

JOSÉ SEBASTIÃO E SILVA
(*Doutor em Ciências Matemáticas,
Professor do Instituto Superior de Agronomia*)

ÁLGEBRA

SEPARATA
DA
«ENCICLOPÉDIA DA VIDA CORRENTE»



LIVRARIA AVELAR MACHADO
LISBOA / 1953

ALGEBRA

O termo *álgebra*, na sua acepção corrente, aplica-se a um ramo da matemática que, na ordem lógica e também, de certo modo, na ordem histórica, ocupa uma posição intermédia entre a aritmética e a análise infinitesimal, tendo de comum com estes domínios fronteiras mal definidas, sujeitas a flutuações no decorrer do tempo. Procuraremos, no que se segue, dar uma ideia da natureza e da evolução dos estudos comumente abrangidos por esta designação.

I. Origens. — A etimologia da palavra encontra-se no título duma obra do matemático árabe Al-Khowarizmi (ou Alkarizmi), aparecida na primeira metade do século IX. O título, *Al-djabr w'al-mukabala*, é composto de dois nomes: o primeiro, *al-djabr* (que se traduziu em latim por *restauratio*), é empregado ali para designar a operação que, na técnica corrente das equações algébricas ⁽¹⁾, consiste em passar um termo dum membro para o outro com troca de sinal; o segundo, *al-mukabala* (em latim *oppositio*), refere-se à redução de termos semelhantes. É de *al-djabr* que deriva manifestamente *álgebra*.

Mas os estudos algébricos não começam aí. A teoria das equações do 1.º e do 2.º grau aparece já, sob as vestes da geometria, nos *Elementos* de Euclides. É preciso notar que os matemáticos gregos, lógicos intransigentes, estavam na posse duma teoria *geométrica* das grandezas, que satisfazia as suas exigências estéticas e racionalistas, mas da qual não tinham conseguido destacar uma correspondente teoria *aritmética* dos números reais: por isso, em todas as questões de álgebra consideravam segmentos de recta em vez de números (v. *número*). Certo é que, para fins utilitários (contas domésticas e comerciais, agrimensura, etc.), os Helenos conheciam uma arte de manejar os números a que davam o nome de *logística*; mas esta não era, como a geometria, uma harmoniosa construção racional que fosse considerada digna das meditações de matemáticos e filósofos. Mais tarde, na segunda escola de Alexandria, vemos a logística tomar o rumo científico pela mão de Diofanto (século IV); porém, trata-se ainda de ensaios cautelosos, demasiado circunscritos ao campo dos números inteiros e dos números fraccionários: para estender a teoria ao caso dos números irracionais (correspondente ao das grandezas incomensuráveis), Diofanto regressava ao método geométrico.

A emancipação da álgebra deve-se principalmente aos Indianos — inventores do sistema de numeração decimal —, que, pondo de parte preocupações de rigor lógico, visavam de preferência as aplicações práticas. São eles que, em cálculos audaciosos, não justificados, se decidem a utilizar abertamente os números irracionais e os números negativos, distinguindo os dois valores da raiz quadrada e colocando indiferentemente numa soma os termos negativos antes ou depois dos positivos.

Finalmente, os Árabes — traço de união entre Oriente e Ocidente — efectuam a síntese fecunda do pragmatismo indiano com o racionalismo grego e, neste sentido, são eles os fautores da álgebra como ciência de carácter autónomo, conquanto ligada ainda, pelos fundamentos teóricos, à mãe geometria. Só em fins do século passado, com a aritmetização da análise efectuada por Dedekind,

⁽¹⁾ Para respeitar a ordem histórica há que inverter em parte a ordem lógica; só mais adiante se tratará da teoria das equações.

Cantor e Weierstrass, a álgebra consegue desvincular-se inteiramente da tutela geométrica (v. *número*). Porém, já desde o século XVII, com a criação da geometria analítica, se vinha observando uma inversão de valores a respeito do período da álgebra geométrica: era então a geometria que começava a exprimir-se na linguagem fluente e poderosa da análise.

II. Álgebra clássica. — 1. *O que distingue a álgebra da aritmética.* — Se nos colocarmos no ponto de vista «ingênuo», que é o do estudante que se abeira do mundo algébrico, a passagem da aritmética para a álgebra caracteriza-se materialmente por três factos principais:

a) Aparecem os números negativos;

b) Introduce-se o cálculo de *expressões literais* (isto é, de expressões com letras), a contrastar com o cálculo *numérico* próprio da aritmética;

c) Inicia-se o estudo das equações.

Quanto aos números negativos, só um critério estritamente histórico autorizaria a considerá-los como entidades estranhas à aritmética. Historicamente, foi o estudo das equações que conduziu aos números negativos (e mais tarde aos números imaginários) como soluções de natureza especial, a interpretar em cada caso. Mas a estruturação do conceito de número, nas suas formas sucessivas (número natural, número racional, número real, número complexo), é da competência da aritmética — pelo menos duma aritmética em sentido lato, como ciência dos números considerados *individualmente*.

Os tópicos b) e c) (principalmente o último) são mais aptos a marcar a transição da aritmética para álgebra. Observa-se, no entanto, que o simbolismo algébrico, com a sua forma actual, só no século XVII começou a ser usado, após uma longa evolução em que, da linguagem escrita comum, se passou a uma espécie de estenografia com base em abreviaturas e em certas convenções (*álgebra sincopada*), para finalmente se chegar à concisa e penetrante linguagem de símbolos hoje empregada (*álgebra simbólica*).

O principal carácter distintivo da álgebra simbólica está no uso que faz das letras. Note-se que os caracteres alfabéticos têm sido usados em aritmética para designar *núme-*

LIBRO DE ALGEBRA EN ARITHMETICA Y GEOMETRIA.

Compuesto por el Doctor Pedro Nuñez, Cosmographo Mayor del Rey de Portugal, y Cathedratico Jubilado en la Cathedra de Mathematicas en la Vniuersidad de Coymbra.



EN ANVERS.

En casa de la Buuda y herederos
de Iuan Stelfio.

1567.

CON PRIVILEGIO REAL.

Nesta obra, uma das mais representativas da sua época, a álgebra é tratada segundo a concepção árabe: a forma é numérica (tradição indiana), mas, por falta dum conceito aritmético de número irracional, os fundamentos teóricos são geométricos (tradição grega). A obra situa-se no período da linguagem sincopada

ros *determinados*, como, por exemplo, sucedia entre os antigos gregos e romanos (v. *algarismo*); ainda hoje, sem falar da numeração romana, subsiste esse uso para certos números, tais como os irracionais e , π e o imaginário i , ligados pela relação $e^{i\pi} = -1$. Mas no simbolismo algébrico as letras são, pelo contrário, usadas principalmente como *variáveis numéricas*, isto é, para designar indistintamente qualquer número pertencente a um dado campo, ou então como *incógnitas*, isto é, como designações de *quantidades desconhecidas*, a determinar.

Seja, por exemplo, a expressão literal $3x^2y - 2x$; aqui as letras x e y podem ter como valores *números quaisquer, não determinados*: são pois *variáveis*. O valor da expressão $3x^2y - 2x$ será ele mesmo indeterminado; porém, esse valor depende ou é *função* das variáveis x , y , querendo-se com isto dizer que se torna determinado logo que o sejam os valores de x e de y ; assim, se fizermos $x = -2$ e $y = 1$, a expressão tomará o valor $3 \times (-2)^2 \times 1 - 2 \times (-2) = 16$, e análogamente para qualquer outro par de valores de x , y .

