Conjuntos linearmente independentes e conjuntos geradores em módulos

Daniel V. Tausk (IME/USP)

Rodrigo A. Freire (CLE/Unicamp)

Em cursos introdutórios de álgebra linear aprende-se que todo espaço vetorial V (sobre um corpo de escalares K) que admite um número finito de geradores (i.e., é finitamente gerado) admite uma base finita e que todas as bases de V possuem o mesmo número n de elementos (chamado a *dimensão* de V). Além do mais, se V tem dimensão n então todo subconjunto linearmente independente de V tem no máximo n elementos e todo conjunto de geradores de V tem ao menos n elementos. Se um subconjunto de V com exatamente n elementos for linearmente independente ou se for um conjunto de geradores então será automaticamente uma base.

Quando trocamos o corpo de escalares K por um anel[1] R, falamos em *módulos* sobre R ou R-*módulos*, em vez de espaço vetoriais. A álgebra linear para módulos é bem diferente da álgebra linear para espaços vetoriais. (Mesmo quando o anel R é comutativo!). Não é sequer verdade que todo módulo finitamente gerado admite uma base. Por exemplo, se o anel R é infinito então nenhum R-módulo finito não nulo admite uma base. Um módulo que admite uma base é chamado *livre*.

É um fato bem conhecido que se R é um anel comutativo e se um R-módulo livre M possui uma base com n elementos então qualquer base de M possui n elementos (veja, por exemplo, [2, p. 171, Thm. 3.4]); o número natural[2] n é chamado o *posto* do módulo livre M. A hipótese de que R seja comutativo é essencial: não é difícil construir um exemplo[3] de um anel não comutativo R tal que R e R^n sejam isomorfos, como R-módulos, para qualquer inteiro positivo n. É também um fato bem conhecido que se R é um anel comutativo então todo conjunto de geradores de um R-módulo livre de posto n tem pelo menos n elementos e que todo conjunto de geradores com exatamente n elementos é automaticamente uma base (veja, por exemplo, [3, p. 415, Prop. 7.20]).

O objetivo desta nota é apresentar duas demonstrações para o fato que o número de elementos de um conjunto linearmente independente em um módulo livre de posto n sobre um anel comutativo é menor ou igual a n. (Não é verdade, no entanto, que num módulo livre de posto n sobre um anel comutativo todo conjunto linearmente independente com n elementos seja uma base[4].) É surpreendente que uma demonstração (ou mesmo apenas o enunciado) de um resultado tão básico não se encontre em muitos dos textos de álgebra usuais destinados ao ensino de pós-graduação[5]. Na ver-

[1] Neste artigo supõe-se sempre que os anéis têm unidade.

[2] É verdade também que duas bases (possivelmente infinitas) de um módulo livre sobre um anel comutativo R possuem a mesma cardinalidade, de modo que podemos definir o posto de um R-módulo livre arbitrário (o qual pode ser um cardinal infinito). Neste artigo focalizaremos nossa atenção apenas no caso de módulos de posto finito.

[3] Seja V um espaço vetorial de dimensão infinita, de modo que existe um isomorfismo $\phi : V \to V^n$. Se $R = \mathrm{Lin}(V, V)$ é o anel dos endomorfismos lineares de V então R^n é isomorfo, como R-módulo à esquerda, ao espaço $\mathrm{Lin}(V^n, V)$ das transformações lineares de V^n em V. A composição à direita com ϕ nos dá um isomorfismo entre $\mathrm{Lin}(V^n, V)$ e $R = \mathrm{Lin}(V, V)$ como R-módulos à esquerda.

[4] Basta observar, por exemplo, que $\mathbb{Z}$ é um $\mathbb{Z}$-módulo livre de posto 1 e que se k é um inteiro maior do que 1 então $\{k\}$ é linearmente independente, mas não é uma base.

[5] O resultado é, porém, bem mais conhecido quando R é um domínio de integridade. Nesse caso, uma demonstração bem mais

dade, encontramos uma demonstração desse fato apenas no livro de álgebra de Bourbaki ([1, p. 524, Prop. 3]), o que motivou a presente exposição. A primeira demonstração exposta aqui é elementar e é uma adaptação da demonstração de Bourbaki que consiste em substituir o uso da álgebra exterior naquela demonstração por computações diretas com matrizes e determinantes. A segunda demonstração é, até onde nós autores sabemos, original e foi elaborada antes de tomarmos contato com a demonstração de Bourbaki. Esta nota mostra que pelo menos uma das duas demonstrações aqui apresentadas poderia estar presente em qualquer texto de álgebra destinado à pós-graduação praticamente sem custo em termos de espaço.

1 Primeira Demonstração

Nesta seção R denota um anel comutativo[6]. Seja $A \in M_n(R)$ uma matriz $n \times n$ com entradas em R. Denotamos por $\det(A)$ seu determinante, definido da forma usual:

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^{n} A_{i\sigma(i)},$$

onde S_n denota o grupo das permutações (bijeções) de $\{1, \ldots, n\}$ e $\operatorname{sgn}(\sigma)$ denota o sinal da permutação σ. O determinante definido dessa forma possui as propriedades usuais: ele é uma função n-linear das colunas (ou das linhas) de A, se duas colunas (ou linhas) de A são iguais o determinante é igual a zero e o determinante pode ser calculado pela fórmula usual de expansão por cofatores. Além do mais, o determinante de uma matriz é igual ao determinante de sua transposta e o determinante do produto de duas matrizes é igual ao produto dos determinantes.

