Dimensão de módulos livres sobre anéis comutativos

M. Luísa Galvão
Centro de Álgebra
Universidade de Lisboa
Av. Prof. Gama Pinto 2,
1649-003 Lisboa, Portugal
e-mail: mlgalvao@ptmat.fc.ul.pt

Pedro J. Freitas
Centro de Estruturas Lineares e Combinatórias
Universidade de Lisboa
Av. Prof. Gama Pinto 2,
1649-003 Lisboa, Portugal
e-mail: pjfreitas@fc.ul.pt

Resumo: Recolhemos e comparamos neste artigo alguns resultados sobre dimensão de módulos livres; em particular, provamos a existência de dimensão de módulos livres sobre anéis comutativos, apresentando também alguns resultados relacionados com este assunto.

Abstract In this article we summarize and compare results on the dimension of free modules. We present several proofs that for modules over commutative rings dimension is well defined.

palavras-chave: módulos, anéis comutativos, dimensão, produto tensorial.

keywords: modules, commutative rings, dimension, tensor product.

1 Bases de Módulos

Neste trabalho, consideraremos sempre anéis com identidade, e módulos unitários. Os homomorfismos de anéis considerados serão também sempre unitários.

É bem sabido que, tal como nos espaços vectoriais, é possível definir em módulos o conceito de base, como conjunto de elementos do módulo, simultaneamente gerador e linearmente independente. Ora, como a estrutura de anel não satisfaz tantas propriedades como a de corpo, é de esperar que algumas propriedades das bases dos espaços vectoriais não sejam válidas em módulos. Por exemplo, é bastante simples de ver que os conjuntos geradores

minimais nem sempre são base, e o mesmo se passa com os conjuntos independentes maximais — para encontrar exemplos, basta considerar $\mathbb{Z}$ como módulo sobre si próprio.

Uma das propriedades que faz das bases um objecto tão importante em espaços vectoriais, é que todas as bases de um espaço vectorial têm a mesma cardinalidade. É isso que permite definir a dimensão de um espaço vectorial, e ter assim uma medida eficaz do seu tamanho.

Ora, supreendentemente, sucede que *as bases de um módulo livre M podem não ter todas a mesma cardinalidade.* Vamos apresentar um exemplo tirado de [Bo]. Considere-se o módulo-$\mathbb{Z}$ $\mathbb{Z}[X]$, e o anel de endomorfismos $A := \mathrm{End}_{\mathbb{Z}}\,\mathbb{Z}[X]$. O anel A, considerado como módulo-A, é finitamente gerado, pois é gerado por $\{\mathrm{id}_A\}$, que forma, por si só, uma base de A, com um só elemento. Note-se que, pelo teorema da extensão linear (que vale também em módulos), cada elemento $f \in A$ fica definido pelas suas imagens nos monómios X^n, pois estes elementos formam uma base de $\mathbb{Z}[X]$.

Definamos agora $f_1, f_2 \in A$ da seguinte forma: para todo o $n \in \mathbb{N}_0$, tomamos

$$\begin{cases} f_1(X^{2n+1}) = X^n \\ f_1(X^{2n}) = 0 \end{cases} \quad \text{e} \quad \begin{cases} f_2(X^{2n+1}) = 0 \\ f_2(X^{2n}) = X^n \end{cases}$$

e prolongamos as aplicações linearmente a todos os elementos de $\mathbb{Z}[X]$. Vamos ver que $\{f_1, f_2\}$ é base de A. Primeiro, vejamos que se trata de uma família livre: sejam $\alpha_1, \alpha_2 \in A$, $\alpha_1 f_1 + \alpha_2 f_2 \equiv 0$. Temos então que, para todo o $n \in \mathbb{N}_0$,

$$\begin{aligned} 0 &= (\alpha_1 f_1 + \alpha_2 f_2)(X^{2n+1}) \\ &= \alpha_1(f_1(X^{2n+1})) + \alpha_2(f_2(X^{2n+1})) \\ &= \alpha_1(X^n), \end{aligned}$$

e portanto $\alpha_1(p) = 0$ para todo o $p \in \mathbb{Z}[X]$ e portanto $\alpha_1 \equiv 0$. Fazendo o mesmo cálculo para X^{2n}, obteríamos $\alpha_2 \equiv 0$. Assim, a família $\{f_1, f_2\}$ é livre.

