MATEMÁTICA UNIVERSITÁRIA
n$^{\underline{os}}$ 38/39 – julho/dezembro 2005 – pp. 93–98

Grupos algébricos lineares comutativos conexos unipotentes

FÁBIO XAVIER PENNA

Introdução

Os grupos algébricos lineares foram tratados pela primeira vez em uma série de artigos escritos por L. Maurer, no final do século XIX. Poucos anos mais tarde, eles foram novamente considerados por E. Cartan, W. Killing, S. Lie e pelo próprio Maurer no estudo de equações diferenciais e teoria de Galois.

Nos anos 40, Chevalley e Kolchin viram-se atraídos pelos grupos algébricos, motivados pelo interesse que nutriam por grupos de Lie. No entanto, uma teoria puramente algébrica surgiu apenas na década de 50, quando os métodos de geometria algébrica passaram a desempenhar papel fundamental junto aos grupos algébricos. Desde então eles surgem naturalmente no estudo de geometria algébrica e de outras áreas da matemática.

A primeira seção deste texto contém uma breve apresentação dos grupos algébricos lineares, com exemplos e resultados básicos. A segunda traz a classificação dos grupos algébricos lineares comutativos conexos unipotentes. Este é um resultado clássico para o qual apresentamos uma nova demonstração envolvendo apenas conhecimentos elementares de geometria algébrica, visando uma argumentação simples e acessível ao leitor não especializado.

Grupos algébricos lineares

Um *grupo algébrico* sobre o corpo dos números complexos $\mathbb{C}$ é uma variedade algébrica G que possui uma estrutura de grupo tal que os mapas

$$\begin{array}{rccc} \pi: & G\times G & \longrightarrow & G \\ & (x,y) & \longmapsto & x\cdot y \end{array} \quad \text{e} \quad \begin{array}{rccc} l: & G & \longrightarrow & G \\ & x & \longmapsto & x^{-1} \end{array}$$

sejam morfismos de variedades. A topologia utilizada é chamada *topologia de Zariski*, na qual os fechados básicos são zeros de polinômios definidos na variedade.

Um grupo algébrico é dito *linear* se a variedade G é afim, isto é, um fechado de $\mathbb{C}^n$. Denotando por $\mathbb{C}[G]$ o anel de coordenadas de G, as aplicações π e l induzem homomorfismos entre os anéis de coordenadas de G e $G\times G$, a saber,

$$\pi^*:\mathbb{C}[G]\longrightarrow\mathbb{C}[G]\otimes_{\mathbb{C}}\mathbb{C}[G] \quad \text{e} \quad l^*:\mathbb{C}[G]\longrightarrow\mathbb{C}[G].$$

Estes mapas satisfazem propriedades refletindo a estrutura de grupo de G. Podemos observar que os grupos algébricos estão para as variedades algébricas da mesma forma como os grupos de Lie estão para as variedades diferenciáveis.

Um exemplo que será útil no decorrer do texto é $G=\mathbb{C}$, com a operação de adição. G define um grupo algébrico linear cujo anel de coordenadas é $\mathbb{C}[x]$. Os homomorfismos induzidos são $\pi^*:\mathbb{C}[x]\longrightarrow\mathbb{C}[t,s]$ e $l^*:\mathbb{C}[x]\longrightarrow\mathbb{C}[x]$ definidos por $\pi^*(x)=t+s$ e $l^*(x)=-x$. Este grupo é chamado *grupo aditivo* e denotado por $(\mathbb{C},+)$.

