1.º ANO - N.º 4 OUTUBRO DE 1940

GAZETA DE MATEMÁTICA

Redacção e Administração: Faculdade de Ciências — Rua da Escola Politécnica — Lisboa

EDITOR: JOSÉ DUARTE DA SILVA PAULO

Composto e impresso na Soc. Industrial de Tipografia, Limitada R. Almirante Pessanha, 3 e 5 - Lisboa

UM PROBLEMA DE GEOMETRIA ANALÍTICA

Sejam

$$\begin{cases} a\ x+b\ y+c\ =0 \\ a'\ x+b'\ y+c'\ =0 \\ a''\ x+b''\ y+c''=0 \end{cases}$$

as equações de três rectas não concorrentes. E representemos por C, C', C'' *os complementos algébricos dos elementos* c, c', c'' *do determinante*

$$\Delta = \begin{vmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{vmatrix}.$$

A condição necessária e suficiente para que o ponto $P(x_1, y_1)$ *seja interior ao triângulo formado pelas três rectas, é que*

$$(a\ x_1+b\ y_1+c\ )\cdot\frac{C}{\Delta}>0$$

$$(a'\ x_1+b'\ y_1+c')\cdot\frac{C'}{\Delta}>0$$

$$(a''\ x_1+b''\ y_1+c'')\cdot\frac{C''}{\Delta}>0.$$

Na verdade, a identidade

$$(ax+by+c)\cdot\frac{C}{\Delta}+(a'x+b'y+c')\cdot\frac{C'}{\Delta}+(a''x+b''y+c'')\cdot\frac{C''}{\Delta}\equiv 1,$$

dá-nos

$$(ax_1+by_1+c)\cdot\frac{C}{\Delta}\equiv 1>0,$$

no caso particular de o ponto P coïncidir com o *vértice oposto* ao lado de equação $ax+by+c=0$. E se o ponto é interior ao triângulo, o sinal de $ax+by+c$ não varia com êsse ponto (sempre interior!).

Logo,

$$(a\ x_1+b\ y_1+c\ )\cdot\frac{C}{\Delta}>0$$

$$(a'\ x_1+b'\ y_1+c')\cdot\frac{C'}{\Delta}>0$$

$$(a''\ x_1+b''\ y_1+c'')\cdot\frac{C''}{\Delta}>0.$$

— **Êste problema foi enviado à Redacção pelo Professor da Faculdade de Ciências do Pôrto Doutor Madureira e Sousa.**

CORPOS QUADRÁTICOS E SEUS IDEAIS

(CONTINUADO DO N.º 2)

Chama-se norma de um número α ao produto $n(\alpha)=\alpha.\alpha'$, de α pelo seu conjugado, que é igual a $\frac{a_0}{a_2}$, se α satisfaz à equação $a_2x^2+a_1x+a_0=0$, e é um número racional e inteiro se α fôr um inteiro. A norma de um número racional é então igual ao quadrado do módulo e a norma de um inteiro α é um inteiro racional.

É fácil ver que a norma de um produto é igual ao produto das normas dos factores; efectivamente $n(\alpha\beta)=(\alpha\beta)(\alpha\beta)'=\alpha\beta\alpha'\beta'=n(\alpha)\,n(\beta)$, por ser $(\alpha\beta)'=\alpha'\beta'$, isto é o conjugado de um produto igual ao produto dos conjugados.

Chamaremos unidade de um corpo, a qualquer inteiro ε do corpo tal que $\frac{1}{\varepsilon}$ seja também um inteiro ε', e diremos que um inteiro β divide um inteiro α se existir um terceiro γ tal que $\alpha=\beta.\gamma$. Quere dizer então que $\varepsilon\varepsilon'=1$, e portanto ε' é também uma unidade. Uma unidade divide todo o inteiro α do corpo pois que $\frac{\alpha}{\varepsilon}=\frac{1}{\varepsilon}\alpha=\varepsilon'\alpha$ visto que o produto de dois inteiros é um inteiro. No caso do corpo de Gauss as unidades são ± 1 e $\pm i$.

Diremos que dois números α e β são associados se qualquer dêles é divisível pelo outro; tem-se então (7) $\frac{\alpha}{\beta}\cdot\frac{\beta}{\alpha}=1$ e $\alpha=\varepsilon\beta$, isto é, α e β só diferem por um factor unidade. De facto de (7) vem $\alpha=\beta\cdot\frac{\alpha}{\beta}$ e como $\frac{\alpha}{\beta}$ é um inteiro γ e $\frac{\beta}{\alpha}$ é também um inteiro igual a $\frac{1}{\gamma}$, γ é uma unidade ε, e $\alpha=\varepsilon.\beta$.

