = c(1 - \frac{\mu(0, Rx)}{|R^*x|}), \quad \forall x \in R$$

Queremos agora ver que wt é um peso homogêneo, ou seja que se verificam 1 e 2. Se $Rx = Ry$, então, pela nota 4.4

$$wt(Rx) = c(1 - \frac{\mu(0, Rx)}{|R^*x|}) = c(1 - \frac{\mu(0, Ry)}{|R^*y|}) = wt(Ry)$$

Considere-se de novo a função $f : I_P(R) \to \mathbb{R}$, que continua bem definida, pois já provamos que 1 se verifica. Temos também de novo que a igualdade (4.2) é válida. Vejamos agora como podemos expressar $f(Rx)$ em função de c e da função μ:

$$\begin{aligned} f(Rx) &= (c - wt(x))|R^*x| = \left(c - c\left(1 - \frac{\mu(0, Rx)}{|R^*x|}\right)\right)|R^*x| \\ &= c\left(\frac{\mu(0, Rx)}{|R^*x|}\right)|R^*x| = c\mu(0, Rx) \end{aligned}$$

Considerando de novo a mesma função $g : I_P(R) \to \mathbb{R}$, podemos ver a igualdade acima como

$$f(Rx) = \sum_{Ry \subseteq Rx} g(Ry)\mu(Ry, Ry)$$

aplicando a inversão de Möbius temos:

$$g(Rx) = \sum_{Ry \subseteq Rx} f(Ry).$$

Logo

$$\sum_{Ry \subseteq Rx} f(Ry) = 0, \quad \forall x \in R \setminus \{0\}.$$

Pela equação 4.2 ficamos com

$$\sum_{y \in Rx} (c - wt(y)) = 0 \Leftrightarrow \sum_{y \in Rx} wt(y) = \sum_{y \in Rx} c \Leftrightarrow \sum_{y \in Rx} wt(y) = c|Rx|, \quad \forall x \in R \setminus \{0\}$$

Verifica-se assim a 2ª condição, logo wt é homogêneo. □

O próximo lema tem como objetivo auxiliar a demonstração do teorema 4.7.

Lema 4.6. *Seja R um anel, $I \leq R$ um ideal esquerdo não nulo qualquer, wt um peso homogéneo e $c \in \mathbb{R}^+$ a constante relativa a esse peso. Então as seguintes condições são equivalentes:*

1. $\sum_{Rx \leq I} \mu(0, Rx) = 0$.
2. $\sum_{y \in I} wt(y) = c|I|$.

Demonstração.

(1) $\Rightarrow$ (2).

Pelo teorema 4.5 temos

$$\begin{aligned}\sum_{x \in I} wt(x) &= \sum_{x \in I} c\left(1 - \frac{\mu(0, Rx)}{|R^*x|}\right) = \sum_{x \in I} c + \sum_{x \in I} c\frac{\mu(0, Rx)}{|R^*x|} \\ &= c|I| + c \sum_{Rx \leq I} |R^*x| \, \frac{\mu(0, Rx)}{|R^*x|} \\ &= c|I| + c \sum_{Rx \leq I} \mu(0, Rx) \\ &= c|I| \qquad \text{(por hipótese)}\end{aligned}$$

(2) $\Rightarrow$ (1).

Da demonstração da primeira implicação retiramos que

$$\sum_{x \in I} wt(x) = c|I| + c \sum_{Rx \leq I} \mu(0, Rx)$$

Como, por hipótese $\sum_{y \in I} wt(y) = c|I|$, então $c \sum_{Rx \leq I} \mu(0, Rx) = 0$, ou seja, $\sum_{Rx \leq I} \mu(0, Rx) = 0$, pois c é não nulo. □

Teorema 4.7. *As seguintes condições são equivalentes para um anel finito R, um peso homogêneo, wt e $c \in \mathbb{R}^+$:*

1. *O $soc({}_RR)$ é principal à esquerda.*
2. *Para todo o ideal esquerdo não nulo $I \leq {}_RR$, $\sum_{y \in I} wt(y) = c|I|$.*

Demonstração.

(1) $\Rightarrow$ (2).

Suponhamos que $soc({}_RR)$ é principal á esquerda, queremos mostrar que $\sum_{Rx \leq I} \mu(0, Rx) = 0$.

Considere-se $I \leq {}_RR$, então $I \bigcap soc({}_RR)$ é um ideal esquerdo principal e corresponde ao $soc(I)$, se virmos I como módulo esquerdo. É um ideal esquerdo porque é a interseção de ideais esquerdos e é principal porque qualquer submódulo de $soc({}_RR)$ é cíclico pelo lema 1.1 e por isso principal. Além disso, como R é artiniano, contém submódulos simples. Logo $I \bigcap soc({}_RR) \neq \{0\}$.

Note-se agora que como $soc(I)$ é cíclico, todos os seus submódulos são principais, pelo lema 1.1 e por isso pertencem a $I_P(R)$. Se considerarmos a função de Möbius em $I_P(R)$ por definição temos $\sum_{0\leq Rx\leq soc(I)} \mu(0, Rx) = 0$.

Assim,

$$\sum_{Rx\leq I} \mu(0, Rx) = \sum_{0\leq Rx\leq soc(I)} \mu(0, Rx) + \sum_{\substack{Rx\leq I \\ Rx\nleq soc({}_RR)}} \mu(0, Rx)$$
$$= \sum_{\substack{Rx\leq I \\ Rx\nleq soc({}_RR)}} \mu(0, Rx)$$

Para finalizar assumimos que existe $Rx \leq I$ tal que $Rx \nleq soc({}_RR)$ e $\mu(0, Rx) \neq 0$. Suponhamos também que esse tal Rx é minimal em relação a essa propriedade. Por definição de μ temos,

$$0 = \sum_{Ry\leq Rx} \mu(0, Ry) = \sum_{Ry\leq soc(Rx)} \mu(0, Ry) + \sum_{\substack{Ry<Rx \\ Ry\nleq soc({}_RR)}} \mu(0, Ry) + \mu(0, Rx)$$

$$= \mu(0, Rx) \qquad \text{(contradição)}$$

Note-se que $\sum_{\substack{Ry<Rx \\ Ry\nleq soc({}_RR)}} \mu(0, Ry) = 0$, porque, por minimalidade de Rx, $\mu(0, Ry) = 0$, $\forall Ry < Rx$ tal que $Ry \nleq soc({}_RR)$. Como obtivemos uma contradição tal Rx não existe e por isso $\forall Rx \leq I$ tal que $Rx \nleq soc({}_RR)$, temos $\mu(0, Rx) = 0$. Logo

$$\sum_{\substack{Rx\leq I \\ Rx\nleq soc({}_RR)}} \mu(0, Rx) = 0.$$

Assim,

$$\sum_{Rx\leq I} \mu(0, Rx) = 0$$

Pelo lema 4.6 temos então o pretendido.

(2) $\Rightarrow$ (1).

Suponhamos que para todo o ideal esquerdo não nulo $I \leq {}_RR$, $\sum_{y\in I} wt(y) = c|I|$. Novamente pelo lema 4.6 temos então que $\sum_{Rx\leq I} \mu(0, Rx) = 0$.

Para demonstrarmos que $soc({}_RR)$ é ideal esquerdo principal, ou seja que é principal, porque $soc({}_RR)$ é sempre ideal esquerdo, vamos supor que não o é. De seguida consideramos um ideal $I \leq {}_RR$ contido em $soc({}_RR)$, não principal e minimal em relação a esta

propriedade (existe porque R é artiniano). Denotando por μ_L a função de Möbius no conjunto de todos os ideais de R, munido com a relação de inclusão, temos por definição,

$$\begin{aligned} 0 &= \sum_{J \leq I} \mu_L(0, J) = \sum_{J < I} \mu_L(0, J) + \mu_L(0, I) = \sum_{Rx \leq I} \mu(0, Rx) + \mu_L(0, I) \\ &= \mu_L(0, I) \qquad \text{(por hipótese)} \end{aligned}$$

Mas $I \leq soc(R)$, ou seja, I, quando visto como submódulo, é semisimples, que neste caso é equivalente á condição de o intervalo $[0, I]$ ser atomístico, como é observado no capítulo 1. Assim, pela proposição 4.2 temos que $\mu_L(0, I) \neq 0$. Absurdo, logo $soc(R)$ é principal. □

4.2 Relação entre os pesos homogéneo e de Hamming

Nesta secção vamos então ver qual a relação dos dois pesos e perceber de que forma provando o teorema principal para pesos homogéneos podemos generalizar para a versão com pesos de Hamming. Vamos começar por fixar um peso homogéneo no anel R, com base no resultado do teorema 4.5:

$$\begin{aligned} w_{hom} : R &\to \mathbb{R} \\ x &\mapsto 1 - \frac{\mu(0, Rx)}{|R^* x|} \end{aligned}$$

Ou seja, com $c = 1$. Este, induz uma função peso em R^n da seguinte forma,

$$\begin{aligned} w_{hom}^{(n)} : R^n &\to \mathbb{R} \\ x &\mapsto \sum_{i=1}^{n} w_{hom}(\pi_i(x)) \end{aligned}$$

Onde π_i denota o homomorfismo que projeta os elementos de R^n na sua i-ésima coordenada. A este peso chamaremos peso homogéneo de R^n.

Definição 4.8. *Seja C um R-código de comprimento n e $f : R^n \to \mathbb{R}$, tal que se $Rx = Ry$, então $f(x) = f(y)$. Um homomorfismo de R-módulos $\varphi : C \to R^n$ é chamado de f-isometria se satisfaz:*

$$f\varphi(c) = f(c), \quad \forall c \in C.$$

Se f for o peso homogéneo de R^n definido atrás, chamamos a φ uma isometria homogénea. Se f for o peso de Hamming, chamamos a φ uma isometria de Hamming ou apenas

isometria.

Lema 4.9. *Seja R um anel finito de Frobenius, C um R-código de comprimento n e $\varphi : C \to R^n$ uma isometria homogénea, então as duas seguintes afirmações são válidas:*

1. $\frac{1}{|C|}\sum_{c\in C} w_{hom}^{(n)}(c) = |\{i|\pi_i(C) \neq \{0\}\}|$.
2. $|\{i|\pi_i(C) = \{0\}\}| = |\{i|\pi_i\varphi(C) = \{0\}\}|$.