Para aumentar as possibilidades de notação, as letras são escolhidas em vários alfabetos e tipos (latino, grego, gótico, cursivo, etc.), maiúsculas ou minúsculas, e usam-se simples ou então diferenciadas por meio de índices, plicas, asteriscos, etc.: $a, b, \dots, x, y, \dots, \alpha, \beta, \dots, \zeta, \eta, \dots, a', a'', \dots, \alpha_0, \alpha_1, \alpha_2, \dots, \Phi^*, \Phi^{**}, \dots$

A vantagem do uso das expressões literais torna-se patente desde logo a respeito das fórmulas que traduzem leis geométricas ou físicas; tal é, por exemplo, o caso da fórmula que dá o volume, V , dum cone, como função do raio, r , da base e da altura, h , do cone:

$$V = \frac{1}{3} \pi r^2 h;$$

aqui as variáveis são V , r e h , porque a letra π , essa, está a designar o já citado número irracional.

É de notar ainda que as letras são igualmente usadas como variáveis nas demonstrações de aritmética racional; todavia, os cálculos e os teoremas da aritmética aplicam-se a *números*, enquanto os da álgebra dizem respeito a *expressões literais* — e é aqui que começa verdadeiramente a diferenciação dos dois campos. De certo modo, poderíamos dizer que as operações da álgebra são raciocínios da aritmética convertidos em cálculo, isto é, em mecanismo formal. Neste sentido, podemos dizer também que a álgebra *contém* a aritmética.

2. *Alguns pormenores sobre a passagem da forma sincopada à forma simbólica.* — Os primórdios da álgebra sincopada não se encontram claramente definidos: há quem os localize em Diofanto, mas nesse ponto as opiniões divergem.

A última fase da linguagem sincopada pertence, por exemplo, o *Libro de Álgebra en Arithmetica y Geometria*, do matemático português Pedro Nunes, publicado em 1567, em língua castelhana. Como o título indica, trata-se duma álgebra no sentido árabe: geométrica nas demonstrações, numérica na prática (com predomínio da influência grega, que se traduz em particular na rejeição dos números negativos, ainda não incorporados, ao tempo, numa doutrina racional). Como vários dos seus contemporâneos, o autor indica a adição com a sigla \tilde{p} , abreviatura de *plus* (em vez do sinal $+$, hoje usado), a subtração com a sigla \tilde{m} , abreviatura de *minus* (em vez de $-$), a raiz quadrada com a letra R , a raiz cúbica com $3R$, etc.; nas equações designa a incógnita por *.co.* (*coisa*), o quadrado da incógnita por *.ce.* (*censo*), o cubo da incógnita por *.cu.* (*cubo*), o termo independente da incógnita por *.nu.* (*número*), etc. (Nesta época o conceito de variável confunde-se praticamente com o de incógnita, já que o estudo das expressões algébricas é então considerado apenas como fase preparatória da teoria das equações).

Para exemplo, consideremos o seguinte problema estudado por Pedro Nunes: «Partamos .10. en tales dos partes que los sus quadrados juntos hagan .60.».

Segundo o moderno sistema simbólico, a resolução pode conduzir-se nestes termos: designemos uma das partes procuradas por x ; então a outra será $10 - x$; pretende-se que «a soma dos quadrados das duas partes seja 60»: esta condição é simbolicamente expressa pela fórmula $x^2 + (10 - x)^2 = 60$, que é uma *equação*

equivalente a, estoura: $40 + 2x^2 = 20x$; tratando-a pelos métodos usuais (v. mais adiante n.ºs 5, 6 e 9), obtêm-se as soluções: $x' = 5 - \sqrt{5}$, $x'' = 5 + \sqrt{5}$.

Ora, adoptando o sistema da linguagem sincopada, Pedro Nunes designa um dos números pedidos por .co., o outro por .10. \tilde{m} .co. e, depois de efectuados os devidos cálculos, chega à mesma equação, assim formulada:

$$.40.\tilde{p}.2.ce. \text{ son yguales a } .20.co.,$$

cuja solução apresenta sob a forma: .5. \tilde{m} .R.5., 5. \tilde{p} .R.5. E são estes afinal os números pedidos — não esquecendo que .R.5. (ou seja $\sqrt{5}$) é um número *irrational*, a que o nosso géometra chama *raiz surda* («La razon del nombre deve ser, porque se puede dar en linea y mostrar a la vista, pero no se puede oyr lo que se representa, y por esso la llaman sorda»).

A respeito da regra de Tartaglia (v. mais adiante n.º 9), diz Pedro Nunes: «Es esta Regla [...] muy cierta para saber el valor de la cosa, quando cosas e cubo son yguales a numero [...]» — referindo-se a equações do tipo $ax + x^3 = b$, como, por exemplo, esta: .3.co. \tilde{p} .1.cu. son yguales a .10. (Três coisas mais um cubo são iguais a 10).

Um inconveniente do anterior sistema é o de não se aplicar aos casos em que intervêm mais de uma incógnita. Quando isto sucede, Pedro Nunes designa uma das quantidades desconhecidas por .co. e, quanto às outras, diz, por exemplo, o *segundo* (número), o *terceiro*, etc., alternando pitorescamente a linguagem sincopada com a linguagem comum. (Os Indianos distinguem as incógnitas atribuindo a cada incógnita uma *cor*, indicada em abreviatura).

Certos autores começam já nesta época a usar letras isoladas, designando, por exemplo, a incógnita por *R* (*res*), o seu quadrado por *C* ou *Z* (*census* ou *zensus*), etc. Mas ainda aqui subsiste, entre outros, o inconveniente de se encobrir a relação entre a quantidade desconhecida e as suas potências. Em 1553 o algebrista alemão Stifel dá um passo decisivo a caminho da notação simbólica, escrevendo 1*A*, 1*AA*, 1*AAA* para nomear a incógnita, o seu quadrado e o seu cubo.

Todavia, já no século XIII Jordanus, matemático alemão pouco conhecido na sua época, tinha usado letras para designar quantidades desconhecidas e mesmo quantidades não especificadas.

Como principal promotor da álgebra simbólica costuma apontar-se o francês Viète, que, segundo consta, foi o primeiro algebrista a usar sistematicamente as letras no papel de incógnitas e de variáveis. Dizia Viète, em expressiva terminologia, que tinha criado assim uma *logistica speciosa* (cálculo das *espécies*, isto é, dos entes abstractos, que são as variáveis numéricas), a par da *logistica numerosa*, que é o cálculo numérico ordinário. Mas algumas das suas notações ainda estão longe da simplicidade das actuais, sendo mesmo inferiores às de Stifel; por exemplo, a equação

$$3BA^2 - DA + A^3 = Z,$$

em que *A* é a incógnita, escrever-se-ia no sistema de Viète:

$$B3 \text{ in } A \text{ quad.} - D \text{ plano in } A + A \text{ cubo } \text{æquatur } Z \text{ solido } (^1).$$

Viète representava as quantidades conhecidas por consoantes (*B*, *C*, *D*, etc.) e as incógnitas por vogais (*A*, *E*, *I*, etc.), podendo assim, em particular, distinguir várias incógnitas numa mesma equação (neste último ponto parece que foi antecedido por Jordanus e Stifel).