Outro exemplo importante é o grupo das matrizes $n\times n$ invertíveis. Ele é chamado *grupo linear geral* e denotado $\mathbb{GL}_n$ (ou $\mathbb{GL}_n(\mathbb{K})$, quando se faz necessário explicitar o corpo no qual estão as entradas das matrizes). Seu anel de coordenadas é $\mathbb{C}[\mathbb{GL}_n]=\mathbb{C}[x_{ij},\frac{1}{D}]$, onde $1\leq i,j\leq n$ e D é a função determinante. Lembrando que $l(M)=M^{-1}=\frac{adjunta(M)}{D(M)}$ é uma aplicação polinomial, os mapas entre os anéis de coordenadas são

$$\begin{array}{rccc} \pi^*: & \mathbb{C}[\mathbb{GL}_n] & \longrightarrow & \mathbb{C}[\mathbb{GL}_n]\otimes\mathbb{C}[\mathbb{GL}_n] \\ & x_{ij} & \longmapsto & \sum_{k=1}^n x_{ik}\otimes x_{kj} \end{array}$$

e

$$\begin{array}{rccc} l^*: & \mathbb{C}[\mathbb{GL}_n] & \longrightarrow & \mathbb{C}[\mathbb{GL}_n] \\ & x_{kl} & \longmapsto & \frac{(-1)^{l+k}|X_{lk}|}{D(X)}, \end{array}$$

onde denotamos $X = [x_{ij}]_{n\times n}$ e X_{lk} o menor correspondente ao elemento x_{lk}.

Dado um grupo algébrico linear G, e H um subgrupo de G, o fecho $\overline{H}$ é um subgrupo de G. Outra propriedade básica é o fato de, dado um homomorfismo de grupos algébricos lineares $f : G \longrightarrow G'$, o núcleo e a imagem de f serem subgrupos fechados de G e G', respectivamente. As demonstrações destes fatos podem ser encontradas na página 38 de [Springer].

É um importante resultado a respeito dos grupos algébricos lineares, porém de demonstração mais elaborada que os anteriores, a existência de uma representação como um grupo de matrizes. Se G é um grupo algébrico linear, então existem um inteiro positivo n e um isomorfismo de G sobre um subgrupo fechado de $\mathbb{GL}_n$. A demonstração deste fato está na página 42 de [Springer]. Outra referência clássica em grupos algébricos lineares é [Borel], no qual também podem ser encontradas demonstrações para os resultados acima citados.

Grupos unipotentes

Dado um grupo abstrato G, dizemos que um elemento x de G é *unipotente* se $x - 1$ é nilpotente, isto é, se $(x-1)^n = 0$ para algum inteiro positivo n. Um grupo algébrico linear é dito *unipotente* se todos seus elementos são unipotentes. O principal objetivo deste texto é demonstrar o seguinte teorema:

Teorema 1: *Seja G um grupo algébrico linear sobre $\mathbb{C}$. Suponha que G seja comutativo, conexo e unipotente. Então G é isomorfo a $(\mathbb{C}, +)^m$, para algum inteiro positivo m.*

Este resultado é válido para qualquer corpo algebricamente fechado de característica nula, sem qualquer alteração na demonstração aqui apresentada. O seguinte exemplo mostra, contudo, que a hipótese de característica zero é realmente necessária. Nele usamos $\overline{\mathbb{Z}}_2$ para indicar o fecho algébrico de $\mathbb{Z}_2$.

Exemplo: Considere o grupo algébrico linear

$$G = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix} \in \mathbb{GL}_n(\overline{\mathbb{Z}}_2) \right\},$$

no qual a operação é a multiplicação de matrizes. G é uma variedade conexa de dimensão 2, de fato um plano afim, com uma operação que a torna um grupo comutativo unipotente. Tomemos um elemento M em G. Visto que a característica do corpo é 2, temos

$$M^2 = \begin{pmatrix} 1 & 0 & x^2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad , \quad M^3 = \begin{pmatrix} 1 & x & x^2+y \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}$$

e $M^4 = I$. Logo, uma condição necessária e suficiente para que a ordem de M seja 2 é $x = 0$. Caso $x \neq 0$, a ordem do elemento M é 4. Concluímos que G não pode ser isomorfo a $(\overline{\mathbb{Z}}_2, +)^m$, pois todos os elementos deste grupo possuem ordem 2. É interessante destacar o fato de a dimensão de G ser 2, pois como pode ser visto na página 66 de [Springer], um grupo algébrico linear unidimensional sobre $\mathbb{K}$, que seja conexo e unipotente, é isomorfo a $(\mathbb{K}, +)$, mesmo no caso da característica de $\mathbb{K}$ ser positiva.