Demonstração.
1 Como R é um anel de Frobenius, o seu socle é principal e por isso podemos usar o teorema 4.7. Relembremos ainda que pelo teorema do isomorfismo temos que dado um homomorfismo de módulos $h : M \to N$,

$$\mathrm{Im}(h) \simeq \frac{M}{\ker(h)}.$$

Assim se considerarmos o homomorfismo π_i e lembrando que $\ker(\pi_i\big|_C) = C \cap \ker(\pi_i)$, temos

$$\pi_i(C) \simeq \frac{C}{C \cap ker(\pi_i)}$$

Logo $|\pi_i(C)| = \frac{|C|}{|C\cap ker(\pi_i)|}$. Notemos ainda que seja $r \in R$ e $A = \{c \in C : \pi_i(c) = r\}$, então $|A| = |C \cap \ker(\pi_i)|$. Isto acontece porque para $c_1, c_2 \in A$,

$$\pi_i(c_1) = \pi_2(c_2) \Leftrightarrow \pi_i(c_1 - c_2) = 0 \Leftrightarrow c_1 - c_2 \in C \cap \ker(\pi_i)$$

logo, seja $c_1 \in A, \forall c \in A, c = c_1 + k, k \in C \cap \ker(\pi_i)$.

Além disso $\pi_i(C)$ é um ideal esquerdo de ${}_RR$. Assim se $\pi_i(C) \neq \{0\}$, pelo teorema 4.7 temos então:

$$\sum_{x\in\pi_i(C)} w_{hom}(x) = |\pi_i(C)|\,.$$

Assim $|C \cap ker(\pi_i)|\sum_{x\in\pi_i(C)} w_{hom}(x) = |C|$

Logo,

$$\begin{aligned}
\sum_{c\in C} w_{hom}^{(n)}(c) &= \sum_{c\in C}\sum_{i=1}^{n} w_{hom}(\pi_i(c)) \\
&= \sum_{i=1}^{n}\sum_{x\in\pi_i(C)} |\{c \in C|\pi_i(c) = x\}|\, w_{hom}(x) \\
&= \sum_{i=1}^{n} |C \cap ker(\pi_i)| \sum_{x\in\pi_i(C)} w_{hom}(x) \\
&= |C| \cdot |\{i|\pi_i(C) \neq \{0\}\}|
\end{aligned}$$

A passagem da penúltima para a última igualdade faz-se dividindo a soma principal em duas outras, a primeira soma $|C \cap ker(\pi_i)| \sum_{x \in \pi_i(C)} w_{hom}(x)$ apenas para as coordenadas tais que $\pi_i(C) \neq \{0\}$, a segunda para as coordenadas com $\pi_i(C) = \{0\}$. No entanto, como $w_{hom}(0) = 0$, a segunda soma é 0 e portanto ficamos só com a primeira. O primeiro resultando obtêm-se então dividindo a igualdade por $|C|$.

2 Pelo Teorema do Isomorfismo temos que

$$Im(\varphi) \simeq \frac{C}{\ker(\varphi)}$$

Logo,

$$|\varphi(C)| = \frac{|C|}{|\ker(\varphi)|} \Leftrightarrow |\varphi(C)| \cdot |\ker(\varphi)| = |C|$$

Além disso notemos que se C é um R-código, então como $\varphi(C) \leq R^n$ é também um R-código. Assim,

$$\begin{aligned}
|\{i|\pi_i(C) \neq \{0\}\}| &= \frac{1}{|C|} \sum_{c \in C} w_{hom}^n(c) \\
&= \frac{1}{|\varphi(C)| \cdot |\ker(\varphi)|} \sum_{c \in C} w_{hom}^n(c) \\
&= \frac{1}{|\varphi(C)| \cdot |\ker(\varphi)|} \sum_{c \in C} w_{hom}^n(\varphi(c)) \\
&\qquad \text{(Porque } \varphi \text{ é uma isometria homogénea)} \\
&= \frac{1}{|\varphi(C)| \cdot |\ker(\varphi)|} \sum_{d \in \varphi(C)} w_{hom}^n(d) \cdot |\{c_i \in C|\varphi(c) = d\}| \\
&= \frac{1}{|\varphi(C)| \cdot |\ker(\varphi)|} \sum_{d \in \varphi(C)} w_{hom}^n(d) \cdot |\ker(\varphi)| \\
&= \frac{1}{|\varphi(C)|} \sum_{d \in \varphi(C)} w_{hom}^n(d) \\
&= |\{i|\pi_i(\varphi(C)) \neq \{0\}\}| \qquad \text{(Por 1)}
\end{aligned}$$

Logo, claramente $|\{i|\pi_i(C) = \{0\}\}| = |\{i|\pi_i\varphi(C) = \{0\}\}|$. □

Seja M um R-módulo esquerdo, denotemos por $F({}_RM, \mathbb{R})$ o espaço vetorial de todas as funções $f : {}_RM \to \mathbb{R}$, tais que se $Rx = Ry$, então $f(x) = f(y)$, $\forall x, y \in M$. O objetivo seguinte é mostrar que os pesos w_{hom}^n e w_H, onde w_H é o peso de Hamming, são iguais. Para isso vamos definir duas aplicações lineares de $F({}_RM, \mathbb{R})$ em $F({}_RM, \mathbb{R})$, Σ e Δ e demonstrar que estas duas aplicações são inversas uma da outra. Para conseguirmos demonstrar o que pretendemos iremos necessitar de um teorema, que também iremos

demonstrar, que nos dá uma fórmula de inversão para elementos de $F({}_RM, \mathbb{R})$ idêntica á fórmula da inversão de Möbius.

Definimos então a função

$$\begin{aligned} K : M \times M &\to \mathbb{R} \\ (x, y) &\mapsto \frac{|Rx|}{|R^*x|} \cdot \frac{|Ry|}{|R^*y|} \cdot \mu(Rx, Ry) \end{aligned}$$

onde μ denota a função de Möbius no conjunto $\{Rx | x \in M\}$ e as aplicações $\Sigma, \Delta : F({}_RM, \mathbb{R}) \to F({}_RM, \mathbb{R})$ dadas por

$$(\Sigma(f))(x) = \Sigma f(x) = \frac{1}{|R|} \sum_{r \in R} f(rx)$$

e

$$(\Delta(f))(x) = \Delta f(x) = \frac{1}{|R|} \sum_{r \in R} f(rx) K(rx, x), \quad \forall x \in M$$

Teorema 4.10. *Dado um R-módulo esquerdo M e $f, g \in F({}_RM, \mathbb{R})$ as seguintes condições são equivalentes:*

1. $g(x) = \frac{1}{|R|} \sum_{r \in R} f(rx), \forall x \in M$
2. $f(x) = \frac{1}{|R|} \sum_{r \in R} g(rx) K(rx, x), \forall x \in M$

Demonstração.

(1) $\Rightarrow$ (2)

Comecemos por notar que seja $x \in R$ o $l.ann_r(x)$ é o núcleo do homomorfismo sobrejetivo $h : R \to Rx$ definido por $h(r) = rx, \forall r \in R$. Logo pelo teorema do isomorfismo, temos que $R/l.ann_R(x) \simeq Rx$. Daqui podemos concluir que $|l.ann_R(x)| = \frac{|R|}{|Rx|}$. Notemos ainda que seja $t \in Rx$ e $A = \{r \in R : rx = t\}$, então $|A| = |\ker(h)| = |l.ann_R(x)|$. Isto acontece pois para $r_1, r_2 \in A$,

$$h(r_1) = h(r_2) \Leftrightarrow h(r_1 - r_2) = 0 \Rightarrow r_1 - r_2 \in \ker(h)$$

logo, seja $r_1 \in A$, $\forall r \in A, r = r_1 + k, k \in \ker(h)$.

Temos então,

$$\begin{aligned} g(x) &= \frac{1}{|R|} \sum_{r \in R} f(rx) = \frac{1}{|R|} \sum_{t \in Rx} f(t) \, |A| \\ &= \frac{1}{|R|} \sum_{t \in Rx} f(t) \, |l.ann_R(x)| = \frac{1}{|R|} \sum_{t \in Rx} f(t) \cdot \frac{|R|}{|Rx|} \end{aligned}$$

$$= \sum_{t \in Rx} f(t) \cdot \frac{1}{|Rx|} = \sum_{Rt \leq Rx} f(t) \cdot \frac{|R^*t|}{|Rx|}$$

Considere-se agora as funções $\alpha, \beta : \{Rx : x \in M\} \to \mathbb{R}$ definidas por $\alpha(Rx) = g(x)\,|Rx|$ e $\beta(Rx) = f(x)\,|R^*x|$, então

$$\alpha(Rx) = \sum_{Rt \leq Rx} f(t) \cdot |R^*t| = \sum_{Rt \leq Rx} \beta(Rt)$$

aplicando a inversão de Möbius, ficamos com:

$$f(x)\,|R^*| = \beta(Rx) = \sum_{Rt \leq Rx} \alpha(Rt)\mu(Rt, Rx) = \sum_{Rt \leq Rx} g(t) \cdot |Rt|\,\mu(Rt, Rx)$$

Logo,

$$\begin{aligned} f(x) &= \sum_{Rt \leq Rx} g(t) \cdot \frac{|Rt|}{|R^*x|} \cdot \mu(Rt, Rx) = \sum_{t \in Rx} g(t) \cdot \frac{|Rt|}{|R^*x| \cdot |R^*t|} \cdot \mu(Rt, Rx) \\ &= \sum_{t \in Rx} g(t) \cdot \frac{1}{|Rx|} \cdot \frac{|Rt| \cdot |Rx|}{|R^*x| \cdot |R^*t|} \cdot \mu(Rt, Rx) = \sum_{t \in Rx} g(t) \cdot \frac{1}{|Rx|} \cdot K(t, x) \\ &= \frac{1}{|R|} \sum_{t \in Rx} g(t) \cdot \frac{|R|}{|Rx|} \cdot K(t, x) = \frac{1}{|R|} \sum_{t \in Rx} g(t) \cdot |ann_R(x)| \cdot K(t, x) \\ &= \frac{1}{|R|} \sum_{r \in R} g(t) K(t, x) \end{aligned}$$