Foram Harriot (inglês) e Descartes que mais contribuíram para o aperfeiçoamento e a difusão da álgebra simbólica. A Descartes se deve em particular a ideia de omitir o sinal de multiplicação entre factores (por exemplo, $a b c$ em vez de $a \times b \times c$) e a introdução dos expoentes naturais, escrevendo, por exemplo, a^3 em vez de $a a a$, a^4 em vez de $a a a a$, etc. (em 1637).

Estava finalmente constituído um dos mais poderosos instrumentos de análise que o homem tem hoje à sua disposição.

(¹) Exemplo dado por Rouse Ball.

3. *Expressões numéricas e expressões literais; equivalências.* — Para melhor apreender a essência da álgebra convém deter um pouco a atenção sobre a morfologia e a sintaxe da linguagem simbólica.

As *expressões numéricas* da aritmética, tais como $5 \times (3 - 0,7)^2$, $\sqrt{3} - 1$, etc., entram na categoria dos *nomes* (ou *designações*), visto que nomeiam ou designam números. Por sua vez, as igualdades e as desigualdades numéricas, tais como $3^2 + 4^2 = 5^2$, $2 - 7 > 0$, etc., são *proposições* (ou *afirmações*), pois que exprimem juízos, verdadeiros ou falsos.

Valor duma expressão numérica é o número por ela nomeado. Duas expressões numéricas dizem-se *equivalentes* (ou *sinónimas*) quando têm o mesmo valor; para indicar este facto escreve-se entre ambas o sinal = (ler «igual a», ou «o mesmo que»), que exprime identidade, não entre as expressões, mas sim entre os seus valores. Por exemplo, são sinónimas as expressões $1 - (3/5)^2$ e $2 \times 0,32$; o mesmo se pode dizer das expressões $\sqrt{3} - 1$ e $\sqrt{4 - \sqrt{12}}$, etc.

Os nomes dos números são também chamados *constantes numéricas*, por oposição às variáveis, que não designam números determinados ⁽¹⁾.

As expressões com variáveis, tais como Rt^2 , $\sqrt{1 - u^2}$, etc., não são nomes de números, mas passam a sê-lo desde que as variáveis sejam substituídas por constantes numéricas. Uma tal expressão é constituída por variáveis e, eventualmente, por constantes numéricas, ligadas entre si por sinais de operações (+, —, $\sqrt{\quad}$, etc.), segundo certos preceitos que, em particular, se referem ao uso dos parênteses. A expressão diz-se precisamente *algébrica* quando as operações nela indicadas são no máximo as seguintes: *adição, subtracção, multiplicação, divisão e extracções de raiz* (incluindo o uso de expoentes naturais para indicação abreviada de produtos com factores iguais); se não há nenhum sinal debaixo do sinal de radical, a expressão algébrica diz-se *racional* (*irracional* no caso oposto); se, além disso, não figura nenhuma variável em denominador, a expressão racional diz-se *inteira* (*fraccionária* no caso oposto). Por exemplo, as expressões algébricas

$$\frac{2}{3}x(3xy - 1)^2, \quad 3y - \frac{\sqrt{2}}{1 + y^3}, \quad 2x + \sqrt[3]{1 - \sqrt{x^2 - 1}}$$

são, respectivamente, inteira, fraccionária e irracional.

Duas expressões algébricas, com uma ou mais variáveis x, y, \dots , dizem-se *formalmente equivalentes* (ou apenas *equivalentes*), quando assumem o mesmo valor, *todas as vezes* que as variáveis x, y, \dots são substituídas por constantes. Por exemplo, prova-se facilmente que as expressões

$$x^2 - 9y^2 \quad \text{e} \quad (x + 3y)(x - 3y)$$

são equivalentes. A passagem duma dada expressão algébrica a outra que lhe seja equivalente é efectuada segundo certas normas fixas, que se reduzem sempre, em última análise, a aplicar as *propriedades fundamentais das operações elementares da aritmética*. Para saber precisamente o que se entende por tais propriedades ver *estruturas algébricas* e *número*. Entretanto indicaremos aqui pelos seus nomes as mais utilizadas:

a) Da adição: *uniformidade, associatividade, comutatividade, neutralidade do zero, existência dum simétrico para cada número*;

b) Da multiplicação: *uniformidade, associatividade, comutatividade, neutralidade da unidade, existência dum inverso para cada número diferente de zero*;

c) Mista: *distributividade da multiplicação a respeito da adição*.

A adição, a multiplicação e as respectivas operações inversas (subtracção e divisão) costumam ainda ser chamadas *operações racionais*.

Quando duas expressões são equivalentes, também se diz que representam a mesma *função* das variáveis nelas contidas; assim, as expressões $(1 - 2x)^2$ e $1 - 4x + 4x^2$ representam uma mesma função de x . Diz-se *racional* toda a função representável por uma expressão racional (*inteira*, se representável por uma

⁽¹⁾ Em matemática é frequente chamar *constantes* aos próprios números, confundindo estes com os símbolos que os representam. Esta confusão é muitas vezes propositada, com o fim de simplificar a linguagem.

expressão inteira; *fraccionária*, no caso oposto). Porém, como se verá mais adiante, o termo *função algébrica* costuma ser aplicado a uma categoria mais extensa do que a das funções representáveis por meio de expressões algébricas.

Para indicar que duas expressões literais são equivalentes escreve-se entre elas o sinal \equiv . Exemplo: $(1 - 2x)^2 \equiv 1 - 4x + 4x^2$.

Pelas transformações de equivalência procura-se muitas vezes reduzir as expressões algébricas a determinadas formas típicas (ou *formas canónicas*), mais cómodas para certos fins. Geralmente, trata-se duma operação de «arranjo e simplificação», a que não é estranho o sentido estético (a linguagem simbólica possui também a sua estilística). É o que se verá exemplificado no número seguinte.

4. *Monómios e polinómios; funções racionais* ⁽¹⁾. — Chamam-se *monómios* as expressões algébricas inteiras, em que não vêm indicadas adições nem subtrações. Todo o monómio pode ser «arranjado» de maneira a ficar formado por um factor numérico (*coeficiente*), seguido de letras não repetidas, com expoentes naturais (*parte literal*). Chama-se *grau do monómio* a soma dos expoentes das suas letras. Por exemplo, a expressão $-7x^3yz^2$ é um monómio de coeficiente -7 e de grau $3 + 1 + 2 = 6$.

Ligando dois monómios por sinal multiplicativo obtém-se ainda um monómio, chamado *produto* dos primeiros e que pode igualmente ser reduzido à forma canónica, aplicando as propriedades associativa e comutativa da multiplicação. Exemplo:

$$\left(\frac{2}{3} r^2 h\right) \cdot (-6 m r h^3) \equiv \left[\frac{2}{3} \times (-6)\right] m (r^2 \cdot r) (h \cdot h^3) \equiv -4 m r^3 h^4;$$

isto é, multiplicam-se os coeficientes e somam-se os expoentes das variáveis comuns, ficando as variáveis não comuns com o mesmo expoente.

