
APLICAÇÕES DA TEORIA DE GALOIS

por

Michèle Audin

A fim de deixar bem claro o que se entende por a teoria de Galois diferencial e como aplica-la, convém dedicar a introdução desta palestra à apresentação de teoremas clássicos de aplicação da teoria de Galois clássica.

A teoria de Galois clássica

A teoria de Galois clássica foi inventada para resolver alguns problemas clássicos, de geometria grega e de equações algébricas.

Os três problemas gregos. — São problemas que possuem uma longa história e são conhecidos respectivamente como

- o quadrado do círculo,
- a duplicação do cubo,
- a trissecção do ângulo.

O problema é de construir, com régua e compasso

- um quadrado de área igual à de um círculo dado
- um cubo de volume igual ao dobro do volume de outro cubo dado
- um ângulo igual à um terço de um ângulo dado.

As figuras a seguir mostram a situação dos dois primeiros problemas. É óbvio que resolver estes pro-



blemas significaria construir o lado do quadrado ou a aresta do cubo procurados. Mas os números construíveis são algébricos, de grau uma potência de 2. As impossibilidades dos problemas gregos decorrem dos factos seguintes.

- O número π é transcendente sobre os racionais
- O grau do número algébrico $\sqrt[3]{2}$ é 3, mas deveria ser uma potência de 2.
- O número $\cos(60^\circ/3)$ é algébrico mas também tem grau 3.

Soluções por meio de radicais. — Para demonstrar o teorema sobre o grau dos números construíveis, só procura a teoria das extensões de corpos, uma teoria bastante eficaz. O problema de resolver as equações por meio de radicais é mais difícil e necessita realmente a teoria de Galois. Seja

$$P(x) = a_0 + a_1x + \cdots + a_nx^n$$

um polinômio, os números a_i sendo racionais. Quando o grau n é igual a 2, as raízes do polinômio são números complexos que se podem escrever por meio de radicais :

$$a_2x^2 + a_1x + a_0 = 0 \Leftrightarrow x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}}{2a_2}.$$

Quando o grau é 3, há também formulas (as formulas de Cardano) : é mais simples e suficiente de escrever a equação

$$x^3 + px + q = 0,$$

as raízes são então

$$x = .$$

Não é muito mais difícil de escrever as raízes em grau 4, mas ninguém estava capaz de fazer mais... quando Abel e Galois mostram que, em geral, em grau 5 ou mais, não há formulas para escrever as raízes por meio de radicais. Por exemplo, a equação

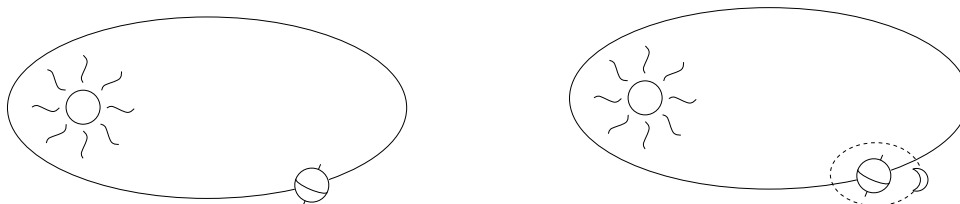
$$x^5 +$$

não é solúvel assim.

A nova ferramenta, inventada por Galois é o grupo de Galois. E seu teorema diz que uma equação algébrica é solúvel por meio de radicais se e só se o o grupo de Galois dela é um grupo « solúvel », quer dizer que é constituído de pedaços que são grupos abelianos. Por exemplo os grupos simétricos $\mathfrak{S}_2$, $\mathfrak{S}_3$, $\mathfrak{S}_4$ são solúveis, mas os grupos $\mathfrak{S}_5$, $\mathfrak{S}_6$, etc. não o são.

Outros problemas famosos

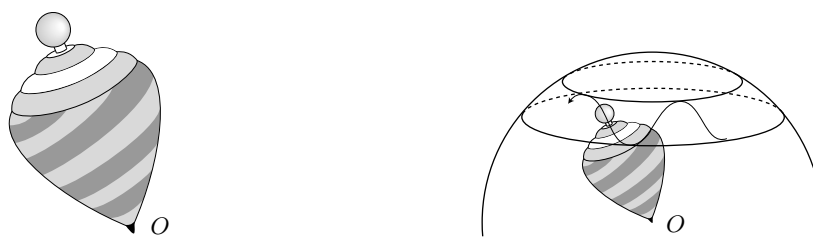
O problema da lua. — O Sol e a Terra constituam um sistema que é chamado « o problema de dois corpos ». É bem conhecido desde Kepler que a trajetória da Terra é uma cônica, como é mostrado sobre a figura a seguir.



O movimento é muito regular. O sistema é integrável. Que tal da lua? Isso é o problema de três corpos. É conhecido, desde Poincaré, que este sistema não é integrável.