(2) $\Rightarrow$ (1)
Analogamente temos:

$$\begin{aligned} f(x) &= \frac{1}{|R|} \sum_{r \in R} g(rx) K(rx, x) = \frac{1}{|R|} \sum_{t \in Rx} g(t)\,|A|\,K(t, x) \\ &= \frac{1}{|R|} \sum_{t \in Rx} g(t)\,|l.ann_R(x)|\,K(t, x) = \frac{1}{|R|} \sum_{t \in Rx} g(t) \cdot \frac{|R|}{|Rx|} K(t, x) \\ &= \sum_{t \in Rx} g(t) \cdot \frac{|Rt|}{|R^*x| \cdot |R^*t|} \cdot \mu(Rt, Rx) = \sum_{Rt \leq Rx} g(t) \cdot \frac{|Rt|}{|R^*x|} \cdot \mu(Rt, Rx) \end{aligned}$$

Considerando novamente as funções α e β,

$$\beta(Rx) = \sum_{Rt \leq Rx} g(t) \cdot |Rt|\,\mu(Rt, Rx) = \sum_{Rt \leq Rx} \alpha(Rt)\mu(Rt, Rx)$$

aplicando a inversão de Möbius, ficamos com:

$$g(x) \cdot |Rx| = \alpha(Rx) = \sum_{Rt \leq Rx} \beta(Rt) = \sum_{Rt \leq Rx} f(t) \cdot |R^*t|$$

Logo,

$$g(x) = \sum_{Rt \leq Rx} f(t) \cdot \frac{|R^*t|}{|Rx|} = \frac{1}{|R|} \sum_{r \in R} f(rx)$$

□

Corolário 4.11. *Σ e Δ são aplicações lineares inversas, ou seja, $(\Sigma \circ \Delta)(f) = f$ e $(\Delta \circ \Sigma)(f) = f$.*

Demonstração. Seja $g = \Sigma f \in F({}_RM)$, pelo teorema 4.10 $f = \Delta(\Sigma f) = (\Delta \circ \Sigma)(f)$. Analogamente seja $g = \Delta f \in F({}_RM)$, pelo teorema 4.10 $f = \Sigma(\Delta f) = (\Sigma \circ \Delta)(f)$.

□

Proposição 4.12. *Tomando ${}_RM = R^n$ como R-módulo esquerdo temos:*

$$\Sigma w_{hom}^{(n)} = w_H \text{ e } \Delta w_H = w_{hom}^{(n)}$$

Demonstração. Para qualquer $x \in R^n$,

$$\begin{aligned}
\Sigma w_{hom}^{(n)}(x) &= \frac{1}{|R|} \sum_{r \in R} w_{hom}^{(n)}(rx) = \frac{1}{|R|} \sum_{t \in Rx} w_{hom}^{(n)}(t) \cdot |ann_R(x)| \\
&= \frac{1}{|Rx|} \sum_{r \in R} w_{hom}^{(n)}(rx) = |\{i | \pi_i(Rx) \neq \{0\}\}| \qquad \text{(por 4.9)} \\
&= |\{i | \pi_i(x) \neq \{0\}\}| = w_H(x)
\end{aligned}$$

Pelo teorema 4.11 temos,

$$\Delta(\Sigma w_{hom}^{(n)})(x) = \Delta w_H(x) \Leftrightarrow \; w_{hom}^{(n)}(x) = \Delta w_H(x), \quad \forall x \in R^n$$

□

Proposição 4.13. *Seja C um R-código de comprimento n e $f \in F(R^n, \mathbb{R})$. Uma aplicação R-linear $\varphi : C \to R^n$ é uma f-isometria se e só se é uma (Σf)-isometria.*

Demonstração. Suponhamos que φ é uma f-isometria, então $f\varphi = f$ Logo,

$$\begin{aligned}
(\Sigma f)\varphi(c) &= \frac{1}{|R|} \sum_{r \in R} f(r\varphi(c)) = \frac{1}{|R|} \sum_{r \in R} f(\varphi(rc)) \\
&= \frac{1}{|R|} \sum_{r \in R} f\varphi(rc) = (\Sigma(f\varphi))(c) \\
&= (\Sigma f)(c), \quad \forall c \in C
\end{aligned}$$

Por isso φ é também uma (Σf)-isometria.

Suponhamos agora que φ é uma (Σf)-isometria, então $(\Sigma f)\varphi = \Sigma f$. Pelos cálculos anteriores também temos $\Sigma f = (\Sigma f)\varphi = \Sigma(f\varphi)$. Assim, pelo corolário 4.11 temos, $f = (\Delta \circ \Sigma)(f) = \Delta(\Sigma(f\varphi)) = (\Delta \circ \Sigma)(f\varphi) = f\varphi$. Logo φ é também uma f-isometria. □

A próxima proposição dá-nos então o resultado final que pretendíamos com esta secção.

Proposição 4.14. *Seja $\varphi : C \to R^n$ uma aplicação R-linear à esquerda, então φ é uma isometria homogénea injetiva, se e só se é uma isometria de Hamming.*

Demonstração. Comecemos por supor que φ é uma isometria de Hamming, ou seja, uma w_H-isometria. Como $w_H = \Sigma w_{hom}^n$, pela proposição 4.13 temos que φ é também uma w_{hom}^n-isometria, logo uma isometria homogénea. Falta apenas ver que é injetiva, mas uma isometria de Hamming é sempre injetiva porque,

$$\begin{aligned}\ker(\varphi) &= \{c \in C | \varphi(c) = 0\} \\ &= \{c \in C | w_H(c) = w_H(\varphi(c)) = w_H(0) = 0\} \\ &= \{0\}\end{aligned}$$

Reciprocamente, suponhamos que φ é uma isometria homogénea injetiva, logo é também uma (Σw_{hom}^n)-isometria e por isso, uma isometria de Hamming, novamente por 4.13. □

4.3 Uma Demonstração Combinatória

Podemos agora, finalmente provar a versão do teorema da extensão para pesos homogéneos e sobre anéis de Frobenius.

Teorema 4.15. *Seja R um anel finito de Frobenius, C um R-código de comprimento n e $\varphi : C \to R^n$ uma aplicação R-linear à esquerda injetiva, então as seguintes condições são equivalentes:*

1. *φ é uma isometria homogénea;*

2. *φ é a restrição de uma transformação monomial de R^n.*

Demonstração. Comecemos por ver que $Rx \simeq Rxu$, onde $u \in R^*$. Para isso considere-se o homomorfismo de módulos:

$$f : Rx \to Rxu$$

$$rx \mapsto rxu$$

Esta aplicação tem um homomorfismo inverso que é

$$\begin{aligned} f' : Rxu &\to Rx \\ rxu &\mapsto rxuu^{-1} \end{aligned}$$

Logo f é um isomorfismo e por isso $Rx \simeq Rxu$. Mas então se estes dois módulos são isomorfos, têm a mesma estrutura e portanto $\mu(0, Rx) = \mu(0, Rxu)$ e $|R^*x| = |R^*xu|$ Assim, temos

$$w_{hom}(x) = 1 - \frac{\mu(0, Rx)}{|R^*x|} = 1 - \frac{\mu(0, Rxu)}{|R^*xu|} = w_{hom}(xu)$$

Suponhamos então que φ é a restrição de uma transformação monomial esquerda, ou seja, $\exists T : R^n \to R^n$ definida por $T(x_1, \cdots, x_n) = (x_{\sigma(1)}u_1, \cdots, x_{\sigma(n)}u_n)$ Onde $u_1, \cdots, u_n$ são unidades de R. Queremos ver se T é uma isometria homogénea, ou seja, se preserva o peso homogéneo. Se isso se verificar então φ também preservará o peso homogéneo, porque é uma restrição de T e como tal é uma isometria homogénea. Seja então,

$$\begin{aligned} w^n_{hom}(T(x_1, \cdots, x_n)) &= w^n_{hom}(x_{\sigma(1)}u_1, \cdots, x_{\sigma(n)}u_n) \\ &= \sum_{i=1}^{n} w_{hom}(x_{\sigma(1)}u_1) = \sum_{i=1}^{n} w_{hom}(x_{\sigma(1)}) \\ &= \sum_{i=1}^{n} w_{hom}(x_i) = w^n_{hom}(x_1, \cdots, x_n) \end{aligned}$$

Logo T é uma isometria homogénea e φ também.

Suponhamos agora que φ é uma isometria homogénea e seja $D := \varphi(C)$. Supomos também que C não possui coordenadas nulas, logo pelo lema 4.9 podemos concluir que D também não possui.

Escolhemos então uma coordenada $i \in \{1, \cdots, n\}$ tal que $\{c \in C | \pi_i(c) \neq 0\}$ tenha cardinalidade mínima e denotamos $C_i := C \cap \ker(\pi_i)$. O novo código C_i é o submódulo de C que contém todos os elementos do código C que têm entrada nula na coordenada i, como tal C_i possui a i-ésima coordenada nula. Logo, novamente pelo lema 4.9, $\varphi(C_i)$ possui também uma coordenada nula, digamos j. Definimos $D_j := D \cap \ker(\pi_j)$, temos então, $\varphi(C_i) \subseteq D_j$, pois $x \in \varphi(C_i) \Rightarrow x \in \varphi(C) \wedge \pi_j(x) = 0$, ou seja, $x \in D_j$.