Diz-se *polinómio* toda a expressão (inteira) que se obtém ligando por sinais de $+$ ou de $-$ dois ou mais monómios, que passam então a chamar-se *termos do polinómio*. (Para comodidade de linguagem costuma incluir-se os monómios na categoria dos polinómios). *Grau dum polinómio* é o maior dos graus dos seus termos. Por exemplo, a expressão

$$-2x^3y^2 + yz^2 + \frac{1}{2}x^2z + 5x^3y^2$$

é um polinómio em x, y, z , de grau 5. Aos polinómios do 1.º grau aplica-se também a designação de *lineares*.

Dizem-se *semelhantes* dois monómios que tenham a mesma parte literal. Quando num polinómio figuram dois ou mais termos semelhantes entre si, podemos sempre substituí-los por um único termo com a mesma parte literal e tendo por coeficiente a soma dos coeficientes dos primeiros; nisto consiste a redução de termos semelhantes de que já falámos a propósito das origens da álgebra; as propriedades operatórias aplicadas são: associatividade e comutatividade da adição, distributividade da multiplicação a respeito da adição. Por exemplo, no anterior polinómio os termos semelhantes $-2x^3y^2$ e $5x^3y^2$ podem ser contraídos no termo único $(-2 + 5)x^3y^2$, ou seja $3x^3y^2$.

Ligando por sinal aditivo dois polinómios, obtém-se ainda um polinómio, chamado *soma* dos primeiros (no qual convirá fazer a redução dos termos semelhantes).

Ligando por notação multiplicativa dois polinómios (encerrados entre parênteses), obtém-se uma nova expressão inteira, que não é, em geral, um polinómio, mas que se reduz por equivalência a um polinómio, chamado *produto* dos primeiros. Para obter o produto de dois polinómios basta aplicar a propriedade distributiva: *multiplicam-se todos os termos de um por todos os termos do outro e somam-se os resultados obtidos*. Exemplo:

$$(x - 2y)(x^2 + 2xy + 4y^2) \equiv x^3 + 2x^2y + 4xy^2 - 2x^2y - 4xy^2 - 8y^3 \equiv x^3 - 8y^3$$

⁽¹⁾ Este número pode, sem inconveniente, ser lido após o n.º 7, ou mesmo ser dispensado, desde que o leitor não tenha interesse especial em esclarecer os conceitos aqui precisados.

Dos factos anteriores decorre facilmente o seguinte: *toda a expressão algébrica inteira é equivalente a um polinómio.*

Merecem particular atenção os polinómios numa só variável. A estes, além da redução dos termos semelhantes, costuma ser dado um arranjo que consiste em dispor os termos segundo a ordem crescente ou decrescente dos expoentes.

Geralmente, prefere-se ordenar o polinómio em sentido decrescente. Deste modo, um polinómio do 1.º grau em x , na forma canónica, será uma expressão do tipo $a_0x + a_1$, em que nos lugares de a_0 e a_1 figuram números quaisquer, sendo $a_0 \neq 0$; por sua vez, a forma canónica dos polinómios do 2.º grau será $a_0x^2 + a_1x + a_2$, com $a_0 \neq 0$, etc. Em geral, um polinómio em x de grau n (n inteiro ≥ 0) será, na forma canónica, uma expressão do tipo

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_{n-1}x + a_n,$$

em que nos lugares de a_0, a_1, \dots, a_n figuram números quaisquer (*coeficientes do polinómio*), sendo $a_0 \neq 0$. Por exemplo, $x^3 - 2x^2 + 1$ é um polinómio do 3.º grau em x , que tem por coeficientes: $a_0 = 1, a_1 = -2, a_2 = 0, a_3 = 1$. Em particular, pode ser $n = 0$: trata-se então dum polinómio de grau 0, que se reduz ao termo independente, a_n .

Para a adição de polinómios numa só variável costuma usar-se um esquema prático que se assemelha muito ao processo normalmente usado para a adição de números inteiros. Consiste esse esquema em dispor os polinómios em várias linhas, de modo que termos semelhantes fiquem numa mesma coluna, o que torna mais cómoda a redução de tais termos. Sejam, por exemplo, os polinómios $2 - 5x + x^2 + 3x^4$ e $3 + 7x - 5x^2 + 2x^3$; ter-se-á então:

$$\begin{array}{r} 2 - 5x + x^2 + 0.x^3 + 3x^4 \\ 3 + 7x - 5x^2 + 2x^3 + 0.x^4 \\ \hline \text{Soma} \quad 5 + 2x - 4x^2 + 2x^3 + 3x^4 \end{array}$$

Mas a analogia formal entre o cálculo de polinómios e o cálculo de números inteiros não se limita a este caso trivial: prolonga-se em vários outros algoritmos, tais como o da multiplicação, o da divisão e o *algoritmo de Euclides* (ou *método das divisões sucessivas*, para o cálculo do máximo divisor comum). A analogia é sobretudo notável na *teoria da divisibilidade*, que se pode transportar, com ligeiras variantes, do campo dos números inteiros para o campo dos polinómios.

Quanto às expressões algébricas fraccionárias, diremos apenas que se demonstra, sob certas reservas, o seguinte facto: «Toda a expressão racional é redutível à forma duma fracção cujos termos são polinómios». Por exemplo, a expressão racional

$$2x - \frac{y}{x - \frac{1}{x}}$$

é equivalente à fracção

$$\frac{2x^3 - 2x - xy}{x^2 - 1}$$

De resto, o cálculo destas fracções é feito segundo regras muito semelhantes às que regem o cálculo de fracções numéricas.

Quanto às expressões algébricas irracionais, o seu estudo é bem mais delicado, relacionando-se intimamente com o das equações algébricas; na verdade, os radicais correspondem a equações disfarçadas, de tipo particular (*equações binómicas*). Assim, por exemplo, $\sqrt[5]{9}$ designa uma qualquer das *cinco* soluções da equação $x^5 - 9 = 0$ (v. *número*).

5. *Equações; identidades.* — Dá-se o nome de *equação* a toda a fórmula que se obtém ligando pelo sinal de igual duas quaisquer expressões com uma ou mais variáveis. As duas expressões assim ligadas dizem-se *membros* da equação; as variáveis passam a chamar-se *incógnitas*. A origem deste último termo está em



FRANÇOIS VIÈTE
(1540-1603)

O simbolismo algébrico, tal como hoje se usa, não é obra dum só matemático. Mas, segundo se admite geralmente, foi Viète o primeiro algebrista que fez reconhecer as vantagens do uso sistemático das letras para designar quantidades não conhecidas (incógnitas) e quantidades não especificadas (variáveis). A introdução do conceito matemático de *variável* é um dos acontecimentos capitais na história do pensamento



NICOLÒ TARTAGLIA
(1499-1557)

A primeira conquista essencial no campo da álgebra, para além dos limites da ciência helénica, é a descoberta da regra de Tartaglia, que fornece a resolução algébrica da equação geral do 3.º grau. Esta regra, que foi primeiro achada por Scipione del Ferro (falecido em 1526) e depois redescoberta por Tartaglia, determinou por sua vez a criação do cálculo com número imaginários

que a equação traduz um problema, uma pergunta — e não uma afirmação. Se a equação tem uma só incógnita, o problema põe-se nestes termos:

«Achar um número que, tomado como valor da incógnita, converta a equação numa igualdade numérica verdadeira».