Com o objetivo de demonstrar o teorema 1, precisamos do seguinte lema, que relaciona subgrupos algébricos conexos de $(\mathbb{C}, +)^n$ e espaços vetoriais.

Lema 2: *Seja H um subgrupo algébrico conexo de $(\mathbb{C}, +)^n$. Então H é um espaço vetorial.*

Demonstração: Como H é subgrupo, H é fechado com relação à soma. Resta mostrar que H é fechado com relação a multiplicação por escalar. Tome v em H. Por ser subgrupo, $nv \in H$ para qualquer valor $n \in \mathbb{Z}$. Defina o mapa

$$\begin{aligned} \mu : \ \mathbb{C} &\longrightarrow \mathbb{C}^n \\ c &\longmapsto cv. \end{aligned}$$

Esta aplicação é um morfismo de variedades. Por definição H é um fechado de $\mathbb{C}^n$ e segue que $\mu^{-1}(H)$ é um fechado em $\mathbb{C}$ que contém $\mathbb{Z}$, um número infinito de pontos. Portanto $\mu^{-1}(H) = \mathbb{C}$ e a demonstração está concluída. ■

Agora estamos preparados para a

Demonstração do teorema 1: Existe uma representação $g : G \hookrightarrow \mathbb{GL}_n$. Segundo [Springer], página 50, por uma mudança de coordenadas podemos considerar $g : G \hookrightarrow \mathbb{U}_n$, onde $\mathbb{U}_n$ é o espaço vetorial das matrizes $n \times n$ unipotentes. Denotando $\mathbb{M}_n$ o espaço das matrizes $n \times n$, considere o morfismo de variedades

$$\begin{array}{rccc} ln: & \mathbb{U}_n & \longrightarrow & \mathbb{M}_n \\ & 1+x & \longmapsto & ln(1+x), \end{array}$$

definido por $ln(1+x) = \sum_0^\infty (-1)^n \frac{x^{n+1}}{n+1}$. Como x é nilpotente, existe n_x tal que $x^n = 0$ para todo $n \geq n_x$, logo este mapa está bem definido. Obtemos uma aplicação composta $ln \circ g : G \longrightarrow \mathbb{M}_n$ que é um homomorfismo de grupos algébricos lineares. De fato,

$$ln \circ g(\overline{x} \cdot \overline{y}) = ln((1+x)(1+y)) = ln(1+x) + ln(1+y) = ln \circ g(\overline{x}) + ln \circ g(\overline{y}),$$

onde a segunda igualdade é válida graças à comutatividade de G. Observe que a operação considerada em $\mathbb{M}_n$ é a adição. Como este grupo é isomorfo a $(\mathbb{C}, +)^{n^2}$, podemos considerar $ln : \mathbb{U}_n \longrightarrow (\mathbb{C}, +)^{n^2}$. Desta forma $ln \circ g(G) \subset (\mathbb{C}, +)^{n^2}$ é subgrupo algébrico conexo. Pelo lema 2, $ln \circ g(G)$ é espaço vetorial, portanto isomorfo a $(\mathbb{C}, +)^m$, para algum $m \leq n^2$. Resta mostrar que $ln \circ g$ é injetiva. Para isto, lançamos mão da aplicação exponencial $exp : \mathcal{N} \longrightarrow \mathbb{M}_n$, definida no conjunto das matrizes nilpotentes $\mathcal{N}$ por $exp(x) = \sum_0^\infty \frac{x^n}{n!}$. Ela está bem definida por uma questão análoga à citada acima para o logaritmo. Visto que $ln(\mathbb{U}_n) \subset \mathcal{N}$, o fato de $exp \circ ln(1+x) = 1+x$ implica a injetividade desejada.■

Agradeço a Israel Vainsencher, cujas idéias são importantes neste trabalho.

Referências

[Borel] A.Borel. *Linear Algebraic Groups.* Benjamin, 1969.

[Springer] T.A.Springer. *Linear Algebraic Groups.* Birkäuser, 1981.

Fábio Xavier Penna
Mestre em Matemática pela UFMG: fabioxp@ig.com.br.