Suponhamos agora que $\varphi(C_i) \subsetneq D_j$, logo $C_i \subsetneq \varphi^{-1}(D_j)$, onde $\varphi^{-1}(D_j)$ é a pré-imagem de D_j por φ. Então como $\varphi(\varphi^{-1}(D_j)) = D_j$ e D_j tem a j-ésima coordenada nula, também

$\varphi^{-1}(D_j)$ tem pelo menos uma coordenada nula, digamos k, que não é i uma vez que supusemos que $C_i \neq \varphi^{-1}(D_j)$. Mas, como i foi escolhido de forma a $\{c \in C | \pi_i(c) \neq 0\}$ ter cardinalidade mínima, então C_i é maximal no conjunto $\{C_i : i = 1, \cdots, n\}$. No entanto, $\varphi^{-1}(D_j)$ contém C_i e está contido em C_k, o que é um absurdo. Assim, podemos concluir que $\varphi(C_i) = D_j$. Aplicando agora o teorema do isomorfismo às restrições dos homomorfismos π_i e π_j a C e a D, respetivamente, temos,

$$\pi_i(C) \simeq \frac{C}{C_i} \overset{\varphi}{\simeq} \frac{D}{D_j} \simeq \pi_j(D)$$

Em que o isomorfismo $\psi : \pi_i(C) \to \pi_j(D)$ é dado por

$$\psi(\pi_i(c)) = \pi_j(\varphi(c)), \forall c \in C$$

$$\begin{array}{ccc} C & \xrightarrow{\pi_i} & \pi_i(C) \\ \downarrow{\scriptstyle \varphi} & & \vdots{\scriptstyle \psi} \\ D & \xrightarrow{\pi_j} & \pi_j(D) \end{array}$$

Relembremos que ${}_RR$ é injetivo porque é de Frobenius. Assim, temos, $\pi_i(C)$ ideal de R, $\sigma_i : \pi_i(C) \to R$, a inclusão de $\pi_i(C)$ em R e $f : \pi_i(C) \to R$, tal que $f = \sigma_j \circ \psi$, onde σ_j é a inclusão de $\pi_j(C)$ em R. Logo, tendo em conta que f é um monorfismo pois é a composição de dois monorfismos, pelo lema 3.7 existe um automorfismo $h : R \to R$ tal que $h \circ \sigma_i = f = \sigma_j \circ \psi$.

$$\begin{array}{ccc} \pi_i(C) & \xhookrightarrow{\sigma_i} & {}_RR \\ & \searrow^{f} & \vdots{\scriptstyle h} \\ & & {}_RR \end{array}$$

Pela nota 3.8 temos que existe $u \in R^*$ tal que $h(r) = ru, \forall r \in R$. Ou seja, $\forall c \in C$:

$$\pi_i(c)u = h(\sigma_i(\pi_i(c))) = \sigma_j(\psi(\pi_i(c))) = \pi_j(\varphi(c)).$$

Considerando agora os códigos C' e D' que resultam de C e D após se "retirar"a i-ésima e a j-ésima coordenada, respetivamente, e notando que φ induz uma isometria homogénea entre os códigos resultantes. Podemos aplicar novamente o mesmo raciocínio e continuar assim até se esgotarem as coordenadas, obtendo assim um conjunto $\{u_1, \cdots, u_n\}$ de unidades de R e uma permutação de S_n, ρ, tal que $\varphi(c_i, \cdots, c_n) = (c_{\rho(1)}u_1, \cdots, c_{\rho(n)}u_n)$, que é claramente uma restrição de uma transformação monomial.

Se C possuir coordenadas nulas, então $D = \varphi(C)$ possui o mesmo número de coordenadas nulas pelo lema 4.9. Podemos então retirar as coordenadas nulas a ambos os códigos, obtendo os códigos C' e D' de comprimento $m \leq n$. Notando novamente que φ induz uma isometria homogénea, φ', entre estes dois códigos, pelo que acabamos de ver existe um conjunto $\{u_1, \cdots, u_m\}$ de unidades de R e $\rho \in S_m$ tais que $\varphi'(c'_i, \cdots, c'_m) = (c'_{\rho(1)}u_1, \cdots, c'_{\rho(m)}u_m)$. Logo se i-ésima coordenada de C é não nula, então seja j a coordenada de C' que lhe corresponde, temos $\pi_i(\varphi(c)) = \pi_j(\varphi')$. Se i for uma coordenada nula $\pi_i(\varphi(c)) =$. Assim, φ continua a ser a restrição de uma transformação monomial. □

Temos então finalmente,

Teorema 4.16. *Seja R um anel de Frobenius finito, $C \leq R^n$ um R-código e $\varphi : C \to R^n$ um homomorfismo linear esquerdo que preserva o peso de Hamming. Então φ pode ser estendido a uma transformação monomial esquerda de R^n.*

Demonstração. Um homomorfismo R-linear à esquerda que preserva o peso de Hamming é uma isometria de Hamming, que por 4.14 é uma isometria homogénea injetiva. Logo, pelo teorema 4.15 é restrição de uma transformação linear.

Da mesma forma podemos ver que o recíproco se verifica. Ou seja, se um homomorfismo R-linear à esquerda que preserva os pesos, φ, for restrição de uma tranformação monomial, então por 4.15 φ é uma isometria homogénea e por 4.14 é uma isometria de Hamming, ou seja preserva o peso de Hamming. □

4.4 Uma Demonstração Algébrica

Utilizando agora os resultados vistos no capítulo 3 e fazendo uso de algumas propriedades do dual do código C, podemos novamente demonstrar o teorema de extensão para anéis de Frobenius.

Teorema 4.17. *Seja R um anel de Frobenius finito, $C \leq R^n$ um R-código direito e $\varphi : C \to R^n$ um homomorfismo R-linear direito que preserva o peso de Hamming. Então φ pode ser estendido a uma transformação monomial de R^n.*

Demonstração. Seja $\mu : C \to R^n$ a inclusão de C em R^n e $\lambda : C \to R^n$ definida por $\lambda = f \circ \mu$. Considere-se os elementos do dual de C, $\lambda_1, \cdots, \lambda_n, \mu_1, \cdots, \mu_n \in Hom_R(C, R)$ tais que $\lambda_i(x) = \pi_i(\lambda(x))$ e $\mu_i(x) = \pi_i(\mu(x)), \forall x \in C$.

Como φ preserva o peso de Hamming vamos ter,

$$w_H(\lambda(x)) = w_H(\varphi \circ \mu(x)) = w_H(\mu(x)).$$

Assim, pela proposição 1.8 temos agora

$$\begin{aligned}\sum_{i=1}^{n}\sum_{\pi\in\widehat{R}} \pi(\lambda_i(x)) &= |R| \cdot (n - w_H(\lambda(x))) \\ &= |R| \cdot (n - w_H(\mu(x))) = \sum_{j=1}^{n}\sum_{\psi\in\widehat{R}} \pi(\mu_j(x)), \quad \forall x \in C\end{aligned}$$

Como R é um anel de Frobenius possui um caractere gerador, χ, logo podemos reescrever a equação anterior da seguinte forma:

$$\sum_{i=1}^{n}\sum_{s\in R} \chi^s \circ \lambda_i = \sum_{j=1}^{n}\sum_{r\in R} \chi^r \circ \mu_i \tag{4.3}$$

Note-se que $\chi^s \circ \lambda_i$ e $\chi^r \circ \mu_j$ são homomorfismos de C em $\mathbb{C}^*$, ou seja, são caracteres de C, $\forall s, r \in R, i, j = 1, \cdots, n$. Além disso, relembrando que $Hom_R(C, R)$ é um R-módulo, o conjunto $\{Rf : Hom_R(C, R)\}$ dos submódulos cíclicos de $Hom_R(C, R)$ é um c.p.o para a inclusão. Logo, de forma análoga ao lema 4.3, seja $f \in Hom_R(C, R)$, $R^*f = \{rf : r \in R^*\}$ é o conjunto de todos os geradores de Rf.

Considere-se ainda $S = \{\lambda_1, \cdots, \lambda_n, \mu_1, \cdots, \mu_n\}$ subconjunto de $Hom_R(C, R)$ e escolhamos um elemento maximal de S relativamente à ordem parcial de $\{Rf : Hom_R(C, R)\}$, digamos, sem perda de generalidade, λ_1. Pela proposição 1.7 os caracteres de C são linearmente independentes. Ou seja, sejam $z_1, \cdots, z_m \in \mathbb{C}^*$ e $\pi_1, \cdots, \pi_m \in \widehat{C}$ distintos, tais que $z_1\pi_1(x) + \cdots + z_m\pi_m(x) = 0, \forall x \in C$, então $z_1 = \cdots = z_m = 0$. Mas pela equação 4.3 temos

$$\sum_{i=1}^{n}\sum_{s\in R} 1 \cdot \chi^s \circ \lambda_i - \sum_{j=1}^{n}\sum_{t\in R} 1 \cdot \chi^t \circ \mu_i = 0$$

Logo, os caracteres não podem ser todos distintos e por isso $\exists t \in R$ e μ_j tais que

$$\chi^1 \circ \lambda_1 = \chi^t \circ \mu_{\sigma(1)} \Leftrightarrow \chi \circ \lambda_1 = \chi \circ t\mu_{\sigma(1)}$$

com $j = \sigma(1)$.

Pela proposição 3.12 temos que a aplicação $f : Hom_R(M, R) \to \widehat{M}$, dada por $f(\lambda) = \chi \circ \lambda$ é um homomorfismo injetivo de grupos abelianos. Ou seja $\lambda_1 = t\mu_{\sigma(1)}$. Mas então $R\lambda_1 \leq R\mu_{\sigma(1)}$, logo, como λ_1 é maximal, isso significa que $R\lambda_1 = R\mu_{\sigma(1)}$, ou seja, $\exists u_1 \in R^* : \lambda_1 = u_1\mu_{\sigma(1)}$.

Vamos ter então

$$\sum_{s\in R}\chi^s\circ\lambda_1=\sum_{s\in R}\chi^s\circ u_1\mu_{\sigma(1)}=\sum_{s\in R}\chi^{su_1}\circ\mu_{\sigma(1)}=\sum_{t\in R}\chi^t\circ\mu_{\sigma(1)}$$

a última igualdade deve-se apenas a uma reindexação dos índices, que é possível pois u_1 é uma unidade.

