Aprenda Teoria de Galois (em 24 horas!)

Eduardo Tengan

7 de fevereiro de 2002

Apresentamos aqui alguns resultados básicos da teoria de Galois. Os resultados são clássicos mas a abordagem difere substancialmente de textos como Jacobson, de modo que incluímos diversas provas. Para simplificar a exposição, enunciaremos os resultados para $\mathbb{Q}$, porém é fácil ver que os resultados se estendem *ipsis literis* para corpos de característica 0 e mesmo para corpos de característica positiva.

Para maiores detalhes e outras abordagens, consulte qualquer livro de Álgebra, como por exemplo Jacobson.

1 Polinômios simétricos

O primeiro conceito de que necessitaremos é o de *polinômio simétrico*: um polinômio é *simétrico* se ele não se altera quando intercambiamos duas de suas variáveis. Provavelmente os polinômios simétricos mais simples são os chamados de *polinômios simétricos elementares*:

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\ s_3 &= x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n \\ &\vdots \\ s_n &= x_1 \ldots x_{n-1}x_n \end{aligned}$$

Utilizando os polinômios simétricos elementares, é fácil produzir outros polinômios simétricos, tais como s_2+s_3, $s_1^2s_n$ e, em geral, qualquer polinômio em $s_1, s_2, \ldots, s_n$. O fato interessante é que esta é a *única* maneira de produzir polinômios simétricos. A demonstração é simples e a reproduzimos aqui.

Em primeiro lugar, ordenamos os monômios segundo uma ordem *grau-lexicográfica*, isto é, diremos que $x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n} > x_1^{\beta_1}x_2^{\beta_2}\ldots x_n^{\beta_n}$ se o grau $\sum \alpha_i$ do primeiro monômio for maior do que o grau $\sum \beta_i$ do segundo ou, se os graus forem iguais, o primeiro for lexicograficamente maior do que o segundo (em outras palavras, existe um k tal que $\alpha_i = \beta_i$ para $1 \leq i < k$ e $\alpha_k > \beta_k$). O *termo líder* de

um polinômio é o maior de seus monômios juntamente com seu coeficiente. Por exemplo, o termo líder de

$$f(x_1, x_2, x_3) = 2x_1^2x_2 + 2x_1^2x_3 + 2x_2^2x_1 + 2x_2^2x_3 + 2x_3^2x_1 + 2x_3^2x_2 + x_1 + x_2 + x_3$$

é $2x_1^2x_2$. Agora, dado um polinômio simétrico $p(x_1, \ldots, x_n)$, seja $cx_1^{\alpha_1}x_2^{\alpha_2}\ldots x_n^{\alpha_n}$ o seu termo líder. Já que p é simétrico, devemos ter $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n$. Utilizando os polinômios simétricos elementares, podemos construir outro polinômio simétrico com mesmo termo líder: basta tomar $cs_1^{\alpha_1-\alpha_2}s_2^{\alpha_2-\alpha_3}\ldots s_{n-1}^{\alpha_{n-1}-\alpha_n}s_n^{\alpha_n}$. Agora $p - cs_1^{\alpha_1-\alpha_2}s_2^{\alpha_2-\alpha_3}\ldots s_{n-1}^{\alpha_{n-1}-\alpha_n}s_n^{\alpha_n}$ é um polinômio simétrico com termo líder menor. Repetindo o processo quantas vezes for necessário, obteremos eventualmente 0, ou seja, desta forma teremos escrito p como polinômio em $s_1, s_2, \ldots, s_n$. No exemplo acima, temos

$$f(x_1, x_2, x_3) - 2s_1s_2 = -3x_1x_2x_3 + x_1 + x_2 + x_3$$

com termo líder $-3x_1x_2x_3 < 2x_1^2x_2$. Continuando o processo, obtemos finalmente

$$f(x_1, x_2, x_3) = 2s_1s_2 - 3s_3 + s_1$$

A partir da expressão

$$\prod_{1\leq i\leq n}(x - x_i) = x^n - s_1x^{n-1} + s_2x^{n-2} - \cdots + (-1)^n s_n$$

temos um importante corolário do resultado acima: *qualquer expressão simétrica das raízes de um polinômio com coeficientes em um corpo k pertence também a k.*

Lembramos que um elemento α é *algébrico* sobre um corpo L se α é raiz de um polinômio com coeficientes em L. Como um exemplo, vamos aplicar o corolário para provar que se α é algébrico sobre um corpo L que, por sua vez, é algébrico sobre $\mathbb{Q}$, então α é algébrico sobre $\mathbb{Q}$ (isto é mais difícil de enunciar do que provar!)