O número pedido tem o nome de *solução* ou *raiz* da equação. Mas pode uma equação ter várias soluções e pode também não ter nenhuma. Por exemplo, a fórmula

$$x(3x+1)=1-x$$

é uma equação que admite como solução qualquer dos números -1 , $1/3$, visto serem verdadeiras ambas as igualdades seguintes:

$$(-1) \cdot [3 \cdot (-1) + 1] = 1 - (-1) \quad , \quad \frac{1}{3} \cdot \left(3 \cdot \frac{1}{3} + 1\right) = 1 - \frac{1}{3}.$$

Uma equação diz-se *resolúvel* ou *possível* se admite pelo menos uma solução; *impossível*, no caso oposto. Por exemplo, a equação $x^2+3=1$ é impossível no campo dos números reais, enquanto a equação $x-1=x+7$ é impossível mesmo no campo dos números complexos.

Quando a equação tem mais de uma incógnita, entende-se por solução ou raiz da equação todo o agrupamento de números que, como valores das incógnitas, convertem a equação numa igualdade numérica verdadeira. Assim, a fórmula

$$2x^2 + y^2 + z^2 = 25$$

é uma equação nas três incógnitas x, y, z , que admite *infinitas* soluções, uma das quais é o terno de números 0, —3, 4, assim localizados:

$$x = 0, y = -3, z = 4,$$

outra solução será: $x = \sqrt{8}, y = 3, z = 0$; etc.

Uma equação diz-se *algébrica* se ambos os seus membros são expressões algébricas (*transcendente*, no caso oposto). Uma equação algébrica diz-se *racional* se ambos os membros são expressões racionais (*irracional*, no caso oposto); diz-se *inteira* se ambos os membros são expressões inteiras (*fraccionária*, no caso oposto).

Pode acontecer que uma equação admita como soluções *todos* os números ou agrupamentos de números que existem [exemplo: a equação $(1-3x)^2 = 1-6x+9x^2$]; costuma dizer-se neste caso que a equação se reduz a uma *identidade*. Porém, a identidade não traduz, como a equação, uma pergunta, mas sim uma afirmação, um *teorema*: afirma que os dois membros são equivalentes. Por isso, a fim de não confundir os dois conceitos, convém usar o sinal \equiv , em vez do sinal $=$, quando se trata duma identidade. Por conseguinte, enquanto traduz um problema nos termos acima precisados, a igualdade literal é sempre uma equação. (É este um dos pontos em que as ideias tradicionais tiveram de ser corrigidas por uma análise lógica moderna).

6. *Equações equivalentes; sistemas de equações.* — Uma equação diz-se *equivalente* a uma outra quando toda a solução da primeira é também solução da segunda e vice-versa. Consegue-se, por vezes, resolver uma dada equação, transformando-a sucessivamente em equações equivalentes à primeira, até se chegar a uma equação que já se sabe resolver. Estas transformações, quando algébricas, assentam em certos princípios, que se deduzem das já referidas propriedades fundamentais das operações aritméticas.

Entre os princípios de equivalência mais usados citaremos os três seguintes:

a) Substituindo qualquer dos membros duma equação por uma expressão equivalente, obtém-se uma equação equivalente à primeira;

b) Se a ambos os membros duma equação numa incógnita x adicionarmos uma mesma expressão algébrica *inteira* em x , obtemos uma equação equivalente à primeira;

c) Multiplicando ambos os membros duma equação por um mesmo número *diferente de 0*, obtém-se uma equação equivalente à primeira.

É a regra b) que torna legítimo passar um termo dum membro para o outro com troca de sinal, operação esta que Al-Khowarizmi designou por *al-djabr*, origem do vocábulo *álgebra*.

Seja, por exemplo, a equação $2x - 3 = 7 - 3x$. Por *al-djabr* e *al-mukabala*, isto é, passando o termo —3 do primeiro membro para o segundo, o termo —3x do segundo para o primeiro e reduzindo os termos semelhantes, vem: $5x = 10$; multiplicando ambos os membros por 1/5, tem-se finalmente: $x = 2$, equação esta equivalente à proposta e cuja solução única é visivelmente 2.

Pode ainda, em vez duma só equação, ser proposto um *sistema de equações* com várias incógnitas x, y, \dots . O que se pretende então é determinar os agrupamentos de números que satisfazem *simultaneamente* a todas as equações dadas (*soluções do sistema*). Por exemplo, o sistema de equações

$$\begin{cases} 2x - 3y = 1 \\ x + 6y + 2 = 0 \end{cases}$$

admite uma solução única, constituída pelo par de números 0, —1/3, assim distribuídos: $x = 0, y = -1/3$.

A resolução dos sistemas de equações algébricas reduz-se em geral ao de equações algébricas com uma só incógnita, mediante processos de eliminação de incógnitas que constituem o objecto dum importante capítulo da álgebra (v. *eliminação*).

7. *Pôr um problema em equação; conceito de equação literal.* — O grande interesse das equações está em que traduzem problemas das mais variadas proveniências (vida quotidiana, ciências físico-naturais, engenharia, etc.) sob uma

forma que conduz automaticamente à sua resolução. *Pôr o problema em equação* é traduzi-lo em linguagem simbólica, na forma duma equação ou dum sistema de equações — o que requer, em geral, habilidade e poder intuitivo. Posto em equação, o problema está virtualmente resolvido, desde que a equação ou sistema entre num tipo clássico: o cálculo algébrico funciona então à maneira de máquina que se encarrega de fornecer as soluções. Haverá ainda uma terceira fase semelhante à primeira, mas geralmente mais simples, que consiste em interpretar e discutir as soluções, passando-as para a linguagem inicial. Seja, por exemplo, o problema:

«Determinar as idades de dois indivíduos F e G, sabendo que F é 5 anos mais velho do que G e que há 10 anos a idade de F era dupla da idade de G».

Designando por x a idade actual de F expressa em anos, a de G será $x-5$; há 10 anos as suas idades seriam, respectivamente, $x-10$ e $x-5-10 \equiv x-15$; portanto o problema ficará assim equacionado:

$$x - 10 = 2(x - 15) \quad \text{[idade de F há 10 anos} = 2 \times \text{idade de G há 10 anos]}$$

Aplicando a esta equação os métodos usuais, obtém-se a solução única $x=20$ (idade de F), sendo portanto 15 a idade de G (ambas expressas em anos).

Um outro conceito que importa esclarecer é o de *equação literal*. Dá-se este nome a equações em que, além da incógnita (ou das incógnitas), figuram uma ou mais letras, que se consideram designativas de *quantidades conhecidas* ou *dadas*. Por opposição, dizem-se *numéricas* as equações tais como inicialmente foram definidas. Seja, por exemplo, o seguinte problema, de que o anterior é um caso particular:

«Determinar as idades de dois indivíduos F e G, sabendo que F é d anos mais velho do que G e que há m anos a idade de F era k vezes a idade de G».