Podemos então reduzir o tamanho das somas exteriores de cada um dos membros de 4.3 em 1. Procedendo de igual forma até se esgotarem os elementos de S em 4.3 obtemos uma permutação $\sigma\in S_n$ e unidades $u_1,\cdots,u_n\in R^*$ tais que $\lambda_i=u_i\mu_{\sigma(i)}$. Relembrando que μ é a função identidade, ficamos finalmente com

$$\begin{aligned}\varphi(x_1,\cdots,x_n)=\varphi(x)=\varphi(\mu(x))=\lambda(x)&=(\lambda_1(x),\cdots,\lambda_n(x))\\&=(u_1\mu_{\sigma(1)}(x),\cdots,u_n\mu_{\sigma(n)}(x))=(u_1x_{\sigma(1)},\cdots,u_nx_{\sigma(n)})\end{aligned}$$

Logo, f é restrição de uma transformação monomial direita. □

Capítulo 5
Notas Finais

Depois de feitas duas demonstrações do Teorema da Extensão de MacWilliams sobre anéis de Frobenius, a primeira usando uma abordagem combinatória e a segunda uma abordagem algébrica, que se encontram nos subcapítulos 4.3 e 4.4, respetivamente, é normal que o leitor se questione se é possível que o Teorema da Extensão seja válido para uma classe maior de anéis, como por exemplo para anéis Quase-Frobenius. Porém, repare-se que a ciclicidade do socle do anel foi indispensável para a demonstração combinatória do teorema. Além disso, apesar de não ter sido exposto nesta dissertação, o leitor pode consultar a demonstração do teorema 3.4 em [15] e concluir que o teorema não é válido para anéis Quase-Frobenius.

De forma a tentar responder a esta questão, no artigo de M. Greferath e de S. Schmidt, [4], no qual se baseou a demonstração combinatória do teorema, é apresentado um exemplo de um anel quase Frobenius para o qual o Teorema da Extensão não é válido. Mais tarde J. Wood, depois de publicar "Duality for modules over finite rings and application on coding theory", [15], artigo no qual se baseou a demonstração algébrica do Teorema da Extensão, publicou ainda um outro artigo, [16]. Neste demonstra que se R é um anel finito para o qual o Teorema da Extensão de MacWilliams é válido, então este tem necessariamente de ser de Frobenius. Demonstração esta que se baseia numa outra que é apresentada em um artigo de Hai Q. Dinh e S. R. López-Permouth, [2], onde é demonstrado o mesmo resultado. Fica assim encerrada a questão de para que anéis finitos é válido o Teorema da Extensão de MacWilliams.

Resta apenas saber se o Teorema da Extensão de MacWilliams é válido para anéis infinitos e se sim para que classe destes anéis. Para dar resposta a esta última questão F. M. Schneider e J. Zumbrägel publicaram um artigo no ano passado, em 2017, com o título "MacWilliams' Extension Theorem for Infinite Rings", [12], que convidamos o leitor interessado a ler.

Bibliografia

[1] Kenneth Bogart, Don Goldberg, and Jean Gordon. An elementary proof of the MacWilliams theorem on equivalence of codes. *Information and Control*, (37), 1978.

[2] H. Q. Dinh and S. R. López-Permouth. On the equivalence of codes over rings and modules. *Finite Fields and Their Applications*, (10):615–625, 2004.

[3] Rui Loja Fernandes and Manuel Ricou. *Introdução à Álgebra*. IST Press, second edition, 2004.

[4] M. Greferath and S. E. Schmidt. Finite ring combinatorics and MacWilliams equivalence theorem. *Journal of Combinatorial Theory*, (92):17–28, 2000.

[5] A. R. Hammons, P. V. Kumas, A. R. Calderbank, N. J. A. Sloane, and P. Sole. The $\mathbb{Z}_4$-linearity of kerdock, preparata, goethals, and related codes. *IEEE Trans. Inform. Theory*, (40):301–319, 1994.

[6] T. Y. Lam. *Lectures om Modules and Rings*. Springer, 1999.

[7] T. Y. Lam. *A First Course in Noncommutative Rings*. Springer, second edition, 2001.

[8] T. Y. Lam. *Exercises in Classical Ring Theory*. Springer, second edition, 2003.

[9] S. Ling and C. Xing. *Coding Theory a First Course*. Cambridge University Press, 2004.

[10] Joseph Rotman. *Galois Theory*. Springer, second edition, 1998.

[11] L. H. Rowen. *Ring Theory*. Academic Press, student edition, 1991.

[12] F. M. Schneider and J. Zumbrägel. MacWilliams' Extension Theorem for infinite rings. *to appear Proc. Amer. Math. Soc*, 2017.

[13] Jean-Pierre Serre. *A Course in Arithmetic*. Springer, first edition, 1973.

[14] R. P. Stanley. *Enumerative Combinatorics: Volume 1.* Cambridge University Press, second edition, 2011.

[15] J. A. Wood. Duality for modules over finite rings and applications to coding theory. *American Journal of Mathematics*, 121(3), 1999.

[16] J. A. Wood. Code equivalence characterizes finite frobenius rings. *Proceedings of the American Mathematical Society*, 136(2):699–706, 2007.

Anexo A
Anexo

A.1 Teorema de Bass

A.1.1 O radical de um anel

De forma a provar o Teorema de de Bass enunciado no capítulo 1 vamos primeiro enunciar alguns resultados sobre o radical de um anel e sobre os submódulos de um módulo quociente.

Lema A.1. *Seja R um anel, as seguintes afirmações são equivalentes:*

1. $y \in rad(R)$.
2. $1 - xy$ *é invertível para qualquer* $x \in R$.

Demonstração. Ver [6, Lemma 4.3]. □

Proposição A.2. *Seja R um anel, M um R-módulo esquerdo e $N \leq M$. Então existe uma bijeção entre o conjunto dos submódulos do módulo quociente M/N e o conjunto dos submódulos de M que contêm N.*

Demonstração. Seja $\pi : M \to M/N$ o homomorfismo canónico, definido por $\pi(m) = m + N, \forall m \in M$. A bijeção do enunciado é a função que envia um submódulo de M que contém N, L, em $\pi(L)$.

Dado qualquer submódulo L de M que contém N, podemos identificar L/N com o subconjunto $\pi(L) := \{m + N : m \in L\}$. Pelas propriedades dos homomorfismos temos que $\pi(L)$ é um submódulo de M/N. Seja agora X submódulo de M/N, novamente pelas propriedades dos homomorfismos, $\pi^{-1}(X) = \{m \in M : m + N \in X\}$ é um submódulo de M. Este submódulo contém N uma vez que $N = \ker(\pi)$. Logo a bijeção está bem definida e falta apenas ver que é de facto bijetiva.

Como π é um homomorfismo sobrejetivo temos que para qualquer X submódulo de M/N, $\pi(\pi^{-1}(X)) = X$, logo a bijeção é sobrejetiva.

Sejam agora $L_1, l_2 \leq M$ que contêm N tais que $\pi(L_1) = \pi(L_2)$, então para qualquer $x \in L_1$ existe $y \in L_2$ tal que $x + N = y + N$, ou seja, $x = y + n, n \in \mathbb{N}$. Como n também pertence a L_2 temos que $x \in L_2$, logo $L_1 \subseteq L_2$. Analogamente obtemos também que $L_2 \subseteq L_1$. Assim $L_1 = L_2$ e a nossa bijeção é também injetiva. □

Um anel R diz-se Jacobson semisimples (ou J-semisimples) se $rad({}_RR) = \{0\}$.

Teorema A.3. *Seja R um anel, as seguintes condições são equivalentes:*

- *R é semisimples;*
- *R é J-semisimples e artiniano à esquerda.*

Demonstração. Ver [6, Theorem 4.14]. □

Proposição A.4. *Seja R um anel. Se R é artiniano à esquerda (resp. à direita), então $R/rad(R)$ é artiniano à esquerda (resp. à direita).*

Demonstração. Ver [6, Proposition 1.20]. □

Lema A.5. *Seja R um anel e $I \leq R$ ideal bilateral tal que $I \subseteq rad(R)$, então*

$$rad(R/I) = rad(R)/I$$

.

Demonstração. Ver [11, Proposition 2.51']. □

Corolário A.6. *Seja R um anel, então $R/rad(R)$ é J-semisimples.*

Demonstração. O $rad(R)$ é um ideal de R, logo pelo lema A.5

$$rad(R/rad(R)) = rad(R)/rad(R) = \{0\}.$$

Assim dado R qualquer anel, $R/rad(R)$ é J-semisimples. □

Corolário A.7. *Seja R um anel artiniano à esquerda, então $R/rad(R)$ é semisimples.*

Demonstração. Pela proposição A.4 se R é artiniano à esquerda, então $R/rad(R)$ também é artiniano á esquerda. Pelo corolário A.6 $R/rad(R)$ é J-semisimples. Finalmente, pelo teorema A.3 temos que $R/rad(R)$ é semisimples. □

Nota A.8. *Num anel unitário, R, todo o ideal próprio, $I \leq R$ está contido num ideal maximal ([11, pág. 9]).*

Lema A.9. *Seja R um anel finito, $L \leq R$ ideal esquerdo tal que $R = L + rad(R)$, então $R = L$.*

Demonstração. Seja R um anel finito e $L \leq R$ ideal esquerdo nas condições do enunciado. Suponhamos que $L \neq R$, como R é unitário, L tem de estar contido num ideal próprio maximal J, pela nota A.8. Por definição de $rad(R)$, $rad(R) \leq J$, e então $L + rad(R) \leq J < R$. Absurdo! Logo $L = R$. □

Nota A.10. *Se $R = Ra + L + rad(R)$, para $a \in R$ e $L \leq R$ esquerdo, podemos concluir que $R = Ra + L$.*

A.1.2 Demonstração do Teorema de Bass

Vamos agora começar a demonstrar o Teorema de Bass. Iremos dividir a sua demonstração em vários lemas e corolários e se a condição do Teorema de Bass for válida para um dado anel R dizemos que o Teorema é válido para esse anel.

Proposição A.11. *Seja R um anel. Então $u \in R$ é uma unidade do anel se e só se $u + rad(R)$ é uma unidade do anel quociente $R/rad(R)$.*

Demonstração. Sejam $u \in R^*$ e $\overline{u} = u + rad(R)$. Supondo que u é uma unidade do anel $\exists v \in R : uv = 1 = vu$. Assim, seja $\overline{v} = v + rad(R)$, vamos ter

$$\overline{u} \cdot \overline{v} = (u + rad(R))(v + rad(R)) = 1 + rad(R) = (v + rad(R))(u + rad(R)) = \overline{v} \cdot \overline{u}.$$

Logo $\overline{u}$ é uma unidade de $R/rad(R)$.