Em primeiro lugar, α é raiz de um polinômio

$$\alpha^n + l_{n-1}\cdot\alpha^{n-1} + l_{n-2}\cdot\alpha^{n-2} + \cdots + l_0 = 0$$

com $l_i \in L$. Cada l_i é algébrico sobre $\mathbb{Q}$, então é raiz de um polinômio $p_i(x)$ com coeficientes em $\mathbb{Q}$. Agora considere o produto

$$P(x) = \prod_{l'_{n-1}, l'_{n-2}, \ldots, l'_0}(x^n + l'_{n-1}\cdot x^{n-1} + l'_{n-2}\cdot x^{n-2} + \cdots + l'_0)$$

em que cada l'_i assume todas as raízes de $p_i(x)$. Obviamente os coeficientes do polinômio $P(x)$ são expressões simétricas das raízes de $p_i(x)$ e portanto pertencem a $\mathbb{Q}$. Como $P(\alpha) = 0$ concluímos que α é de fato algébrico sobre $\mathbb{Q}$.

2 Imersões

Se

$$\left(\frac{1}{2-3i}+5i+\frac{1}{7}\right)\cdot\frac{(2+i)\cdot(\frac{3}{4}-5i)}{7+13i}=\frac{276099-158443i}{79352}$$

você pode dizer o valor de

$$\left(\frac{1}{2+3i}-5i+\frac{1}{7}\right)\cdot\frac{(2-i)\cdot(\frac{3}{4}+5i)}{7-13i}?$$

É fácil! Como a segunda expressão é conjugada da primeira, não precisamos repetir as contas novamente, a resposta é simplesmente $(276099+158443i)/79352$. Este fenômeno merece uma atenção maior.

As propriedades da conjugação $\tau(a+bi)=a-bi$, $a,b\in Q$, que utilizamos acima são $\tau(z_1+z_2)=\tau(z_1)+\tau(z_2)$, $\tau(z_1z_2)=\tau(z_1)\tau(z_2)$ e $\tau(z)=z$ para $z\in Q$. Dizemos que uma função $\tau\colon L\to\overline{\mathbb{Q}}$ satisfazendo estas propriedades é uma *imersão* do corpo L em $\overline{\mathbb{Q}}$ sobre Q. A função τ leva i em $-i$, que são as raízes de x^2+1, um polinômio irredutível com coeficientes em $\mathbb{Q}$. De fato, toda imersão σ leva i em i ou $-i$: basta observar que $i^2+1=0\Rightarrow\sigma(i)^2+1=0$, de modo que $\sigma(i)=\pm i$. É claro que não precisamos nos restringir a este caso especial; o mesmo ocorre com as raízes de qualquer polinômio irredutível, isto é, *qualquer imersão leva uma raiz de um polinômio irredutível em $\mathbb{Q}$ em uma raiz do mesmo polinômio*. Em analogia ao caso acima, diremos que raízes de um mesmo polinômio irredutível em $\mathbb{Q}$ são *conjugadas*. Elas terão um importante papel no que segue.