Designando ainda por x a idade actual de F, ter-se-á agora a equação

$$x - m = k(x - d - m).$$

Na realidade, trata-se aqui duma equação com quatro incógnitas: x, d, m, k . Porém, se quisermos que traduza o sentido do problema, devemos antes considerá-la como *equação variável*, que se concretiza em infinitas equações com uma só incógnita, x , ao substituir d, m, k por constantes. O que se pretende é obter uma fórmula que dê a solução de qualquer dessas infinitas equações, uma vez conhecidos os valores de d, m, k . Ora a fórmula procurada é:

$$x = \frac{m - k(m + d)}{1 - k}$$

restando ainda averiguar que valores se podem atribuir a d, m, k de modo que o problema seja possível, determinado, etc. (*discussão do problema*). Para $k \neq 1$, o segundo membro desta fórmula é uma expressão que, colocada no lugar de x , converte a equação literal numa identidade: exprime-se este facto dizendo que tal função de d, m, k é a *raiz*, ou *solução*, da equação considerada. Por conseguinte, *as raízes das equações literais são funções, e não números*. Tornaremos a este ponto mais adiante (v. *função*).

Entretanto, interessa observar que é costume (não obrigatório!) designar as incógnitas por letras finais do alfabeto, tais como x, y, z, \dots , e os dados (ou quantidades conhecidas) por letras iniciais, a, b, c, \dots . Esse hábito, que foi introduzido por Descartes, reflecte-se por sua vez no estudo das expressões algébricas, em que, segundo se lê ainda hoje nos textos didácticos, *as letras finais costumam ser usadas como variáveis, enquanto as letras iniciais se usam para designar constantes*. Porém, esta maneira de dizer (como já a anterior) é paradoxal:

Quando, por exemplo, se diz que um polinómio do 1.º grau em x é uma expressão do tipo $ax+b$, sendo a, b constantes ($a \neq 0$), há aqui um modo abreviado de dizer: *sendo as variáveis a, b substituídas por constantes numéricas* (tais como $-5, 2/3, \pi$, etc.). Considerada em si, a expressão $ax+b$ é um polinómio (do 2.º grau) nas variáveis a, b, x , podendo ainda ser interpretada como *polinómio em x de coeficientes variáveis* — mas não, decerto, como polinómio em x de coeficientes numéricos.

Todavia, para comodidade de linguagem, torna-se vantajoso empregar locuções abreviadas como aquela, que não provocam equívoco, desde que se faça um aviso prévio sobre o seu uso. De resto, as questões deste tipo só puderam ser inteiramente esclarecidas à luz da lógica moderna.

8. *O que distingue a álgebra da análise infinitesimal.* — Para completar o inventário do material sobre que incidem normalmente as considerações da álgebra clássica, resta-nos citar as *inequações algébricas* (fórmulas que se obtêm ligando duas expressões algébricas por um dos sinais $<$ ou $>$, com sentido apenas no campo real) e certos símbolos algorítmicos que nascem do estudo geral das expressões algébricas (símbolos do cálculo combinatório) e das equações algébricas (matrizes, determinantes, substituições, etc.). Quanto a métodos de cálculo e de raciocínio aplicáveis a esse material, *são próprios da álgebra unicamente aqueles métodos de carácter finitista que se firmam, em última análise, nas propriedades fundamentais da adição e da multiplicação.*

Desde que, tratando-se, por exemplo, de equações algébricas, se façam considerações que impliquem uma *infinidade* (potencial) de operações elementares, com subsequente passagem ao *limite*, deixa-se o campo da álgebra para se entrar no da análise infinitesimal.

Com efeito, o que caracteriza essencialmente a transição da álgebra para a análise infinitesimal (ou *análise transcendente*) é a intervenção do *conceito de limite*, aliado ao *conceito geral de função*, incluindo o de *sucessão infinita* (v. *função*).

Todavia, razões de ordem metodológica levam muitos autores a incluir em tratados de álgebra vários assuntos de carácter transcendente, tais como séries, produtos infinitos, fracções contínuas, funções trigonométricas, derivadas, etc.

De resto, a álgebra constitui, com a análise infinitesimal, uma unidade a que se aplica o nome de *análise*; por isso, também, a álgebra é algumas vezes chamada *análise algébrica* ou *análise finita*. Nesta ordem de ideias, a análise contém a álgebra, do mesmo modo que a álgebra contém a aritmética. Na base de todo o edifício está o conjunto dos números reais ou o conjunto dos números complexos, conforme se trata de *análise no campo real* ou de *análise no campo complexo*. Todavia, o estudo das equações algébricas virá indicar que o campo natural da álgebra é o dos números complexos.

9. *Equações algébricas de grau inferior ao 5.º; fórmula de Tartaglia; introdução dos números imaginários.* — É fácil ver que, pela aplicação dos princípios de equivalência, toda a equação algébrica inteira pode ser reduzida à forma dum polinómio igualado a zero (*forma canónica*); o grau desse polinómio dir-se-á o *grau da equação*. Portanto, a forma canónica duma equação de grau n em x será

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n = 0,$$

figurando nos lugares de a_0, a_1, \dots, a_n números quaisquer, com $a_0 \neq 0$ (*coeficientes da equação*), e sendo n um inteiro não negativo.

(Uma equação algébrica fraccionária ou mesmo irracional poderá ainda — no campo complexo — ser conduzida à forma inteira; mas esse é um ponto mais delicado).

Para $n=1$ ter-se-á a forma canónica das equações do 1.º grau:

$$a_0 x + a_1 = 0,$$

cujas soluções únicas é dada imediatamente pela fórmula $x = -a_1/a_0$.

Para $n=2$ tem-se a forma canónica das equações do 2.º grau:

$$a_0 x^2 + a_1 x + a_2 = 0,$$

cujas soluções (no máximo duas) são dadas pela fórmula:

$$x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0 a_2}}{2a_0}$$

[Transigimos com o uso escrevendo aqui o duplo sinal \pm (*mais* ou *menos*), que na realidade é supérfluo, porquanto o símbolo \sqrt{a} , sendo a um número $\neq 0$, tem sempre dois valores (simétricos), do mesmo modo que $\sqrt[3]{a}$ tem três, $\sqrt[4]{a}$ quatro, etc. (v. *número*)].

Para $x=3$ tem-se a forma canónica das equações do 3.º grau:

$$a_0 x^3 + a_1 x^2 + a_2 x + a_3 = 0,$$

e assim sucessivamente.

É preciso não perder de vista que os símbolos a_0, a_1, \dots são na realidade variáveis e que só substituindo-os por constantes numéricas se obtêm determinadas equações em x (numéricas); se não se fizer qualquer substituição, tem-se a *equação geral do 1.º grau*, a *equação geral do 2.º grau*, etc., cujos coeficientes são, em vez de números, as variáveis a_0, a_1, \dots (equações literais).

Para as equações do 3.º grau existe, como para as do 2.º, uma fórmula geral que fornece todas as raízes da equação (no máximo 3) mediante uma expressão algébrica que envolve os coeficientes a_0, a_1, a_2, a_3 ; a fórmula pode ser apresentada com o aspecto

$$(1) \quad x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \frac{a_1}{3a_0},$$

em que

$$p = \frac{a_2}{a_0} - \frac{a_1^2}{3a_0^2}, \quad q = \frac{a_3}{a_0} - \frac{a_1 a_2}{3a_0^2} + \frac{2a_1^3}{27a_0^3},$$

devendo as determinações das raízes cúbicas ser tomadas de modo que o seu produto seja igual a $-p/3$ (v. *número*).

No caso particular em que é $a_1=0$, vem $p=a_2/a_0$, $q=a_3/a_0$, e a equação cúbica reduz-se à forma

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

para a qual foi deduzida directamente a fórmula (1), em que se anula então o termo $-a_1/3a_0$.