Vejamos agora que a família é geradora. Seja $f \in A = \mathrm{End}_{\mathbb{Z}}\,\mathbb{Z}[X]$, qualquer. Considerem-se então $\beta_1, \beta_2 \in A$ definidos assim: para todo o $n \in \mathbb{N}_0$,

$$\begin{aligned} \beta_1(X^n) &:= f(X^{2n+1}) \\ \beta_2(X^n) &:= f(X^{2n}), \end{aligned}$$

e prolongadas por extensão linear. Verifiquemos que $f = \beta_1 f_1 + \beta_2 f_2$: para todo o $n \in \mathbb{N}_0$,

$$\begin{aligned}(\beta_1 f_1 + \beta_2 f_2)(X^{2n+1}) &= \beta_1(f_1(X^{2n+1})) + \beta_2(f_2(X^{2n+1})) \\ &= \beta_1(X^n) + 0 \\ &= f(X^{2n+1}),\end{aligned}$$

e calculando agora $(\beta_1 f_1 + \beta_2 f_2)(X^{2n})$ do mesmo modo, veríamos que coincide com $f(X^{2n})$. Assim, e mais uma vez por linearidade, $f = \beta_1 f_1 + \beta_2 f_2$. Portanto, a família $\{f_1, f_2\}$ é também geradora, e portanto é base.

Este processo pode generalizar-se por forma a obter famílias geradoras linearmente independentes com qualquer número k de elementos, com $f_i(X^{nk+j}) = \delta_{ij} X^n$, $1 \leq i, j \leq k$, $n \in \mathbb{N}_0$. Assim, $\mathrm{End}_{\mathbb{Z}}\, \mathbb{Z}[X]$ admite bases como módulo sobre si próprio *com qualquer cardinalidade finita.*

Uma razão forte para certas propriedades das bases dos espaços vectoriais falharem em módulos, é que nestes não é válido o teorema de Steinitz. Observando a demonstração deste resultado, vemos que para que esta funcione é crucial a existência de inverso de um elemento não nulo no corpo.

No último exemplo apresentámos um módulo que admitia bases finitas de qualquer cardinalidade, mas não apresentámos nenhuma base infinita, e com razão: não é possível encontrar uma. Isto é provado no próximo resultado.

Proposição 1.1 *Seja M um módulo livre.*

1. Se M for finitamente gerado, então todas as bases de M são finitas, não necessariamente com a mesma cardinalidade.

2. Se M não for finitamente gerado, todas as bases são infinitas e têm a mesma cardinalidade.

Demonstração. 1. Seja $\{x_1, \ldots, x_n\}$ um conjunto gerador de M, módulo livre, e seja $\{e_i : i \in I\}$ uma base. Queremos provar que I é finito.

Vamos exprimir cada x_j como combinação linear da base: para $1 \leq j \leq n$, ponhamos

$$x_j = \sum_{i \in I_j} a_{ij} e_i,$$

em que cada $I_j \subseteq I$ é um conjunto finito. Tome-se então $I' := \bigcup_{j=1}^{n} I_j$, e, acrescentando coeficientes nulos se necessário, temos que todo o x_j é combinação linear dos elementos $\{e_i : i \in I'\}$, com I' finito. Assim, e por o

conjunto $\{x_1, \ldots, x_n\}$ ser gerador, o conjunto $\{e_i : i \in I'\}$ é também gerador, e, por ser subconjunto de uma base, é linearmente independente; ou seja, é também uma base. Como qualquer base é um conjunto independente maximal, temos que ter $I = I'$ e I é finito, como desejávamos.