Vejamos agora um resultado interessante relacionando determinantes e dependência linear. Suponha que as colunas da matriz $A \in M_n(R)$ sejam elementos linearmente dependentes de R^n, i.e., se $x_1, \ldots, x_n \in R^n$ denotam as colunas de A, existem escalares $c_1, \ldots, c_n \in R$ não todos nulos tais que:

$$\sum_{i=1}^{n} c_i x_i = 0.$$

Usando a n-linearidade do determinante, obtemos:

$$\begin{aligned} c_1 \det(x_1, x_2, \ldots, x_n) &= \det(c_1 x_1, x_2, \ldots, x_n) \\ &= -\sum_{i=2}^{n} c_i \det(x_i, x_2, \ldots, x_n) = 0, \end{aligned}$$

onde $\det(x_1, x_2, \ldots, x_n)$ denota o determinante da matriz cujas colunas são x_1, x_2, …, x_n. De modo análogo, vemos que $c_i \det(A) = 0$, para todo $i = 1, \ldots, n$. Como algum c_i é não nulo, provamos o seguinte:

Lema 1. *Se as colunas de $A \in M_n(R)$ são linearmente dependentes em R^n então existe $c \in R$ não nulo tal que $c \det(A) = 0$.* □

Nosso objetivo é provar a recíproca desse lema e, mais geralmente, provar a seguinte:

Proposição 2. *Seja $A \in M_{n\times k}(R)$ uma matriz $n \times k$ com entradas em R. Então as colunas de A são linearmente dependentes em R^n se e somente se existe $c \in R$ não nulo tal que $c \det(A_I) = 0$ para todo subconjunto I de $\{1, \ldots, n\}$ contendo k elementos, onde $A_I \in M_k(R)$ denota a matriz cujas linhas são precisamente as linhas de A cujo número está em I.*

Demonstração. Um argumento completamente análogo ao usado para mostrar o Lema 1 mostra que se as colunas de A são linearmente dependentes então existe c em R não nulo tal que $c \det(A_I) = 0$ para todo $I \subset \{1, \ldots, n\}$ com k elementos. Mostremos a recíproca por indução em k. O caso $k = 1$ é trivial. Sejam dados $k \geq 2$, $A \in M_{n\times k}(R)$ e suponha o resultado válido para matrizes com menos do que k colunas. Dados $I \subset \{1, \ldots, n\}$ e $r \in \{1, \ldots, k\}$, denotamos por A_I^r (resp., A^r) a matriz obtida de A_I (resp., de A) pela remoção da r-ésima coluna. Suponha que exista $c \in R$ não nulo tal que $c \det(A_I) = 0$ para todo $I \subset \{1, \ldots, n\}$ com k elementos. Se tivermos $c \det(A_I^1) = 0$ para todo $I \subset \{1, \ldots, n\}$ com $k - 1$ elementos então, pela hipótese de indução, as colunas de

simples para o resultado é baseada no seguinte fato: um sistema linear homogêneo com n equações e $n + 1$ incógnitas possui uma solução não trivial no corpo de frações de R, da qual obtém-se facilmente uma solução não trivial em R.

[6] Exceto pelo Teorema 5, não é necessário supor que R possui unidade.

A^1 (e, *a fortiori* as colunas de A) são linearmente dependentes. Suponha então que exista $I \subset \{1,\dots,n\}$ com $k-1$ elementos tal que $c\det(A^1_I) \neq 0$. Sejam $x_1,\dots,x_k \in R^n$ as colunas de A e vamos mostrar que elas são linearmente dependentes. A estratégia é mostrar que:

$$\sum_{r=1}^{k}(-1)^{r+1}c\det(A^r_I)x_r = 0 \qquad (1.1)$$

e daí, como $c\det(A^1_I) \neq 0$, a conclusão seguirá. Seja $i \in \{1,\dots,n\}$. Temos que a i-ésima coordenada (com relação à base canônica de R^n) do somatório do lado esquerdo de (1.1) é igual a $c\det(B)$, onde a matriz $B \in M_k(R)$ é definida da seguinte forma: a primeira linha de B é a i-ésima linha de A e as outras $k-1$ linhas de B são as linhas de A_I. (De fato, considere o cálculo do determinante de B usando expansão por cofatores na primeira linha.) Se $i \in I$, temos que B tem duas linhas iguais e portanto $\det(B) = 0$. Se $i \notin I$, temos que B é igual a $A_{I\cup\{i\}}$ a menos de uma permutação de linhas; em todo caso, concluímos que $c\det(B) = 0$. Isso prova (1.1) e conclui a demonstração da proposição. □

Corolário 3. *Se $A \in M_n(R)$ então as colunas de A são linearmente dependentes se e somente se existe $c \in R$ não nulo tal que $c\det(A) = 0$.* □

Corolário 4. *Um subconjunto de R^n com mais do que n elementos é sempre linearmente dependente.*

Demonstração. De fato, se $k > n$ então a condição de que exista $c \in R$ não nulo tal que $c\det(A_I) = 0$ para todo $I \subset \{1,\dots,n\}$ com k elementos é vaziamente satisfeita. □

Evidentemente, segue desse último corolário que se R é um anel comutativo então um subconjunto linearmente independente de um R-módulo livre de posto n possui no máximo n elementos. Além do mais, temos também o seguinte teorema.