Agora estamos prontos para caracterizar as imersões de uma *extensão algébrica simples*, isto é, um corpo $\mathbb{Q}(\alpha)$ gerado sobre $\mathbb{Q}$ por um único elemento algébrico α. Uma vez que qualquer elemento de $\mathbb{Q}(\alpha)$ é uma função racional (i.e., o quociente de dois polinômios) com coeficientes em $\mathbb{Q}$, tudo o que precisamos para descrever uma imersão é dizer quem é a imagem de α. A discussão acima restringe as possibilidades aos conjugados de α. Então por que não tentar definir $\sigma(r(\alpha))=r(\alpha')$, em que α' é qualquer conjugado de α e $r(\alpha)$ é uma função racional em α? Bem, em primeiro lugar, há várias maneiras de se escrever um elemento como uma função racional (por exemplo $i=i^2+i+1=1/(-i)$), de modo que a função acima pode não estar bem definida. Além disso, ainda precisamos garantir que a função acima é de fato uma imersão. Ambas as questões são tratadas pelo seguinte lema:

Teorema 1 *Se $q(x)$ é um polinômio com coeficientes em $\mathbb{Q}$ tal que $q(\alpha)=0$, então $q(\alpha')=0$ para qualquer conjugado α' de α.*

Seja $p(x)$ o *polinômio minimal* de α, isto é, o polinômio de menor grau com coeficientes em $\mathbb{Q}$ do qual α é raiz. Dividindo $q(x)$ por $p(x)$, podemos escrever $q(x)=a(x)\cdot p(x)+r(x)$, em que $r(x)$ é 0 ou tem grau menor do que $p(x)$. Mas já que $q(\alpha)=a(\alpha)\cdot p(\alpha)+r(\alpha)\Rightarrow r(\alpha)=0$, e $p(x)$ é o polinômio minimal de α, devemos ter $r(x)=0$, ou seja, $p(x)$ divide $q(x)$. Em particular, se α e α' são raízes de um mesmo polinômio irredutível $t(x)$, temos que $t(x)$ é um múltiplo de

$p(x)$, ou seja, $t(x) = c \cdot p(x)$, $c \in \mathbb{Q}$. Assim, α e α' são raízes de $p(x)$ e, portanto, qualquer raiz de $p(x)$ é também raiz de $q(x)$, o que termina a demonstração.

O resultado acima estende-se de maneira óbvia a funções racionais, de modo que se $r(\alpha) = s(\alpha)$, isto é, α é raiz de $r(x) - s(x)$, então $r(\alpha') - s(\alpha') = 0$. Desta forma, a função σ acima realmente está bem definida. Além disso, se $r(\alpha)s(\alpha) = t(\alpha)$, então $r(\alpha')s(\alpha') = t(\alpha') \iff \sigma(r(\alpha))\sigma(s(\alpha)) = \sigma(t(\alpha)) \iff \sigma(r(\alpha))\sigma(s(\alpha)) = \sigma(r(\alpha)s(\alpha))$. Resumimos este importante resultado:

Teorema 2 *Se α é raiz de um polinômio irredutível $p(x)$ de grau d com coeficientes em $\mathbb{Q}$, então existem exatamente d imersões de $\mathbb{Q}(\alpha)$ em $\overline{\mathbb{Q}}$ sobre $\mathbb{Q}$, dadas por $\sigma(\alpha) = \alpha'$, em que α' é qualquer raiz de $p(x)$.*

3 Extensões Simples

Agora que temos uma descrição razoavelmente completa de imersões de extensões simples de $\mathbb{Q}$, o que podemos dizer sobre o resto? Felizmente, podemos reduzir nosso estudo ao caso anterior:

Teorema 3 *(Elemento Primitivo) Seja $L = \mathbb{Q}(\gamma_1, \gamma_2, \ldots, \gamma_n)$ o corpo gerado por elementos γ_i algébricos sobre $\mathbb{Q}$. Então existe um elemento $\theta \in L$ tal que $L = \mathbb{Q}(\theta)$.*

É suficiente provar o resultado para $n = 2$ já que o caso geral segue por indução. Então vamos supor que L é gerado por dois elementos α e β, que são raízes dos polinômios irredutíveis $p(x)$ e $q(x)$, respectivamente. Denotaremos ainda por $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$ e $\beta_1 = \beta, \beta_2, \ldots, \beta_s$ os conjugados destes elementos.