2. Trata-se de uma adaptação do argumento anterior. Do ponto anterior sai imediatamente que todas as bases de M têm que ser infinitas. Sejam então $E = \{e_i : i \in I\}$ e $F = \{f_j : j \in J\}$ duas bases de M. Para cada $i \in I$, existe um subconjunto finito de J, digamos J_i, tal que

$$e_i = \sum_{j \in J_i} a_{ij} f_j.$$

Tomando então $J' := \bigcup_{i \in I} J_i$, temos que a família $\{f_j : j \in J'\}$ é também geradora por construção, e linearmente independente por estar contida numa base. Assim, como acima, $J = J'$. Finalmente, como $|J_i| \leq \aleph_0$, para todo o i, temos

$$|J| = |J'| \leq |I|.\aleph_0 = |I|,$$

por I ser infinito. Assim $|J| \leq |I|$, e analogamente se provaria que $|I| \leq |J|$, e portanto $|I| = |J|$. □

Os anéis para os quais se pode definir dimensão de módulos livres têm um nome especial na teoria de anéis.

Definição 1.2 *Diz-se que um anel A é um* anel IBN *(do inglês* invariant base number*) se em qualquer módulo-A livre, as bases tiverem todas a mesma cardinalidade.*

Se M for um módulo-A livre sobre um anel IBN, chama-se dimensão *de M à cardinalidade de qualquer uma das suas bases. Se estas forem finitas, o módulo diz-se de dimensão finita.*

Pode mostrar-se que, para um anel ser anel IBN, basta que em todos os módulos-A à esquerda livres, todas as bases tenham a mesma cardinalidade; ou analogamente, que isto aconteça para todos os módulos-A à direita. Assim, para um anel ser anel IBN, basta que o seja "à direita" ou "à esquerda". Veremos isto na secção 3, proposição 3.2.

2 Dimensão no Caso Comutativo

Como já vimos, o exemplo mais simples de anéis IBN são, evidentemente, os corpos, pois num espaço vectorial todas as bases têm a mesma cardinalidade. Veremos no próximo teorema que na verdade é preciso muito menos

que isso: todo o anel comutativo é anel IBN. Vamos apresentar nesta secção e nas seguintes três demonstrações deste facto, relacionando duas delas num exercício final.

Começamos por estabelecer alguns resultados intermédios.

Lema 2.1 *Sejam A e B anéis, $f : A \to B$ um epimorfismo, e M um módulo-A tal que* $\operatorname{Nuc} f \subseteq \operatorname{An}_A(M)$. *Então é possível introduzir no grupo abeliano $(M, +)$ uma estrutura de módulo-B, pondo, para todo o $x \in M$ e $b \in B$, com $b = f(a)$,*

$$b.x = f(a).x := a.x.$$

Demonstração. É simples de ver que a acção está bem definida: se $b = f(a) = f(a')$, então $f(a - a') = 0$, $a - a' \in \operatorname{Nuc} f \subseteq \operatorname{An}_A(M)$, logo $(a - a').x = 0$, e $a.x = a'.x$, como desejávamos. Todas as outras verificações são de rotina. □

Proposição 2.2 *Sejam A e B anéis, com B imagem homomorfa de A. Então, se B for anel IBN, A é anel IBN.*

Demonstração. Considere-se $f : A \to B$ um epimorfismo. Seja M um módulo-A à esquerda, $J = \operatorname{Nuc} f$, e tome-se $N := JM$, que é um submódulo de M. É simples de ver que $\operatorname{Nuc} f \subseteq \operatorname{An}_A(M/N)$, pois se $a \in \operatorname{Nuc} f = J$, então $a(x + N) = ax + N = 0 + N$, pois $ax \in JM = N$. Assim, pelo que vimos acima, é possível introduzir em M/N uma estrutura de módulo-B, de acordo com a fórmula acima escrita para o produto escalar.