Teorema 5. *Seja R um anel comutativo. Se M é um R-módulo que admite um conjunto de geradores com n elementos então todo subconjunto linearmente independente de M possui no máximo n elementos.*

Demonstração. Se M admite um conjunto de geradores com n elementos então a aplicação R-linear $\phi : R^n \to M$ que leva a base canônica de R^n sobre esse conjunto de geradores é sobrejetora. Um subconjunto linearmente independente de M com $n+1$ elementos seria então a imagem por ϕ de algum subconjunto linearmente independente de R^n com $n+1$ elementos. Isso contradiz o Corolário 4. □

2 Segunda Demonstração

Recordamos que um módulo sobre um anel (não necessariamente comutativo) R é chamado *Noetheriano* quando não admite uma seqüência infinita estritamente crescente de submódulos. Dizemos que o anel R é *Noetheriano* quando R, entendido como um R-módulo à esquerda, for Noetheriano.

O lema abaixo ocorre como um exercício no livro de Bourbaki ([1, p. 384, Ex. 16]) e tem como conseqüência imediata que para anéis Noetherianos o número de elementos de um conjunto linearmente independente num módulo livre é menor ou igual ao posto.

Lema 6. *Seja R um anel (não necessariamente comutativo). Se existe um subconjunto linearmente independente de R^n com $n+1$ elementos então existe um subconjunto linearmente independente infinito de R^n.*

Demonstração. Se $u_1, \dots, u_k, v_1, \dots, v_n$ é uma sequência linearmente independente em R^n então o submódulo $\langle v_1,\dots,v_n\rangle$ gerado por $v_1, \dots, v_n$ é isomorfo a R^n e, portanto, contém um conjunto linearmente independente $\{w_1,\dots,w_{n+1}\}$ com $n+1$ elementos. Fazendo $u_{k+1} = w_{n+1}$, $v'_i = w_i$, $i = 1,\dots,n$, então a sequência $u_1, \dots, u_k, u_{k+1}, v'_1, \dots, v'_n$ é linearmente independente. Por recursão, obtemos uma sequência linearmente independente infinita $(u_m)_{m\geq 1}$. □

Corolário 7. *Seja R um anel (não necessariamente comutativo). Se R é Noetheriano então todo subconjunto linearmente independente de R^n possui no máximo n elementos.*

Demonstração. Se em R^n existisse um subconjunto linearmente independente com $n+1$ elementos, então exis-

tiria também um subconjunto infinito linearmente independente e disso seguiria a existência de uma seqüência estritamente crescente de submódulos de R^n. Mas, como R é Noetheriano, R^n também é Noetheriano e tais sequências não existem. □

Outra demonstração para o Corolário 4. Suponha por absurdo que exista um subconjunto linearmente independente $\{u_1, \ldots, u_{n+1}\}$ de R^n com $n+1$ elementos. O conjunto de todas as coordenadas dos vetores $u_i \in R^n$ possui no máximo $k = (n+1)n$ elementos. Considere o anel de polinômios $\mathbb{Z}[X_1, \ldots, X_k]$ e seja $f : \mathbb{Z}[X_1, \ldots, X_k] \to R$ um homomorfismo de anéis que leva as indeterminadas $X_1, \ldots, X_k$ sobre o conjunto das coordenadas dos vetores u_i na base canônica de R^n. Se S é a imagem de f então S é um subanel de R e $\{u_1, \ldots, u_{n+1}\}$ é um subconjunto linearmente independente do S-módulo S^n. Mas S é isomorfo a um quociente de $\mathbb{Z}[X_1, \ldots, X_k]$ e, com isso, é Noetheriano, já que $\mathbb{Z}[X_1, \ldots, X_k]$ é Noetheriano pelo Teorema da Base de Hilbert. Isso contradiz o Corolário 7. □

Referências

[1] Bourbaki, N. *Algebra I*. Berlin: Springer, 1989. Chapters 1–3. (Elements of Mathematics)

[2] Jacobson, N. *Basic algebra I*. 2. ed. New York: Dover, 2009.

[3] Jacobson, N. *Basic algebra II*. 2. ed. New York: Dover, 2009.

Daniel V. Tausk
Instituto de Matemática e Estatística da USP
www.ime.usp.br/~tausk
tausk@ime.usp.br

Rodrigo A. Freire
Centro de Lógica, Epistemologia e História da Ciência
Universidade Estadual de Campinas
freire@cle.unicamp.br