Concluímos assim que todo o inteiro é divisível pelas unidades do corpo e pelos seus associados; se o inteiro não tiver outros divisores diremos que êle é *indecomponível* no corpo e como vemos esta noção generaliza a de número primo no

corpo R. Demonstra-se que todo o número α cuja norma é um número primo ordinário é indecomponível em $R(\sqrt{m})$.

Se fôr $\alpha=\beta_1\beta_2\cdots\beta_n$, e pertencendo os $\beta\beta$ ao corpo nenhum dêles é uma unidade ou associado a α, diz-se que aquela decomposição de α é *essencial*; e esta decomposição é equivalente à decomposição em factores primos no campo racional.

Concretizemos estas definições num exemplo. Seja o corpo $R(\sqrt{-5})$. Os números do corpo são da forma $\frac{a+b\sqrt{-5}}{c}$, e os inteiros da forma $a+b\sqrt{-5}$; as unidades são ± 1. A norma de um inteiro será $(a+b\sqrt{-5})(a-b\sqrt{-5})=a^2+5b^2$. Mas sucede agora que existem no corpo números que têm mais do que uma decomposição em factores indecomponíveis o que não sucede no corpo dos números racionais, em que a decomposição em factores primos é única. Assim o número $21=3.7=(4+\sqrt{-5})(4-\sqrt{-5})=(1+2\sqrt{-5})(1-2\sqrt{-5})$ em que os inteiros $3, 7, 4+\sqrt{-5}, 4-\sqrt{-5}, 1+2\sqrt{-5}$ e $1-2\sqrt{-5}$ são indecomponíveis em $R(\sqrt{-5})$. De facto se $3=(a+b\sqrt{-5})(a_1+b_1\sqrt{-5})$ então $3=aa_1-5bb_1$ e $0=ab_1+a_1b$, e da última tira-se $\frac{a}{a_1}=-\frac{b}{b_1}=r$ ou $a=ra_1$, e $b=-rb_1$, e por conseqüência $3=ra_1^2+5rb_1^2$ em que ra_1^2 e rb_1^2 são inteiros não negativos, e como para $b_1\neq 0$ $5rb_1^2>3$ a primeira igualdade é impossível e então $b_1=0$, $b=0$, $a=3$ e $a_1=1$ ou $b_1=0$, $b=0$, $a=1$ e $a_1=3$ quere dizer que 3 é indecomponível. Anàlogamente se demonstra que 7 é indecomponível. Se fôsse $4+\sqrt{-5}=(a+b\sqrt{-5})(a_1+b_1\sqrt{-5})$ então tomando as normas, $21=(a^2+5b^2)(a_1^2+5b_1^2)$ e por serem racionais e inteiros os dois membros será $21=a^2+5b^2$ e $1=a_1^2+5b_1^2$ sistema que tem as soluções $(a=4, b=1)(a_1=\pm 1, b_1=0)$ que não satisfazem a (8) e as soluções $a=1, b=2$ e $a_1=\pm 1$, $b_1=0$ ou então $3=a^2+5b^2$ e $7=a_1+5b_1^2$ que é impossível. Logo $4+\sqrt{-5}$ é indecomponível. Demonstrações análogas se fazem para os outros números.

As decomposições de 21 são por isso essencialmente diferentes.

Um número pode assim apresentar, num dado corpo, mais do que uma decomposição em factores indecomponíveis, e como conseqüência tôda a teoria dos números racionais, que assenta na decomposição única de qualquer número em produto de factores primos, é insusceptível de se generalizar.

Para obviar a êste inconveniente, Kummer que o tinha notado quando do estudo da divisão da circunferência em partes iguais, criou o conceito de números ideais, números de que se fazia a adjunção ao corpo.

Mais tarde Dedekind modifica a noção e em vez de um número não pertencente ao corpo introduz um conjunto de números pertencentes ao corpo. Esta noção permite a decomposição única de qualquer número do corpo em factores ideais.

Vejamos num caso particular como se pode explicar o conceito de ideal.

Consideremos o conjunto de números da forma $4n+1$, que não formam evidentemente um corpo, pois que a soma ou diferença de números do conjunto não pertence ao conjunto, mas para os quais o produto e a divisão se podem definir à maneira ordinária.

Seja então a sucessão $1, 5, 9, 13, 17\cdots 73, 77\cdots 141\cdots$ é claro que $(4n+1)\times(4m+1)=4p+1$.

Daquela sucessão os números $5, 9, 13, 17, 21, 29\cdots$ são indecomponíveis no conjunto considerado.