Se M for livre de base infinita, já vimos que todas as bases têm a mesma cardinalidade. Supondo então que M tem uma base finita, $\{e_1, \ldots, e_n\}$, vejamos que $\{e_1 + N, \ldots, e_n + N\}$ é base de M/N como módulo-B.

Para ver que se trata de um conjunto gerador, tome-se $x + N \in M/N$ qualquer. Temos que $x = a_1e_1 + \ldots + a_ne_n$, e portanto

$$\begin{aligned} x + N &= (a_1e_1 + N) + \ldots + (a_ne_n + N) \\ &= f(a_1).(e_1 + N) + \ldots + f(a_n).(e_n + N), \end{aligned}$$

de acordo com a definição de produto escalar de elementos de M/N por elementos de B. Assim, o conjunto apresentado é gerador.

Tomando agora uma combinação linear nula

$$f(a_1)(e_1 + N) + \ldots + f(a_n).(e_n + N) = N,$$

obtemos, depois de simplificar a expressão, $a_1e_1 + \ldots + a_ne_n \in N = JM$. Ora, por J ser ideal,

$$JM = JA\{e_1, \ldots, e_n\} \subseteq J\{e_1, \ldots, e_n\},$$

e portanto as expressões dos elementos de JM como combinação linear da base têm coeficientes em J, e, como se trata de uma base, este coeficientes estão bem definidos. Assim, $a_1, \ldots, a_n \in J = \operatorname{Nuc} f$, e portanto $f(a_1) = \ldots = f(a_n) = 0$, e a família considerada é linearmente independente.

Ora, tomando agora uma outra base qualquer de M, necessariamente finita, digamos, $\{e'_1, \ldots, e'_m\}$, podemos repetir o processo anterior, e concluir que $\{e'_1 + N, \ldots, e'_m + N\}$ é também base de M/N como módulo-B. Como B é anel IBN, por hipótese, vem que $m = n$, o que quer dizer que também A é anel IBN. □

Precisamos agora de um facto conhecido de teoria de anéis: num anel comutativo[1] (com identidade) existe pelo menos um ideal maximal (próprio). A demonstração deste facto assenta, como seria de esperar, no lema de Zorn. Tomando uma cadeia de ideais próprios $(I_k : k \in K)$, podemos tomar $I := \bigcup I_k$, que é claramente um majorante da cadeia. Para garantir que se trata de um ideal próprio, isto é, que $I \neq A$, basta ver que se isso não acontecesse, teríamos $1 \in I$, e portanto $1 \in I_t$ para um certo $t \in K$, o que é falso, pois nesse caso $I_t = A$, e não seria ideal próprio. Assim, encontrámos um majorante para a cadeia inicial, o que, pelo lema de Zorn, implica que tem que existir um ideal maximal em A.

Uma das utilidades da existência de um ideal maximal I num anel comutativo A é que o quociente A/I fica com a estrutura de corpo. Para provar que, nestas condições, todo o elemento não nulo $a + I \in A/I$ tem inverso, basta notar que, como $a + I \neq I$, então $a \notin I$, e portanto $Aa + I$ é um ideal de A (é o ideal gerado por $I \cup \{a\}$), contendo estritamente I. Pela maximalidade de I, este ideal tem que ser A, e, em particular, $1 \in aA + I$, o que quer dizer que existe $b \in A$ tal que $ab + I = 1 + I$. Reescrevendo esta igualdade, temos

$$ab + I = 1 + I \Leftrightarrow (a + I)(b + I) = 1 + I,$$

e encontrámos assim um inverso multiplicativo para $a + I$ em $b + I$.

[1] O resultado vale também para anéis não comutativos, e nesse caso teríamos que falar de ideais esquerdos, direitos ou bilaterais. Neste momento precisamos apenas do resultado em anéis comutativos.