A descoberta desta fórmula deve-se aos italianos Del Ferro e Tartaglia (século XVI). Trata-se dum acontecimento notabilíssimo na história da álgebra, ocorrido ainda no período da linguagem sincopada. É com a pesada indumentária da época que a referida fórmula aparece no tratado de Cardan *Ars Magna de rebus algebraicis* (1545), onde o autor apresenta uma resolução análoga da equação geral do 4.º grau, obtida pelo seu discípulo Ferrari, que consegue reduzir o problema ao da resolução da equação do 3.º grau mediante uma transformação algébrica simples.

(O tratado de Cardan apareceu pouco antes de Pedro Nunes publicar o *Libro de Algebra*; o nosso matemático apressou-se a actualizar a sua obra com um aditamento em que expõe e analisa a regra de Tartaglia).

Foi a fórmula (1) que obrigou a introduzir os números imaginários, sem os quais deixaria de ter sentido, precisamente no caso em que são reais todas as raízes da equação (*caso irreductível*). Acontece isto quando é negativo o valor da expressão

$$\frac{q^2}{4} + \frac{p^3}{27}$$

que figura sob o sinal da raiz quadrada; ora entre os números até então utilizados (números reais) não há nenhum que possa ser raiz quadrada dum número negativo, pois que o quadrado de qualquer deles é positivo ou nulo. Em face desta situação paradoxal, uma atitude seria a de rejeitar a fórmula e tentar a resolução por outra via; foi assim precisamente que procedeu Viète, indicando fórmulas trigonométricas (não algébricas, portanto) para o caso em questão.

Pelo contrário, Bombelli, professor em Bolonha depois de Tartaglia, adopta a attitude progressiva, decidindo-se a considerar as raízes de números negativos como números de nova espécie ⁽¹⁾, a que chama *quantidades silvestres* (hoje dizemos *imaginárias*) e que combina por adição com os números reais, obtendo expressões do tipo $a + b\sqrt{-1}$, onde os coeficientes a, b são números reais quaisquer. Bombelli ensina depois a operar sobre tais expressões (hoje denominadas *números complexos*), e, embora o novo cálculo só muito mais tarde venha a receber uma completa justificação, a verdade é que conduz a resultados exactos — impondo-se cada vez mais, ao longo dos séculos, pela sua comodidade (v. *número*).

Em particular, a fórmula (1) passa agora a ter sentido no caso irreductível, fornecendo efectivamente as soluções da equação; verifica-se então este facto notável: partindo de números *reais* (coeficientes da equação), obtêm-se resultados *reais* (as soluções), depois de se ter trabalhado com números *imaginários*. Esta circunstância há-de apresentar-se depois em numerosas questões de análise, algébrica e transcendente, observando-se muitas vezes que, «para ir dum ponto a outro do campo real, o caminho mais curto passa pelo campo imaginário».

O uso dos imaginários estava pois sancionado do ponto de vista pragmático.

10. *Resolubilidade algébrica; funções algébricas; números algébricos* ⁽²⁾. — A sensacional descoberta dos quinhentistas italianos instigou vivamente os estudiosos a procurarem fórmulas análogas para as equações de graus superiores ao 5.º e até, se possível, uma fórmula geral que compreendesse todos os graus. Durante cerca de três séculos se fizeram esforços para encontrar essa chave encantada do mundo algébrico; mas todos foram em vão. Finalmente, o grande matemático norueguês N. Henrik Abel (1802-1829), precedido em parte por Ruffini, consegue demonstrar rigorosamente que a equação geral do 5.º grau — e portanto a do 6.º, a do 7.º, etc. — não é resolúvel algébricamente, isto é, mediante uma expressão algébrica sobre os coeficientes.

Mas não quer isto dizer que não existam classes particulares de equações de grau > 4 resolúveis algébricamente. Como identificar, em geral, essas classes e atribuir-lhes o respectivo processo de resolução algébrica? E antes disso ainda: como pôr o problema em termos precisos?

A resposta é a *teoria da resolubilidade algébrica*, concebida por um jovem matemático francês, Evaristo Galois, cuja vida se fecha abruptamente aos 20 anos, num duelo, em 1832. A sua obra genial, condensada hoje em 60 páginas, só catorze anos depois da sua morte começou a ser revelada ao mundo científico, pelo matemático Liouville: essa obra inaugura uma nova era na história das matemáticas, pela originalidade e pela potência dos conceitos introduzidos.

Quando se aborda a teoria de Galois, convém ter presente a distinção entre *equações numéricas* e *equações literais*. As raízes duma equação numérica são sempre *números*; por exemplo, as soluções da equação numérica do 2.º grau $x^2 - 2x - 4 = 0$ são $1 + \sqrt{5}$ e $1 - \sqrt{5}$.

Mas suponhamos que nos lugares dos coeficientes duma equação de grau n em x figuram, em vez de números, expressões com uma ou mais variáveis u, v, \dots . Trata-se então, segundo o ponto de vista explanado no n.º 7, duma equação literal na incógnita x . Se $n < 5$, podemos sempre resolver algébricamente a equação em ordem à incógnita x , expressa como função de u, v, \dots . Por exemplo, a equação

$$x - 2ux + (3u^2 - v) = 0$$

é equivalente à equação

$$x = u \pm \sqrt{v - 2u^2},$$

que indica explicitamente as *duas soluções* da primeira em ordem a x (as funções $u + \sqrt{v - 2u^2}$ e $u - \sqrt{v - 2u^2}$), supondo que se escolhe sempre a raiz quadrada de menor argumento, entre 0 e 2π (v. *número*).

Mas, se o grau da equação em x é > 4 , a resolução algébrica já não é possível em geral e apresenta-se primeiro que tudo a seguinte dificuldade: o que se

⁽¹⁾ Antes de Bombelli já Cardan tinha apresentado algumas sugestões neste sentido.

⁽²⁾ Este número e o seguinte podem ser lidos, sem grande inconveniente, após o n.º 13.



EVARISTE GALOIS

(1811-1832)

Com a teoria da resolubilidade algébrica atinge-se um ponto culminante na história da álgebra. O genial criador desta teoria, E. Galois, não chega a atingir os 21 anos, morrendo num duelo, ignorado e desiludido. Galois inspirou-se em grande parte nas pesquisas feitas por Lagrange no sentido de encontrar um método geral (que não existe) para a resolução algébrica de equações de qualquer grau.



AMALIE EMMY NOETHER

(1882-1935)

Entre os principais construtores da álgebra moderna figura a matemática Emmy Noether, que foi primeiro professora em Göttingen e depois emigrou para os Estados Unidos. Era filha de Max Noether, um dos eminentes fundadores da geometria algébrica — à qual a moderna álgebra veio dar nova forma e novo impulso.

entende neste caso por *soluções* da equação? Não dispomos de dados para aprofundar aqui o assunto ⁽¹⁾. Entretanto diremos que as soluções duma equação algébrica literal são definidas, de certo modo, como *funções contínuas* — *ramos unívocos duma função plurívoca* — que, colocadas no lugar de x , convertem a equação numa identidade. Diz-se precisamente que uma função de u, v, \dots é *algébrica* quando é raiz de alguma equação algébrica cujos coeficientes sejam funções racionais de u, v, \dots ; caso contrário, a função diz-se *transcendente* (v. função). Portanto, do teorema de Abel resulta que *nem todas as funções algébricas podem ser representadas explicitamente por meio de expressões algébricas*. A recíproca, porém, é verdadeira: *toda a função representável por uma expressão algébrica é uma função algébrica*.