Reciprocamente, suponhamos que $\overline{u} = u + rad(R)$ é uma unidade de $R/rad(R)$. Então $\exists \overline{v} = v + rad(R) \in R/rad(R)$ tal que

$$\overline{u} \cdot \overline{v} = uv + rad(R) = 1 + rad(R) = vv + rad(R) = \overline{v} \cdot \overline{u}.$$

Assim, $1 - uv \in rad(R)$ e $1 - vu \in rad(R)$.

Mas então, pelo lema A.1 os elementos $1 - (1 - uv)$ e $1 - (1 - vu)$ são invertíveis. Ou seja, os elementos uv e vu são invertíveis. Logo, $\exists w, z \in R$:

$$wuv = 1 = uvw \wedge zvu = 1 = vuz.$$

Ou seja, u tem inverso esquerdo zv e inverso direito vw. Facilmente se verifica que $zv = vw$:

$$zv = zv \cdot uvw = zvu \cdot vw = vw.$$

Logo, u é unidade de R. □

Lema A.12. *O Teorema de Bass é válido para um anel R se e só se é válido para $R/rad(R)$.*

Demonstração. Suponhamos que o Teorema é válido para um anel R e note-se que qualquer ideal esquerdo de $R/rad(R)$ é da forma $L/rad(R)$ pela proposição A.2, onde L é ideal esquerdo de R que contém $rad(R)$. Seja então $\overline{a} = a + rad(R) \in R/rad(R)$ e $L/rad(R) \leq R/rad(R)$ esquerdo, tais que $R/rad(R) = (R/rad(R))\overline{a} + L/rad(R)$. Logo $R = Ra + L + rad(R)$ e pelo lema A.9 $R = Ra + L$, e por hipótese $\exists u \in R^* : u = a + l$, com $l \in L$. Pela proposição A.11, $\overline{u} = u + rad(R)$ é uma unidade de $R/rad(R)$ e $u+rad(R) = a+l+rad(R) = a+rad(R)+l+rad(R)$, ou seja, $u+rad(R) \in \overline{a}+L/rad(R)$. Logo o Teorema de Bass também é válido para $R/rad(R)$.

Reciprocamente, suponhamos que é válido o Teorema de Bass em $R/rad(R)$. Seja $a \in R$ e $L \leq R$ ideal esquerdo tal que $R = Ra + L$, então

$$R/rad(R) = (R/rad(R))\overline{a} + L/rad(R).$$

Onde $\overline{a} = a + rad(R)$. Novamente, por hipótese, $\exists \overline{u} = u + rad(R) \in (R/rad(R))^*$ tal que $\overline{u} = \overline{a} + L/rad(R)$. Pela proposição A.11 $u \in R^*$. Além disso $u = a + l + r$, para $l \in L$ e $r \in rad(R)$. Mas como u é unidade, $\exists v \in R : uv = 1 = vu$. Temos então,

$$1 = vu = va + vl + vr \Leftrightarrow 1 - vr = va + vl$$

Pelo lema A.1 $1 - vr$ é invertível, logo, $u(1 - vr) = a + l$ é também invertível porque R^* é fechado para a multiplicação. Logo o Teorema de Bass é válido para R. □

Lema A.13. *Seja $R = A \times B$ um produto de anéis. Se o Teorema de Bass é válido em A e em B, então é válido em R.*

Demonstração. Suponhamos então que o Teorema de Bass é válido para dois anéis A e B. Considere-se $R = A \times B$, e os elementos $a = (1, 0)$ e $b = (0, 1)$. Um ideal esquerdo de R é da forma $L = L_A a + L_B b$, onde L_A é ideal esquerdo de A e L_B é ideal esquerdo de

B. Seja, então $\alpha = (\alpha_1, \alpha_2) \in R$ e $L \leq R$ ideal esquerdo tais que $R = R\alpha + L$. Temos,

$$R = A \times B = (A\alpha_1 + L_A, B\alpha_2 + L_B),$$

ou seja, $A = A\alpha_1 + L_A$ e $B = B\alpha_2 + L_B$. Mas, por hipótese $\exists u_A \in A^* : u_A \in \alpha_1 + L_A$ e $\exists u_B \in B^* : u_B \in \alpha_2 + L_B$. Assim $(u_A, u_B) \in R^*$ e $(u_A, u_B) \in \alpha + L$. Logo o Teorema de Bass é válido para R. □

Para demonstrar o próximo lema essencial para a demonstração do Teorema de Bass vamos ainda necessitar do seguinte resultado:

Lema A.14. *Seja $R = End(V_D)$, onde V é um espaço vetorial de dimensão finita sobre D. Considere-se $I \leq R$ ideal esquerdo e $W \leq V$, e defina-se os seguintes conjuntos*

$$ann(W) := \{r \in R : rW = 0\} \text{ e } ann(I) := \{v \in V : Iv = 0\}.$$

Então

$$ann(ann(I)) = I.$$

Demonstração. Ver [8, Ex. 11.15]. □

Lema A.15. *O Teorema de Bass é válido para qualquer anel de matrizes $M_n(D)$, onde D é um anel de divisão.*

Demonstração. Seja $A = M_n(D)$ onde D é um anel de divisão, então $A = End(V)$, onde V é um espaço vetorial de dimensão n sobre D. Considere-se $B \leq A$, ideal esquerdo, então $W = \{v \in V : Bv = 0\}$ é um subespaço de V. Assim, pelo lema A.14, $B = ann_A(W) := \{f \in A : f(w) = 0, \forall w \in W\}$.

Seja então $g \in A$ tal que $A = Ag + B$, temos que $g|_W$ é um isomorfismo, pois W é finito e se $g(w) = 0$, para $w \in W$, então seja $b \in B$ e $r \in R : 1 = rg + b$, ficamos com $w = (rg + b)w = b(w) = 0$.

Considere-se agora $f \in A$ um D-automorfismo que restringido a W é igual a g, ou seja $f(w) = g(w), \forall w \in W$. Então, claramente, $f - g \in ann(W) = B$, ou seja, $f \in g + B$. Logo o Teorema de Bass é válido em A.

Falta apenas ver que de facto existe tal automorfismo f. Como g restringido a W é um isomorfismo, W e $g(W)$ são subespaços de V isomorfos, logo têm a mesma dimensão. Sejam então U e $U' \leq V$, tais que $U \oplus W = V$ e $U' \oplus g(W) = V$. Sejam $b_1, \cdots, b_m$ uma base de U e $c_1, \cdots, c_m$, uma base de U', podemos definir o isomorfismo:

$$h : U \to U'$$

$$b_j \mapsto c_j$$

Assim, basta considerarmos $f : V \to V$ como sendo o automorfismo que envia elementos de W em $g(W)$, elementos de U em $h(u)$. Ou seja, como os elementos de $v \in V$, podem ser escritos de forma única como $v = w + u$, para $w \in W, u \in U$, $f(w+u) = g(w) + h(u)$. □

Corolário A.16. *O Teorema de Bass é válido para qualquer anel semisimples.*

Demonstração. Se R é um anel semisimples então

$$R = M_{n_1}(D_1) \times \cdots \times M_{n_n}(D_n)$$

para $D_1, \cdots, D_n$ anéis de divisão. Assim, como o Teorema de Bass e é válido em cada um dos anéis de matrizes da decomposição de R pelo lema A.15 e pelo lema A.13 é válido para o produto deles, ou seja, para R. □

Vamos então finalizar a demonstração.

Demonstração Teorema de Bass. Como R é artiniano, $R/rad(R)$ é semisimples, logo o Teorema é válido, mas então pelo lema A.12, o Teorema de Bass também é válido para R. □

Nota A.17. *Seja R um anel finito, $a \in R$ e $B \leq R$ ideal direito, tais que, $R = aR + B$. Então considere-se o anel oposto R^{op}, ou seja, o anel R com a operação $\cdot_{op}$ tal que $\forall x, y \in R^{op}, x \cdot_{op} y = y \cdot x$. Temos $R^{op} = R^{op}a + B$, onde $B \leq R^{op}$ é ideal esquerdo. Logo, $\exists u \in R^{op*} : u = a + b, b \in B$.*

Mas como u é unidade, $\exists v \in R^{op*} : u \cdot_{op} v = 1 = v \cdot_{op} u$, ou seja, $v \cdot u = 1 = u \cdot v$, logo também é unidade em R.

Assim se o Teorema de Bass é válido para um anel em R, então também a sua versão para ideais direitos é válida.

A.2 Módulos

Neste subcapítulo vão ser demonstrados alguns dos resultados que foram apresentados no capítulo 1 referentes a módulos. Estes resultados são o lema 1.1, o lema 1.5 e o lema 1.4.

Lema A.18. *Seja M um módulo esquerdo finito semisimples. Então qualquer submódulo N de M tem um complemento direto em M.*

Demonstração. Seja M um módulo esquerdo semisimples e N um seu submódulo. Podemos escolher um outro submódulo V de M maximal em relação à condição $N \cap V = \{0\}$.

Note-se que este submódulo maximal existe de facto porque M é finito. Se V_1 satisfaz $N \cap V_1 = \{0\}$, mas não é maximal em relação a esta propriedade, então existe um V_2 que contém V_1 e satisfaz também $N \cap V_2 = \{0\}$. Se V_2 não for maximal, então podemos repetir o raciocínio, obtendo uma cadeia $V_1 \subseteq V_2 \subseteq \ldots$ de submódulos V_i que satisfazem $N \cap V_i = \{0\}$. No entanto, este processo tem de parar porque M é finito. Logo existe de facto um submódulo V que é maximal relativamente à condição $N \cap V = \{0\}$.