Teorema 2.3 *Um anel comutativo é anel IBN.*

Demonstração. Tomamos então um anel comutativo A, I um ideal maximal, que sabemos existir em A, e consideramos o corpo A/I. Basta agora notar que existe um epimorfismo óbvio de A para A/I, o epimorfismo canónico. Como A/I é corpo, é anel IBN, e portanto, pela proposição anterior, A vem anel IBN. □

É de notar que estes não são os únicos exemplos de anéis IBN. Também os anéis noetherianos, tanto à esquerda como à direita, e os artinianos, igualmente tanto à esquerda como à direita, são anéis IBN.

3 Dimensão e Matrizes

Na última secção, para provar que um anel comutativo é anel IBN, passámos por uma proposição que afirmava que se existe um homomorfismo de anéis sobrejectivo, $A \to B$, e B é anel IBN, então A é anel IBN. Vamos ver que isso pode ser demonstrado de uma forma mais geral e mais simples recorrendo a matrizes, mesmo com um enfraquecimento da hipótese: basta que f seja homomorfismo de anéis.

Antes disso, vamos fazer um pequeno estudo de como as matrizes podem representar aplicações lineares entre módulos, e desse estudo tirar um resultado adicional sobre anéis IBN.

Tal como nos espaços vectoriais, é possível definir matriz de uma aplicação linear, tendo apenas cuidado com a maneira como essas matrizes representam a aplicação linear. Suponhamos que M e N são módulos-A à esquerda, livres, e fixemos em cada um uma base. Se $f : M \to N$ for uma aplicação linear, podemos representá-la por uma matriz contendo nas *linhas* as coordenadas das imagens da base de M, por meio de f na base de N. Se R for a dita matriz, e se representarmos por $[x]$ a matriz coluna das coordenadas de um vector, nas bases fixadas, temos que $[f(x)]^T = [x]^T R$. Como se espera, à composição de aplicações lineares corresponde o produto de matrizes, mas *por ordem contrária*: se $g : N \to P$ for outra aplicação linear para P, módulo-A à esquerda, também com uma base fixada, e S for a matriz de g em relação às bases fixadas, então a matriz de $f \circ g$ vem a ser RS.

Se os módulos forem à direita, então todo o formalismo habitual nos espaços vectoriais funciona: as coordenadas das imagens dos vectores aparecem nas colunas da matriz que representa a aplicação linear, a matriz é

multiplicada à esquerda pelos vectores coluna das coordenadas, e, à composição de aplicações lineares, corresponde a multiplicação de matrizes na ordem correspondente.

Estes estudos com matrizes permitem que, para verificar que um anel é IBN, não precisemos de verificar o que se passa com todos os módulos, mas apenas com os esquerdos, ou os direitos, como veremos na próxima proposição. Antes dela, vamos apresentar um lema técnico.

Lema 3.1 *Seja A um anel. Então as seguintes afirmações são equivalentes.*

1. ${}_AA^n \cong {}_AA^m$.

2. $A_A^n \cong A_A^m$.

3. Existem matrizes $R \in M_{m\times n}(A)$ e $S \in M_{n\times m}(A)$ tais que $RS = I_m$ e $SR = I_n$.

Demonstração. Basta ver que $1 \Leftrightarrow 3$ e $2 \Leftrightarrow 3$, o que é simples de verificar, depois do que expusemos sobre matrizes e aplicações lineares, se considerarmos R e S como as matrizes dos isomorfismos em questão. □

Proposição 3.2 *Seja A um anel para o qual, em todos os módulos-A à direita livres, todas as bases têm a mesma cardinalidade. Então A é anel IBN. O mesmo se passa se tivermos a propriedade apenas para módulos-A à esquerda livres.*