Bem, se estamos tentado encontrar um único gerador para $L = \mathbb{Q}(\alpha, \beta)$, por que não tentar inicialmente um elemento da forma $\theta = \alpha + c\beta$ com $c \in Q$? Se θ gera L sobre $\mathbb{Q}$, então existe um polinômio $m(x)$ com coeficientes em $\mathbb{Q}$ tal que $\alpha = m(\theta)$ (e, portanto, $\beta = (m(\theta) - \alpha)/c$). Guiados por nossa experiência anterior, sabemos que se $\overline{\theta}$ é conjugado de θ, então $\overline{\alpha} = m(\overline{\theta})$. Mas quem são os conjugados de θ? Podemos encontrar facilmente um polinômio que admite θ como uma de suas raízes. Considere

$$t(x) = \prod_{i,j} (x - \alpha_i - c\beta_j)$$

Assim, os conjugados de θ formam um subconjunto de $\{\alpha_i + c\beta_j\}$, e seriam *exatamente* estes elementos se soubéssemos que $t(x)$ é irredutível. Infelizmente, $t(x)$ não precisa ser irredutível. Porém, é ainda possível construir um polinômio $m(x)$ tal que $m(\alpha_i + c\beta_j) = \alpha_i$. Vejamos como.

Escolhemos $c \in \mathbb{Q}$ tal que $\alpha_i + c\beta_j$ são todos distintos. Agora, seja $l(\alpha, \beta) \in L$. Considere o seguinte *polinômio interpolador de Lagrange*

$$m(x) = \sum_{\sigma \in \mathfrak{S}_n} \prod_{\substack{\tau \in \mathfrak{S}_n \\ \tau \neq \sigma}} \frac{(x - \alpha_{\tau(i)} - c\beta_{\tau(i)})}{(\alpha_{\sigma(i)} + c\beta_{\sigma(i)} - \alpha_{\tau(i)} - c\beta_{\tau(i)})} \cdot l(\alpha_{\sigma(i)}, \beta_{\sigma(i)})$$

Os coeficientes de $m(x)$ são funções simétricas de $\alpha_1, \alpha_2, \ldots, \alpha_r$ e $\beta_1, \beta_2, \ldots, \beta_s$, assim temos que estes coeficientes estão em $\mathbb{Q}$. Finalmente, $m(\theta) = m(\alpha + c\beta) = l(\alpha, \beta)$, em outras palavras, $l(\alpha, \beta) \in \mathbb{Q}(\theta)$.

Agora que sabemos que toda extensão algébrica finitamente gerada é simples, podemos definir o *grau de uma extensão*: se $L = K(\alpha)$ e α é raiz de um polinômio irredutível com coeficientes em K e de grau d, dizemos que L tem *grau* d sobre K e escrevemos $d = [L : K]$. Observe que esta noção coincide com a noção usual de grau de L sobre K, sendo L um espaço vetorial sobre K: basta tomar $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ como base. Em particular, a noção de grau está bem definida, isto é, independe da escolha do elemento gerador de α. Temos ainda que o grau é multiplicativo no seguinte sentido: se $E \supset L \supset K$ são corpos, então $[E : K] = [E : L][L : K]$. A demonstração é simples: se ω_i é uma base de E sobre L e τ_j, uma base de L sobre K, é fácil verificar que $\omega_i \tau_j$ é uma base de E sobre K.

4 Automorfismos e Extensões Galoisiana

Um *automorfismo* de um corpo L é uma imersão cuja imagem é o próprio L. Mais explicitamente, uma bijeção $\sigma\colon L \to L$ é automorfismo se $\sigma(x + y) = \sigma(x) + \sigma(y)$ e $\sigma(xy) = \sigma(x)\sigma(y)$ para todo $x, y \in L$. Se K é um subcorpo de L, diremos ainda que σ é um *automorfismo sobre* K se ele fixar cada elemento de K, isto é, se $\sigma(k) = k$ para todo $k \in K$.

É fácil ver que o conjunto de todos os automorfismos de L sobre K formam um grupo. Pela resultados anteriores, temos que há no máximo $[L : K]$ tais automorfismos. Se $L = K(\alpha)$ e todos os conjugados de α pertencem a L, então haverá *exatamente* $[L : K]$ automorfismos, dados por $\sigma(\alpha) = \alpha'$, em que α' é um conjugado de α. Se isto ocorrer, diremos que L é uma *extensão galoisiana* de K. Neste caso, denotamos o grupo de automorfismos de L sobre K por $\mathrm{Gal}(L/K)$.