Seja agora S um submódulo simples de M. Se $(V + S) \cap N = \{0\}$ então pela maximalidade de V, $V + S = V$, ou seja, $S \subseteq V$. Se $(V + S) \cap N \neq \{0\}$ então existe $0 \neq x \in (V + S) \cap N$ e $v \in V, s \in S$ tais que $x = v + s$. Como $N \cap V = \{0\}$, $s \neq 0$ temos $s = x - v \in V + U$ e consequentemente $S = Rs \subseteq V + U$.

Como M é semisimples, $M = \mathrm{Soc}(M)$, ou seja, M é soma de submódulos simples. Como acabamos de ver que todo o submódulo simples de M está contido em $N + V$ podemos concluir assim que $N + V = M$. □

Lema A.19. *Seja M um módulo esquerdo finito tal que* $\mathrm{soc}(M)$ *é cíclico e não nulo. Então qualquer submódulo de* $\mathrm{soc}(M)$ *é cíclico.*

Demonstração. Por hipótese $\mathrm{Soc}(M) = Rx$ para um elemento $x \in \mathrm{Soc}(M)$.

Seja N um submódulo de $\mathrm{Soc}(M)$, então pelo Lema A.18 existe um complemento direto V em $\mathrm{Soc}(M)$ tal que $N \oplus V = \mathrm{Soc}(M) = Rx$. Logo $x \in N + V$ e existem elementos $y \in N$ e $z \in V$ tais que $x = y + z$. Como $N \subseteq Rx$, para qualquer $n \in N$ existe um $r \in R$ tal que

$$n = rx = ry + rz \Rrightarrow n - ry = rz \in N \cap V = \{0\}.$$

Logo, $n = ry$, ou seja $N = Ry$ e por isso N é cíclico. □

Lema A.20. *Seja R um anel injetivo á esquerda, então para qualquer $a \in R$ temos*

$$r.ann_R(l.ann_R(a)) = aR$$

Demonstração. Seja $x \in l.ann_R(a)$ e $r \in R$, então $x \cdot ar = 0$. Logo $ar \in r.ann_R(l.ann_R(a))$. Logo $aR \subseteq r.ann_R(l.ann_R(a))$.

Reciprocamente, seja $x \in r.ann_R(l.ann_R(a))$, definimos o homomorfismo

$$f : Ra \to Rx$$

$$ra \mapsto rx$$

Temos que verificar se f está bem definido. Seja $r, r' \in R : ra = r'a$, então $(r - r')a = 0$, ou seja, $r - r' \in l.ann_R(a)$.

Mas como $x \in r.ann_R(l.ann_R(a))$, $(r - r')x = 0 \Leftrightarrow rx = r'x$, ou seja, $f(ra) = f(r'a)$. Assim, f está bem definida e é claramente um homomorfismo de R-módulos á esquerda. Agora, pela injectividade de R, temos que existe $f' : R \to R$ tal que $f'(ra) = f(ra) = rx$.

$$\begin{array}{ccccc} \{0\} & \longrightarrow & Ra & \xhookrightarrow{i} & R \\ & & \downarrow{\scriptstyle f} & & \vdots{\scriptstyle f'} \\ & & Rx & \xhookrightarrow{i'} & R \end{array}$$

onde $i : Ra \to R$ e $i' : Rx \to R$ são a função identidade restrita a Ra e Rx, respetivamente.

Em particular temos $x = f'(a) = af'(1)$, logo, $x \in aR$. Ou seja $r.ann_R(l.ann_R(a)) \subseteq aR$. E, finalmente $r.ann_R(l.ann_R(a)) = aR$. □

Lema A.21. *Seja L um reticulado, se L é modular, então é semimodular.*

Demonstração. Seja então L um reticulado modular e $a, b \in L$. Comecemos por notar que em qualquer reticulado temos

$$a \wedge (a \vee b) = a = a \vee (a \wedge b)$$

Suponhamos então que a e b são coberturas de $a \wedge b$, queremos mostrar que isso implica que $a \vee b$ seja cobertura de a e b.

Seja então $c \in L : a \leq c \leq a \vee b$, então

$$a \wedge b \leq c \wedge b \leq (a \vee b) \wedge b = b$$

Mas como b é cobertura de $a \wedge b$ temos de ter

$$a \wedge b = c \wedge b \text{ ou } c \wedge b = b$$

Se tivermos $a \wedge b = c \wedge b$, por $a \leq c \leq a \vee b$ temos

$$a \vee b \leq c \vee b \leq a \vee b \vee b = a \vee b$$

Logo $c \vee b = a \vee b$ e temos então,

$$c = c \wedge (c \vee b) = c \wedge (a \vee b) \overset{L \text{ modular}}{=} a \vee (c \wedge b) = a \vee (a \wedge b) = a$$

Suponhamos agora que a condição que se verifica é a segunda, ou seja, $c \wedge b = b$. Mas

então $b \leq c$, mas de cima temos que $a \leq c$, logo $a \vee b \leq c$. Mas, como também $c \leq a \vee b$, então $a \vee b = c$ e por isso $a \vee b$ é cobertura de a.

Analogamente se vê que $a \vee b$ é cobertura de b.

Logo, L é semimodular. □

A.3 Caracteres

Dos resultados apresentados sobre caracteres no capítulo Noções Básicas, vamos apenas demonstrar um, o lema 1.6.

Lema A.22. *Seja G um grupo abeliano e $\widehat{G}$ o seu grupo de caracteres, então $|G| = \left|\widehat{G}\right|$.*

Demonstração. De forma a simplificar a demonstração vamos começar por demonstrar primeiro as duas seguintes proposições:

(1) Sejam G e H grupos, então $\widehat{G \times H} \simeq \widehat{G} \times \widehat{H}$.

(2) Seja $G = \langle x \rangle$ um grupo cíclico de ordem n, então

$$n = |G| = \left|\widehat{G}\right|.$$

(1) Considere-se os homomorfismos de grupos $f_1 : G \to G \times H$ e $f_2 : H \to G \times H$, definidos por $f_1(g) = (g, 1_H), \forall g \in G$ e $f_2(h) = (1_G, h), \forall h \in H$, onde 1_H e 1_G são os elementos neutros de H e G respetivamente.

Podemos então definir a seguinte aplicação:

$$\begin{aligned} \Psi : \widehat{G \times H} &\to \widehat{G} \times \widehat{H} \\ \varphi &\mapsto (\varphi \circ f_1, \varphi \circ f_2) \end{aligned}$$

Precisamos agora de mostrar que Ψ é de facto um homomorfismo de grupos e que é bijetivo. Começamos por ver que é homomorfismo, ou seja, que $\forall \varphi, \psi \in \widehat{G \times H}$ temos $\Psi(\varphi\psi) = \Psi(\varphi)\Psi(\psi)$ e que Ψ está de facto bem definido.

$$\begin{aligned} \Psi(\varphi\psi)(g,h) &= ((\varphi\psi) \circ f_1(g), (\varphi\psi) \circ f_2(h)) \\ &= ((\varphi\psi)(f_1(g)), (\varphi\psi)(f_2(h))) = (\varphi(f_1(g))\psi(f_1(g)), \varphi(f_2(h))\psi(f_2(h))) \\ &= (\varphi(f_1(g)), \varphi(f_2(h)))(\psi(f_1(g)), \psi(f_2(h))) = (\Psi(\varphi)\Psi(\psi))(g,h) \end{aligned}$$

Está bem definido pois, $\varphi \circ f_i, i = 1, 2$ são homomorfismos porque resultam da composição de dois homomorfismo.

Vamos agora ver que é um isomorfismo.

É sobrejetiva pois sejam $\alpha \in \widehat{G}, \beta \in \widehat{H}$ e $\varphi \in \widehat{G \times H}$ definida por $\varphi(g,h) = \alpha(g)\beta(h)$, $\forall (g,h) \in G \times H$, então $\Psi(\varphi) = (\alpha, \beta)$. Começamos por ver que φ é de facto um homomorfismo de grupos,

$$\begin{aligned}\varphi((g_1,h_1)(g_2,h_2)) &= \alpha(g_1,g_2)\beta(h_1h_2) = \alpha(g_1)\beta(h_1)\alpha(g_2)\beta(h_2) \quad \text{(porque } \mathbb{C}^* \text{ é abeliano)} \\ &= \varphi(g_1,h_1)\varphi(g_2,h_2).\end{aligned}$$

Falta apenas ver que (α, β) é de facto imagem de φ. $\forall (g,h) \in G \times H$:

$$\begin{aligned}\Psi(\varphi)(g,h) &= (\varphi(f_1(g)), \varphi(f_2(h))) = (\varphi(g, 1_H), \varphi(1_G, h)) \\ &= (\alpha(g), \beta(h)) \qquad\qquad \text{(porque } \alpha(1_G) = 1_{\mathbb{C}} = \beta(1_H))\end{aligned}$$

Ψ é injetiva porque se $\Psi(\varphi) = (1_{\widehat{G}}, 1_{\widehat{H}})$, então

$$\Psi(\varphi)(g,h) = (\varphi(f_1(g)), \varphi(f_2(h))) = (1,1), \forall (g,h) \in G \times H \tag{A.1}$$

$$\varphi(g,h) = \varphi(g, 1_H) \cdot \varphi(1_G, h) \overset{A.1}{=} 1$$

Logo, $\varphi = 1_{\widehat{G \times H}}$.

Concluímos então que $\widehat{G \times H} \simeq \widehat{G} \times \widehat{H}$

(2) Suponhamos que $G = \langle x \rangle$ é um grupo cíclico gerado por x de ordem n. Considere-se o conjunto

$$\Omega_n = \{\omega \in \mathbb{C} : \omega^n = 1\} = \{\epsilon^{\frac{2\pi i}{n}k} : k = 0, 1, \cdots, n-1\} \subseteq \mathbb{C}$$

e a aplicação

$$\begin{aligned}\Psi : \Omega_n &\to \widehat{G} \\ \omega &\mapsto \Psi_\omega\end{aligned}$$

Onde $\Psi_\omega : G \to \mathbb{C}^*$ é definido por $\Psi_\omega(x^k) = \omega^k, \forall k = 0, 1, \cdots, n-1$.