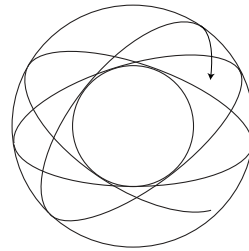
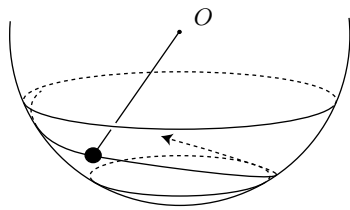
Aqui são outros exemplos de sistemas integráveis.

O pião. — A figura seguinte mostra um pião e também o movimento do seu eixo. A extremidade do

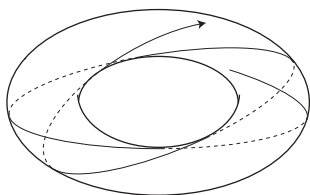
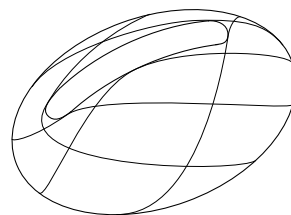
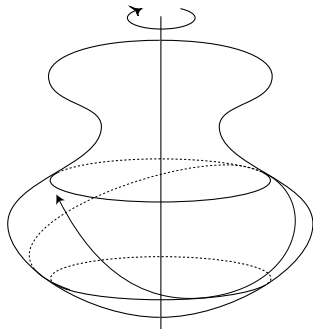


axo de revolução XX

O pendulo « esférico ». — Agora um pendulo e uma trajetória.



Geodésicas. — A trajetória duma partícula livre sobre uma superfície é uma geodésica desta superfície. As figuras seguintes mostram geodésicas duma superfície de revolução e dum elipsóide.



Bandas sobre toros. Uma expressão geométrica ou dinâmica do facto de ser integrável é a regularidade das soluções. O movimento dum sistema integrável é muito regular. As trajetórias ficam sobre toros (é o teorema de Arnold e Liouville) como o mostra a figura.

A teoria de Galois diferencial

É uma teoria análoga de la teoria de Galois clássica, mas agora, nós consideremos equações que são diferenciais em lugar de ser algébricas.

Uma equação diferencial linear é uma equação da forma

$$\frac{d}{dt}Y(t) = A(t)Y(t)$$

onde $Y(t)$ é um vector desconhecido dependendo do tempo e $A(t)$ é uma matriz, também dependendo do tempo.

As equações diferenciais lineares são o análogo nesta teoria das equações algébricas na teoria clássica.

Na teoria clássica, partimos dos números racionais (o corpo $\mathbf{Q}$) e duma equação algébrica sobre este corpo, pois construímos um novo corpo em acrescentar as raízes da equação.

Aqui o análogo do corpo dos números racionais é o corpo das *fracções* racionais. Nós suponhamos que só conhecemos as fracções racionais e consideremos, por exemplo, a equação $y' = y$.

Esta equação é uma equação diferencial linear de ordem 1 (quer dizer que o vector y é um vector dum espaço de dimensão 1). Embora a equação ser muito simples (é análogo, por exemplo da equação $x^2 - 2 = 0$ sobre $\mathbf{Q}$), não tem soluções que sejam fracções racionais (como a $x^2 - 2 = 0$ não tinha soluções em $\mathbf{Q}$).

Nós sabemos todos que o espaço de soluções é o conjunto das fracções $y = C \exp(t)$, um espaço vectorial de dimensão 1.

O conjunto $\mathbf{C}(t)$ das fracções racionais é um corpo, é possível construir um novo corpo, uma extensão de $\mathbf{C}(t)$, a mais pequena extensão naquela nossa equação tem soluções (análogo do corpo das raízes de $x^2 - 2 = 0$). É bastante acrescentar a $\mathbf{C}(t)$ as soluções e considerar o corpo engendrado por $\exp(t)$.

Agora chega a teoria de Galois. O grupo de Galois da equação $x^2 - 2 = 0$ é o grupo das transformações do corpo

$$\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbf{Q}\}$$

que fixam o subcorpo $\mathbf{Q}$, isso é o grupo constituído das transformações

$$a + b\sqrt{2} \mapsto a \pm b\sqrt{2},$$

um grupo de ordem 2, isomorfo ao grupo $\mathbf{Z}/2\mathbf{Z}$.

Do mesmo modo, o grupo de Galois diferencial da equação $y' = y$ é o grupo das transformações do corpo engendrado sobre $\mathbf{C}(t)$ por e^t que fixam o subcorpo $\mathbf{C}(t)$ e são compatíveis com a derivação. Isso é o grupo das transformações

$$e^t \mapsto \lambda e^t,$$

um grupo isomorfo ao grupo multiplicativo $\mathbf{C}^*$ dos números complexos diferentes de zero.

MICHÈLE AUDIN, Institut de Recherche Mathématique Avancée, Université Louis Pasteur et CNRS, 7 rue René Descartes, 67084 Strasbourg cedex, France • *E-mail* : `Michele.Audin@math.u-strasbg.fr`
Url : `http://www-irma.u-strasbg.fr/~maudin`