O jeito mais fácil (de fato, o único jeito) de se obter uma extensão galoisiana é acrescentar a K *todas* as raízes $\alpha_1, \alpha_2, \ldots, \alpha_n$ de um polinômio $p(x)$ com coeficientes em K; neste caso, qualquer imersão σ de $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ permuta as raízes de $p(x)$, já que $p(\sigma(\alpha_i)) = \sigma(p(\alpha_i)) = 0$. Assim, $\sigma(L) = L$ e, portanto σ é um automorfismo de L.

Por exemplo, se $L = \mathbb{Q}(x_1, x_2, \ldots, x_n)$ é o *corpo das funções racionais* e $K = \mathbb{Q}(s_1, s_2, \ldots, s_n)$, o *subcorpo das funções racionais simétricas*, temos que as permutações das variáveis das funções racionais definem automorfismos de L sobre K. Além disso, como

$$\prod_{1 \le i \le n} (x - x_i) = x^n - s_1 x^{n-1} + s_2 x^{n-2} - \cdots + (-1)^n s_n,$$

temos que $L = K(x_1, x_2, \ldots, x_n)$ é uma extensão galoisina de K.

5 Teorema Fundamental

A idéia da teoria de Galois é classificar extensões de corpos através de seus grupos de automorfismos. Vejamos como.

Seja L uma extensão de K. Podemos associar, para cada subcorpo intermediário E (isto é, $L \supset E \supset K$), o subgrupo do grupo de automorfismos de L sobre K que são também automorfismos de L sobre E, ou seja, o subgrupo dos automorfismos que fixam cada elemento de E. Reciprocamente, a cada subgrupo H do grupo de automorfismos de L sobre K, associamos o seu *corpo fixo* $L^H = \{x \in L \mid \sigma(x) = x \quad \forall \sigma \in H\}$.

É natural imaginar se as duas correspondências acima são inversas uma da outra, o que é verdade se exigirmos que L seja extensão galoisiana de K. Neste caso, L é uma extensão galoisiana de E e o temos que o grupo associado a E é nada mais nada menos do que $\mathrm{Gal}(L/E)$.

Temos o seguinte

Teorema 4 (Teorema Fundamental da Teoria de Galois) *Seja L uma extensão galoisiana de K. Então existe uma bijeção entre os subcorpos E de L que contêm K e os subgrupos de* $\mathrm{Gal}(L/K)$*, dada por*

$$E \to \mathrm{Gal}(L/E)$$

e cuja inversa é

$$H \to L^H$$

Demonstração Sejam E um subcorpo de L e $H = \mathrm{Gal}(L/E)$. Pela definição, sabemos que $L^H \supset E$. Para mostrar a inclusão reversa, escrevemos $L = E(\theta)$. Seja $p(x)$ o polinômio minimal de θ sobre E e sejam $\theta_1 = \theta, \theta_2, \ldots, \theta_r$ as raízes conjugadas de θ, que estão em L pois L é uma extensão galoisiana de E. Temos então que os automorfismos de H são dados por $\sigma_i(\theta) = \theta_i$, $i = 1, 2, \ldots, r$. Agora, seja $l \in L^H$, então podemos escrever $l = l(\theta)$ para alguma função racional de θ com coeficientes em E e

$$l = \frac{1}{r} \sum_{\sigma \in H} \sigma(l) = \frac{l(\theta_1) + l(\theta_2) + \cdots + l(\theta_r)}{r},$$

que é uma expressão simétrica das raízes de $p(x)$, logo é um elemento de E. Portanto $L^H \subset E$ e, assim, $L^H = E$.