Demonstração. Já vimos que se as bases forem infinitas, têm todas a mesma cardinalidade, vamos trabalhar então no caso em que as bases são finitas. Vamos agora supor que, nos módulos-A à direita livres, todas as bases têm a mesma cardinalidade. É simples de ver que um módulo--A à direita livre que admita uma base com n elementos é isomorfo a A_A^n. Assim, supor que em todos os módulos à direita livres, todas as bases têm a mesma cardinalidade é equivalente a afirmar que se $A_A^n \cong A_A^m$ temos $n = m$. Tomemos agora um módulo-A à esquerda livre, admitindo bases com n e m elementos, respectivamente. Isto implica que ${}_AA^n \cong {}_AA^m$, o que, pelo lema anterior, implica que $A_A^n \cong A_A^m$, e, pela nossa hipótese, $n = m$. Isto mostra que em qualquer módulo-A à esquerda livre, todas as bases têm a mesma cardinalidade, e portanto, A é anel IBN. □

Assim, dizer que A é anel IBN é dizer que, sempre que existam matrizes $X \in M_{m\times n}(A)$ e $Y \in M_{n\times m}(A)$ com $XY = I_m$ e $YX = I_n$, temos necessariamente $m = n$.

Vamos agora apresentar uma nova demonstração do teorema 2.3, que afirma que um anel comutativo é anel IBN, usando os resultados que acabámos de estabelecer. No caso em que A é comutativo, e, para além disso, a característica de A é zero, torna-se imediato mostrar que A é anel IBN: basta tomar traços nas igualdades anteriores, sabendo que $\mathrm{tr}(XY) = \mathrm{tr}(YX)$, o que é verdade no caso comutativo. Assim $n.1 = m.1$, o que, em característica zero, implica que $n = m$. Obtemos assim uma demonstração muito curta para o facto de todo o anel comutativo ser anel IBN, no caso em que a característica é zero.

Vejamos agora o caso geral.

Proposição 3.3 *Sejam A e B anéis, e suponhamos que existe um homomorfismo de anéis $f : A \to B$ e que B é anel IBN. Então A é anel IBN.*

Demonstração. Tomemos duas matrizes $R \in M_{m\times n}(A)$ e $S \in M_{n\times m}(A)$, com $RS = I_m$ e $SR = I_n$, queremos concluir que $n = m$. Ora, aplicando o homomorfismo f às entradas das matrizes, e tendo em conta que todas as operações são respeitadas pelo homomorfismo, obtemos duas matrizes R' e S', com entradas em B, com $R'S' = I_m$ e $S'R' = I_n$. Como B é anel IBN, temos que $n = m$, o que era o resultado pretendido. □

Agora podemos seguir para o teorema 2.3, e obter que todo o anel comutativo é anel IBN, sem termos tido que fazer toda a construção da secção anterior. A comutatividade intervém apenas quando necessitamos que A/I seja corpo.

4 Dimensão e Produtos Tensoriais

Este mesmo resultado pode ser obtido recorrendo à definição de produto tensorial de módulos sobre anéis comutativos. Nesse caso, todo o formalismo que se usa com os espaços vectoriais, na definição de produto tensorial, funciona também para os módulos, sem ter que se recorrer às definições de aplicação balanceada, ou bimódulo. Vamos então considerar que estas coisas são conhecidas, e passar ao resultado, cuja demonstração, sendo mais complicada que aquela que acabámos de apresentar, tem aplicações para além deste resultado.

Dado um módulo M sobre um anel A, e B um anel de certo modo relacionado com A, é por vezes útil tentar encontrar um módulo-B que seja parecido com M enquanto módulo-A. A relação que vamos exigir entre os

anéis A e B será relativamente fraca: vamos apenas supor que existe um homomorfismo $f : A \to B$. Note-se que isto inclui os casos em que $A \subseteq B$ e em que B é imagem homomorfa de A, que serão os que nos vão interessar mais tarde.