No entanto o número $10857=141\times 77=21\times 517$ pode ser decomposto de 2 modos essencialmente diferentes. Da mesma maneira $693=21\times 33=9\times 77$ e $441=21^2=9\times 49$.

Mas nós sabemos neste caso como restabelecer a decomposição única. Basta juntar ao conjunto dos números considerados, quando por exemplo se trata da decomposição de 10857, os números 3, 7, 11 e 47. De modo que $10857=3\times 7\times 11\times 47$.

Esta era a idéia de Kummer: a adjunção de certos números que não pertencendo ao corpo restabelecem a decomposição única. Notemos que 3 pode ser considerado como o *m. d. c.* de 21 e 141, 7 o *m. d. c.* de 21 e 77, 11 o *m. d. c.* de 77 e 517 e 47 o *m. d. c.* de 141 e 517.

Se designarmos pelo símbolo $j=(a, b)$ o máximo divisor comum dos inteiros a e b o número 3 do exemplo anterior é exactamente igual a $(21, 141)$. E o número 10857 pode escrever-se $10857=(21, 141)(21, 77)(77, 517)(141, 517)$.

Vejamos agora como se define ideal no corpo quadrático, segundo Dedekind.

Chama-se ideal do corpo $R(\sqrt{m})$ e designa-se por $j=(\alpha, \beta, \gamma\cdots)$ um sistema infinito de números do corpo tais que tôda a combinação linear $\alpha\lambda+\beta\mu+\gamma\nu+\cdots$ dos números $\alpha, \beta, \gamma\cdots$ em que os coeficientes $\lambda, \mu, \nu\cdots$ são números inteiros do corpo, pertence ainda ao corpo.

Em particular um ideal chama-se ideal principal, quando os números que o definem são múltiplos dum inteiro do corpo $j=(\alpha, \alpha\lambda, \alpha\mu\cdots)$ escreve-se então $j=(\alpha)$.

Quando um ideal contém 1 ou um divisor ε de 1, chamar-lhe-emos ideal unidade e designa-se pelo símbolo $j=(1)$.

Define-se então, igualdade de ideais, produto de ideais, etc.

Apliquemos agora estes conceitos à decomposição de 21 no corpo $R(\sqrt{-5})$ já estudado.

Formemos os ideais do exemplo anterior $(3, 4+\sqrt{-5})$ $(3, 4-\sqrt{-5})$, $(3, 1+2\sqrt{-5})$, $(3, 1-2\sqrt{-5})$, $(7, 4+\sqrt{-5})$, $(7, 4-\sqrt{-5})$, $(7, 1+2\sqrt{-5})$, $(7, 1-2\sqrt{-5})$, $(4+\sqrt{-5}, 1+2\sqrt{-5})$, $(4+\sqrt{-5}, 1-2\sqrt{-5})$, $(4-\sqrt{-5}, 1+2\sqrt{-5})$, $(4-\sqrt{-5}, 1-2\sqrt{-5})$ o que nos vai permitir tornar única a decomposição 3×7 de 21.

Os ideais que formamos não são todos diferentes uns dos outros. É fácil ver que $(3, 4+\sqrt{-5})=(3, 1-2\sqrt{-5})$ porque $3.3-2(4+\sqrt{-5})=1-2\sqrt{-5}$. Quere dizer $(3, 4+\sqrt{-5})=-(3, 4+\sqrt{-5}, 1-2\sqrt{-5})$. Só são diferentes os ideais $(3, 4+\sqrt{-5})$, $(3, 4-\sqrt{-5})$, $(7, 4+\sqrt{-5})$ e $(7, 4-\sqrt{-5})$; ora $(3)=(3, 4+\sqrt{-5})(3, 4-\sqrt{-5})=(9, 12+3\sqrt{-5}, 12-3\sqrt{-5}, 21, 3)$ porque $3=21-2.9$ e $(7)=(7, 4+\sqrt{-5})(7, 4-\sqrt{-5})=(49, 28+7\sqrt{-5}, 28-7\sqrt{-5}, 21)$ e portanto $21=(3, 4+\sqrt{-5})(3, 4-\sqrt{-5})(7, 4+\sqrt{-5})(7, 4-\sqrt{-5})$ o que restabelece a decomposição única do número 21 no corpo $R(\sqrt{-5})$.

J. DA SILVA PAULO

NOTA: — Os exemplos foram tirados da tradução francesa do livro de J. Sommer, *Introduction à la théorie des nombres algébriques*. Podem consultar-se com proveito àlém dêste livro os seguintes:

Hilbert — *Théorie des corps de nombres algébriques.*

Bianchi — *Teoria dei numeri algebrici.*

J. S. P