Para finalizar, temos que se H é um subgrupo de $\mathrm{Gal}(L/K)$ e $E = L^H$, então $H \subset \mathrm{Gal}(L/E)$. Novamente, escrevemos $L = E(\theta)$ e consideramos o polinômio

$$p(x) = \prod_{\sigma \in H} (x - \sigma(\theta))$$

Temos os coeficientes de $p(x)$ são fixados por elementos de H, logo pertencem a E. Assim, $|\mathrm{Gal}(L/E)| = [L : E] \leq |H|$. Da inclusão anterior, concluímos que $H = \mathrm{Gal}(L/E)$.

□

6 Exemplo

Dizem que um exemplo fala mais do 10^3 palavras, então deixe-me tentar desta maneira. Vamos calcular o grupo de Galois do polinômio

$$1 + x + x^2 + \cdots + x^4$$

Este polinômio é irredutível (substitua x por $x+1$ e Eisenstein nele!). Seja ζ uma de suas raízes. Temos $\zeta^5 = 1$ e as raízes demais são ζ^2, ζ^3 e ζ^4. Logo o corpo gerado pelas raízes deste polinômio é simplesmente $\mathbb{Q}(\zeta)$. Assim, temos que os automorfismos de $\mathbb{Q}(\zeta)$ sobre $\mathbb{Q}$ são

$$\begin{aligned} \zeta &\to \zeta \\ \zeta &\to \zeta^2 \\ \zeta &\to \zeta^3 \\ \zeta &\to \zeta^4 \end{aligned}$$

Seja $\sigma(\zeta) = \zeta^2$. Ele gera $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, já que $\sigma^2(\zeta) = \sigma(\zeta^2) = \zeta^4$, $\sigma^3(\zeta) = \zeta^3$ e $\sigma^4(\zeta) = \zeta$. Logo $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ é o grupo cíclico gerado por σ. Seus subgrupos são $\{1\}$, $\{1, \sigma^2\}$ e $\{1, \sigma, \sigma^2, \sigma^3\}$. Os corpos fixos correspondentes estão listados a seguir:

$$\begin{array}{ccc} \{1\} & \leftrightarrow & \mathbb{Q}(\zeta) \\ \cap & & \cup \\ \{1, \sigma^2\} & \leftrightarrow & \mathbb{Q}(\zeta^2 + \zeta^3) \\ \cap & & \cup \\ \{1, \sigma, \sigma^2, \sigma^3\} & \leftrightarrow & \mathbb{Q} \end{array}$$

Para determinar o polinômio minimal de $\zeta^2 + \zeta^3$, basta montar uma equação invariante por todas as potências de σ, por exemplo,

$$(x - (\zeta^2 + \zeta^3))(x - \sigma(\zeta^2 + \zeta^3)) = (x - (\zeta^2 + \zeta^3))(x - (\zeta^4 + \zeta)) = x^2 + x - 1$$

O polinômio minimal de ζ sobre $\mathbb{Q}(\zeta^2 + \zeta^3)$ é obtido da mesma forma:

$$(x - \zeta)(x - \sigma^2(\zeta)) = (x - \zeta)(x - \zeta^4) = x^2 + (1 + \zeta^2 + \zeta^3)x + 1$$

Utilizando estes dois polinômios, podemos calcular ζ:

$$\zeta^2 + \zeta^3 = \frac{-1 \pm \sqrt{5}}{2} \qquad \text{e} \qquad \zeta = \frac{-1 - \frac{-1 \pm \sqrt{5}}{2} \pm \sqrt{(1 + \frac{-1 \pm \sqrt{5}}{2})^2 - 4}}{2}$$

7 Exercícios

1. Calcule o grupo de Galois de um polinômio de grau 2 irredutível.
2. Calcule o grupo de Galois de $1 + x + \cdots + x^{p-1}$ e $x^p - 1$, em que p é primo.

3. Escreva uma expressão para $e^{2\pi i/17}$ utilizando radicais. Mostre como construir um polígono de 17 lados utilizando este resultado.

4. Calcule o grupo de Galois de $x^3 - 3x + 1$.

5. Calcule o grupo de Galois de $x^3 - 2$.

6. Mostre que se $p(x)$ é irredutível, seu grupo de Galois é transitivo: se r e r' são raízes de $p(x)$, existe um automorfismo tal que $\sigma(r) = r'$.