Nestas condições, é possível dotar B de uma estrutura de módulo-A de uma forma natural: pomos $a.b := f(a).b$. É trivial verificar que B fica de facto com estrutura de módulo-A. Note-se que se $A \subseteq B$, o produto escalar corresponde simplesmente à multiplicação em B, uma vez que $f(a) = a$ para todo o $a \in A$.

Uma vez isto feito, é possível construir o produto tensorial $B \otimes_A M$ e dar-lhe uma estrutura de módulo-B também de uma forma natural (como agora estamos a lidar com dois anéis, pomos A como índice no símbolo $\otimes$ para mostrar claramente que estamos a fazer o produto tensorial de B e de M enquanto módulos-A). A estrutura de módulo-B de $B \otimes_A M$ é dada da seguinte forma: para $b \in B$, e um tensor decomponível $b' \otimes x$, pomos

$$b.(b' \otimes x) := (bb') \otimes x.$$

e prolongamos por linearidade a todo o produto tensorial. É igualmente simples ver que isto confere a $B \otimes_A M$ a estrutura de módulo-B.

A parecença de $B \otimes_A M$ enquanto módulo-B com M enquanto módulo-A é posta então em evidência pela proposição 4.3, antes da qual precisamos de um resultado técnico.

Proposição 4.1 *Sejam N e M módulos-A, em que M é livre de base $\{e_i : i \in I\}$. Então todo o elemento de $N \otimes M$ admite uma expressão do tipo $\sum_{i \in I} y_i \otimes e_i$, em que a família y_i de elementos de N é quase toda nula, e bem determinada.*

Demonstração. A existência decorre de um simples cálculo. Dado qualquer tensor decomponível $y \otimes x$ o elemento x escreve-se como $x = \sum_{i \in I} a_i e_i$, e, usando a multilinearidade, vem

$$y \otimes x = y \otimes (\sum_{i \in I} a_i e_i) = \sum_{i \in I} a_i (y \otimes e_i) = \sum_{i \in I} (a_i y) \otimes e_i.$$

A soma é claramente finita, pois a família a_i é quase toda nula. Exprimindo agora um tensor arbitrário como soma de tensores decomponíveis, basta exprimir cada um dos tensores parcelas como acima, e depois, para cada i, associar as parcelas que têm e_i do lado direito, usando mais uma vez a multilinearidade. Obtemos assim a expressão desejada.

Quanto à unicidade, suponhamos que $\sum_{i\in I} y_i \otimes e_i = \sum_{i\in I} y'_i \otimes e_i$. Queremos provar que, para $k \in I$ arbitrário, $y_k = y'_k$. Tomamos então a aplicação linear η_k, definindo

$$\eta_k(y \otimes (\sum_{i\in I} a_i e_i)) := a_k y,$$

prolongada por linearidade a $N \otimes M$ — trata-se da aplicação que factoriza a aplicação bilinear $(y, x) \mapsto f_k(x).y$, em que f_k é o elemento da família dual da base, definido por $f_k(e_j) = \delta_{kj}$ para todo o $j \in I$. É simples de verificar que esta aplicação é bilinear.

Notamos que, para $y \in N$, $\eta_k(y \otimes e_i) = \delta_{ik} y$, uma vez que $e_i = \sum_{i\in I} \delta_{ij} e_j$.

Aplicando então η_k a ambos os membros da igualdade acima, obtemos

$$\eta_k(\sum_{i\in I} y_i \otimes e_i) = \sum_{i\in I} \delta_{ik} y_i = y_k,$$

e analogamente $\eta_k(\sum_{i\in I} y'_i \otimes e_i) = y'_k$. Assim, $y_k = y'_k$, como desejávamos.□

Corolário 4.2 *1. Sejam V e U espaços vectoriais sobre um corpo K, $\{v_1, \ldots, v_t\} \subseteq V$, uma família linearmente independente, e $\{u_1, \ldots, u_t\} \subseteq U$. Então $u_1 \otimes v_1 + \ldots + u_t \otimes v_t = 0$ se e só se $u_1 = \ldots = u_t = 0$.*