Novamente precisamos de ver que Ψ é um homomorfismo bijetivo. Comecemos por ver

que é homomorfismo, $\forall k = 0, 1, \cdots, n-1$:

$$\Psi(\omega_1\omega_2)(x^k) = \Psi_{\omega_1\omega_2}(x^k) = (\omega_1\omega_2)^k = \omega_1^k\omega_2^k = \Psi_{\omega_1}(x^k)\Psi_{\omega_2}(x^k) = \Psi(\omega_1)(x^k)\Psi(\omega_2)(x^k)$$

Para vermos se Ψ está bem definido precisamos de verificar se $\Psi_\omega \in \widehat{G}$. Ou seja, que Ψ_ω é homomorfismo

$$\Psi_\omega(x^k x^l) = \Psi_\omega(x^{k+l}) = \omega^{k+l} = \omega^k\omega^l = \Psi_\omega(x^k)\Psi_\omega(x^l)$$

Logo preserva a operação e $\Psi_\omega(1) = \Psi_\omega(x^n) = \omega^n = 1$. Concluímos assim que Ψ está bem definido.

Vamos agora ver que é isomorfismo. Seja $\varphi \in \widehat{G}$, então $1 = \varphi(1) = \varphi(x^n) = (\varphi(x))^n$. Ou seja, $\varphi(x) \in \Omega_n$. Logo $\varphi(x^k) = (\varphi(x))^k = \Psi_{\varphi(x)}(x^k)$, podemos então concluir que $\Psi(\varphi(x)) = \Psi_{\varphi(x)} = \varphi$. Assim Ψ é sobrejetiva.

Se $\omega \in \ker(\Psi)$, então $\Psi_\omega = 1_{\widehat{G}}$, ou seja, $\forall k = 0, 1, \cdots, n-1, \Psi_\omega(x^k) = \omega^k = 1$. Em particular para $k = 1$, ou seja, $\omega = 1$. Logo Ψ é injetiva.

Temos então que $\Omega_n \simeq \widehat{G}$, logo $n = \left|\widehat{G}\right|$.

Falta então provar o resultado principal. Como é sabido se G é um grupo abeliano finito então,

$$G \simeq C_1 \times C_2 \times \cdots \times C_m$$

onde os $C_i's$ são grupos abelianos cíclicos finitos. Assim, por (1) temos

$$\left|\widehat{G}\right| = \left|\widehat{C_1}\right| \left|\widehat{C_2}\right| \cdots \left|\widehat{C_m}\right|$$

Por (2) temos agora

$$\left|\widehat{C_1}\right| \left|\widehat{C_2}\right| \cdots \left|\widehat{C_m}\right| = |C_1|\,|C_2| \cdots |C_m| = |G|\,.$$

□

A.4 Álgebra Incidente

Relembremos que um intervalo de um c.p.o, $(P, \leq)$ é um subconjunto da forma

$$[x, y] := \{z \in P : x \leq z \wedge z \leq y\}$$

onde $x, y \in P$ são elementos tais que $x \leq y$. Vamos denotar por $Int(P)$ o conjunto dos intervalos de P.

Um c.p.o é chamado de localmente finito se todos os intervalos $[x, y]$ são finitos.

Podemos agora definir a Álgebra Incidente $\mathcal{A} = \mathcal{F}(Int(P), \mathbb{R})$ de P sobre o anel dos números reais $\mathbb{R}$ como o conjunto das funções de $Int(P)$ em $\mathbb{R}$. $\mathcal{A}$ é um espaço vetorial sobre $\mathbb{R}$ com a adição usual defina por $(f + g)(I) = f(I) + g(I)$ e multiplicação escalar definida por $(\lambda f)(I) = \lambda f(I), \forall I \in Int(P), \forall \lambda \in \mathbb{R}$ e $f, g \in \mathcal{A}$. Para abreviar vamos usar $f(x, y) := f([x, y])$ sempre que $x \leq y$ e $f \in \mathcal{A}$.

$\mathcal{A}$ é ainda um anel associativo e unitário com multiplicação definida por

$$(f \cdot g)(x, y) := \sum_{x \leq z \leq y} f(x, z)g(z, y), \quad \forall f, g \in \mathcal{A}.$$

A função identidade do anel é $\delta \in \mathcal{A}$ defina por $\delta(x, x) = 1$ e $\delta(x, y) = 0$ para $x < y$. Podemos facilmente verificar esta afirmação, $\forall f \in \mathcal{A}$ e $\forall x, y \in P : x \leq y$:

$$(f \cdot \delta)(x, y) = \sum_{x \leq z \leq y} f(x, z)\delta(z, y) = f(x, y) = \sum_{x \leq z \leq y} \delta(x, z)f(z, y) = (\delta \cdot f)(x, y).$$

Ou seja, $f \cdot \delta = f = \delta \cdot f$.

Definimos ainda a função **zeta** como $\zeta(I) = 1, \forall I \in Int(P)$.

Esta função tem um inverso á esquerda em $\mathcal{A}$ que é definido recursivamente por $\mu_1(x, y) = -\sum_{x \leq z \leq y} \mu_1(x, z)$ se $x < y$ e $\mu_1(x, x) = 1$. A forma como esta função é definida resulta do facto de $\forall x, y \in P : x \leq y$ termos de ter $\mu_1 \cdot \zeta = \delta$. Assim,

$$0 = \delta(x, y) = (\mu_1 \cdot \zeta)(x, y) = \sum_{x \leq z \leq y} \mu_1(x, z)\zeta(z, y) = \sum_{x \leq z \leq y} \mu_1(x, z)$$

e $(\mu_1 \cdot \zeta)(x, x) = \mu_1(x, x) = \delta(x, x) = 1$.

Analogamente, **zeta** admite um inverso direito definido recursivamente por $\mu_2(x, y) = -\sum_{x \leq z \leq y} \mu(z, y)$ se $x < y$ e $\mu_2(x, x) = 1$. A forma como esta função é definida resulta do facto de $\forall x, y \in P : x \leq y$ termos de ter $\zeta \cdot \mu_2 = \delta$. Assim,

$$0 = \delta(x, y) = (\zeta \cdot \mu_2)(x, y) = \sum_{x \leq z \leq y} \zeta(x, z)\mu_2(z, y) = \sum_{x \leq z \leq y} \mu_2(z, y)$$

e $(\zeta \cdot \mu_2)(x, x) = \mu_2(x, x) = \delta(x, x) = 1$.

É fácil ver que estes dois inversos são na verdade iguais. Logo podemos falar do inverso da função **zeta**, $\mu = \mu_1$, ao qual chamamos Função de Möbius de P.

Teorema A.23 (Fórmula da Inversão de Möbius)**.** *Seja P um c.p.o localmente finito,*

tal que $\forall t \in P$ *o conjunto* $\{s \in P : s \leq t\}$ *é finito e, sejam* $g, f : P \to \mathbb{R}$ *duas funções. Então as seguinte condições são equivalentes:*

$$g(x) = \sum_{y \leq x} f(y), \quad \forall x \in P$$

se e só se

$$f(x) = \sum_{y \leq x} g(y)\mu(y, x), \quad \forall x \in P.$$

Demonstração. Considere-se o espaço vetorial das funções de P em $\mathbb{R}$, $\mathbb{R}^P$ como um $\mathcal{A}$-módulo direito. A multiplicação escalar deste módulo é dada por $\circ : \mathbb{R}^P \times \mathcal{A} \to \mathbb{R}^P$, definida por $\forall f \in \mathbb{R}^P, \alpha \in \mathcal{A}$:

$$\begin{aligned} f \circ \alpha : P &\to \mathbb{R} \\ x &\mapsto \sum_{y \leq x} f(y)\alpha(y, x) \end{aligned}$$

Facilmente se verifica que $\forall f, g \in \mathbb{R}^P, \alpha, \beta \in \mathcal{A}$ e $x \in P$ temos

$$((f + g) \circ \alpha)(x) = (f \circ \alpha)(x) + (g \circ \alpha)(x) \text{ e } (f \circ (\alpha + \beta))(x) = (f \circ \alpha)(x) + (f \circ \beta)(x).$$

Claramente temos também $f \circ \delta = f, \forall f \in \mathbb{R}^P$,

$$(f \circ \delta)(x) = \sum_{y \leq x} f(y)\delta(y, x) = f(x)\delta(x, x) = f(x), \qquad \forall x \in P.$$

Para verificar que $\mathbb{R}^P$ é de facto um $\mathcal{A}$-módulo falta apenas ver uma última propriedade: $(f \circ \alpha) \circ \beta = f \circ (\alpha \cdot \beta), \forall f \in \mathbb{R}^P, \alpha, \beta \in \mathcal{A}$. Temos assim,

$$\begin{aligned} ((f \circ \alpha) \circ \beta)(y) &= \sum_{z \leq y} (f \circ \alpha)(z)\beta(z, y) = \sum_{z \leq y} \sum_{x \leq z} f(x)\alpha(x, z)\beta(z, y) \\ &= \sum_{x \leq z \leq y} f(x)\alpha(x, z)\beta(z, y) = \sum_{x \leq y} f(x) \sum_{x \leq z \leq y} \alpha(x, z)\beta(z, y) \\ &= \sum_{x \leq y} f(x)(\alpha \cdot \beta)(x, y) = (f \circ (\alpha \cdot \beta))(y). \end{aligned}$$

Podemos finalmente provar o pretendido. Na nova notação as funções f e g do enunciado podem ser escritas da seguinte forma: $f = g \circ \mu$ e $g = f \circ \zeta$. O objetivo é então provar que $g = f \circ \zeta$ se e só se $f = g \circ \mu$ Temos então

$$g = f \circ \zeta \implies g \circ \mu = (f \circ \zeta) \circ \mu = f \circ (\zeta \cdot \mu) = f \circ \delta = f.$$

Reciprocamente

$$f = g \circ \mu \implies f \circ \zeta = (g \circ \mu) \circ \zeta = g \circ (\mu \cdot \zeta) = g \circ \delta = g.$$

□

Note-se que no nosso caso, como estamos a trabalhar com c.p.o.'s finitos, eles são necessariamente localmente finitos e a condição de $\forall t \in P$ o conjunto $\{s \in P : s \leq t\}$ é finito também se verifica. Assim, o enunciado do capítulo 4, teorema 4.1, está também correto.

Índice