2. Seja $M \neq 0$ um módulo-A livre, e $N \neq 0$ um módulo-A qualquer. Então $M \otimes N \neq 0$.

Proposição 4.3 *Sejam A e B anéis, com $f : A \to B$ um homomorfismo. Suponhamos que M é um módulo-A livre, com base $\{e_i : i \in I\}$. Então $B \otimes_A M$ é também um módulo-B livre, com base $\{1 \otimes e_i : i \in I\}$.*

Demonstração. O resultado sai facilmente da proposição 4.1. Para ver que se trata de um conjunto gerador, basta ver que, de acordo com essa proposição, qualquer elemento de $B \otimes_A M$ se escreve como

$$\sum_{i\in I} b_i \otimes e_i = \sum b_i (1 \otimes e_i),$$

de acordo com a estrutura de módulo-B definida em $B \otimes_A M$.

Quanto à independência linear,

$$\sum_{i\in I} b_i (1 \otimes e_i) = 0 \Leftrightarrow \sum_{i\in I} (b_i \otimes e_i) = 0,$$

e, mais uma vez pela proposição anterior, $b_i = 0$ para todo o $i \in I$. □

Este resultado pode ser aplicado não só para resolver o nosso problema, como noutras circunstâncias.

Dimensão de módulos sobre anéis comutativos. Como vimos no teorema 2.3, os anéis comutativos são anéis IBN. Ora, este facto pode demonstrar-se também recorrendo à proposição anterior. Tal como no teorema, considerando A um anel comutativo, e I um ideal maximal de A, sabemos que $B := A/I$ é corpo, e é imagem homomorfa de A. Assim, pela proposição anterior, se M for um módulo-A livre, com bases $\{e_i : i \in I\}$ e $\{f_j : j \in J\}$, podemos obter duas bases de $B \otimes_A M$, como módulo-B, $\{1 \otimes e_i : i \in I\}$ e $\{1 \otimes f_j : j \in J\}$. Ora, como B é corpo, temos que ter $|I| = |J|$ e as bases originais têm a mesma cardinalidade.

Complexificação de um espaço real. Se V for um espaço vectorial real, $\mathbb{R} \subseteq \mathbb{C}$, o espaço $\mathbb{C} \otimes_{\mathbb{R}} V$ é um espaço vectorial complexo, ao qual se chama a *complexificação de* V. Os resultados anteriores dizem-nos que se $\{e_i : i \in I\}$ for uma base de V, $\{1 \otimes e_i : i \in I\}$ é uma base de $\mathbb{C} \otimes_{\mathbb{R}} V$.

É possível verificar que há pontos em comum entre as demonstrações da segunda secção e as desta última. Tomemos A, um anel comutativo, I um seu ideal maximal, e $B := A/I$, que é um corpo. Na primeira demonstração que num módulo-A livre finitamente gerado M todas as bases tinham a mesma cardinalidade, considerámos o submódulo $N = IM$, e o módulo-B M/N. Na secção do produto tensorial, construímos outro módulo-B a partir de M, que foi $B \otimes_A M$. Construindo dois homomorfismos inversos, é possível provar que estes dois módulos-B são isomorfos. Deixamos isso ao cargo do leitor.

Referências

[AF] F. Anderson e K. Fuller, *Rings and Categories of Modules*, Springer Verlag, 1992.

[AR] D. D. Anderson and J. Robeson, *Bases for Modules*, Expo. Math. 22 (2004): 283–296.

[Bo] N. Bourbaki, *Éléments de Mathématique — Algèbre: chapitres 1 à 3*, Hermann, 1970.

[FR] R. Fernandes, M. Ricou, *Introdução à Álgebra*, IST Press, 2003.

[Fr] P. J. Freitas, *Tópicos de Álgebra Superior*, Textos de Matemática, Universidade de Lisboa, no prelo.