Posto isto, o conceito de *resolubilidade algébrica* pode ser precisado nos seguintes termos: diz-se que uma dada equação é *resolúvel algébricamente* (ou *resolúvel por meio de radicais*), a respeito dos seus coeficientes, quando todas as raízes da equação podem ser obtidas, efectuando só operações racionais ⁽²⁾ e extracções de raiz, um número finito de vezes, a partir dos coeficientes (quer estes sejam números quer funções). A definição pode ser dada ainda com maior generalidade — como fez Galois — considerando, em vez dos coeficientes, um conjunto qualquer de números (ou funções) que englobe os coeficientes.

⁽¹⁾ A questão é na realidade muito delicada e só pode ser inteiramente esclarecida por dois meios: ou pela *teoria das funções analíticas*, que transcende o campo da álgebra (v. função), ou pelos métodos da *álgebra moderna* (esses puramente algébricos).

⁽²⁾ Já atrás se disse que é dado o nome de *operações racionais* às seguintes operações: *adição, subtracção, multiplicação e divisão*.

Por exemplo, prova-se com a teoria de Galois que a equação $x^5 - 4x + 2 = 0$ não é resolúvel algèbricamente a respeito dos coeficientes; quer isto dizer que as suas raízes (que são cinco números, três reais e dois imaginários) não podem exprimir-se por meio dos sinais $+$, $-$, \times , $:$, $\sqrt{}$, $\sqrt[3]{}$, ..., $\sqrt[n]{}$, ..., a partir dos coeficientes. Mas já a equação do 6.º grau em x

$$x^6 + (1 - t^2)x^4 - t = 0$$

é resolúvel algèbricamente; com efeito, a sua resolução pode reduzir-se à da equação do 3.º grau em y

$$y^3 + (1 - t^2)y^2 - t = 0,$$

com a qual está relacionada por meio da fórmula $x = t \pm \sqrt[3]{y}$.

Chama-se *número algébrico* todo o número que é raiz de alguma equação algébrica de coeficientes racionais; os números não algébricos dizem-se *transcendentes*. Por exemplo, são números algébricos as raízes da equação $x^5 - 4x + 2 = 0$, os valores de $\sqrt[5]{2 - \sqrt[3]{7}}$, etc. Em 1873 Hermite demonstrou a transcendência do número e ; nove anos depois, seguindo a mesma pista, Lindeman demonstrou a transcendência de π . Este último facto implica em particular a impossibilidade de resolver o clássico problema da quadratura do círculo por meio da régua e do compasso (v. *geometria*).

11. *Primeira noção de corpo*. — Um conceito que joga essencialmente na teoria de Galois é o de *corpo* (ou *domínio de racionalidade*). Diz-se que um dado conjunto Ω constituído por vários números é um *corpo*, quando é fechado a respeito das operações racionais, isto é, quando, dados dois números a, b de Ω , se verifica sempre que também a soma $a + b$, o produto ab , a diferença $a - b$ e o quociente a/b (sendo $b \neq 0$) pertencem a Ω . Assim, o conjunto dos números racionais, o conjunto dos números reais, o conjunto dos números complexos, são exemplos de corpos; mas já o conjunto de números inteiros não é um corpo, pois que o quociente de dois números inteiros pode não ser um número inteiro. Análogamente se define *corpo de funções*; por exemplo, o conjunto de todas as funções racionais duma variável x é um corpo de funções.

Diz-se que um número a é *racionalmente conhecido* a respeito dum dado conjunto M de números, quando se pode obter a partir de elementos de M , mediante operações racionais, efectuadas um número finito de vezes. A totalidade dos números que são racionalmente conhecidos a respeito de M constitui um corpo, que se chama o *corpo gerado por M* (definição análoga para conjuntos de funções).

Exemplos: 1) o corpo gerado pelo número 1 é o corpo racional; 2) o corpo gerado por um dos números $\sqrt{2}$ é o conjunto dos números da forma $a + b\sqrt{2}$, sendo a, b números racionais; 3) o corpo gerado pela adjunção de i ($=\sqrt{-1}$) ao corpo real é o corpo complexo, cujos elementos são da forma $a + bi$, com a, b reais; 4) o corpo gerado pela adjunção da variável x ao corpo racional é o conjunto das funções racionais de x , com coeficientes racionais, etc.

12. *Teorema fundamental da álgebra; resolução numérica das equações*. — Costuma dar-se imprópriamente o nome de *teorema fundamental da álgebra* (ou *teorema de D'Alembert*) a uma proposição cuja primeira demonstração rigorosa se deve a Gauss e que afirma o seguinte: «toda a equação algébrica de grau superior a zero, com coeficientes numéricos (isto é, situados no corpo complexo), é resolúvel»; com isto se pretende dizer, naturalmente, que existe, pelo menos, um número (real ou imaginário) que verifica a equação. Todavia este teorema não pode ser demonstrado com raciocínios puramente algébricos, e por isso, em rigor, transcende o campo da álgebra.

Uma vez provado que, em tais condições, toda a equação algébrica é resolúvel, surge logo a seguinte questão, que tende a concretizar o significado daquele teorema:

Como determinar efectivamente a solução ou as soluções duma dada equação algébrica (numérica)?

Já se viu que, sendo o grau 5, a *resolução algébrica* é geralmente impossível. Do ponto de vista prático, o problema situa-se no campo da análise infinitesimal. Com efeito, o cálculo das raízes duma equação numérica (ou, como também se diz, a *resolução numérica da equação*) é geralmente efectuado por meio de certos *métodos de aproximações sucessivas*, que fazem intervir necessariamente o conceito de limite. Permitem esses métodos obter, para cada raiz da equação, valores numéricos tão próximos da raiz quanto se quiser. E é isso afinal o que interessa nas aplicações. Acontece por vezes a um engenheiro ter de conhecer alguma ou mesmo todas as raízes duma dada equação algébrica; mas é claro que lhe basta conhecer essas raízes com um certo grau de aproximação (por exemplo, com erro inferior a 0,01), visto que já os coeficientes da equação provêm de medições que dão sempre valores aproximados das grandezas medidas (comprimento dum fio, resistência dum condutor eléctrico, intensidade duma corrente, etc.); nem sequer faria sentido falar do *valor exacto* de tais grandezas.

Também não seria justo dizer que os referidos métodos não fornecem as *soluções exactas* da equação; a verdade é que permitem definir cada raiz como *limite* duma sucessão, da qual se sabe calcular *tantos termos quantos se quiser*.

Por outro lado, convém notar que, na prática, as raízes reais duma equação algébrica são quase sempre números irracionais, isto é, números representáveis por meio de dízimas infinitas não periódicas (o mesmo sucedendo a respeito dos coeficientes reais das raízes complexas); portanto, qualquer que seja o método utilizado — algébrico ou não algébrico —, quando se trata de conhecer os valores numéricos das raízes, é aos métodos de aproximações sucessivas que se tem de recorrer inevitavelmente. De resto, já assim sucede com o cálculo das raízes quadradas, cúbicas, etc.; quando, por exemplo, um número inteiro não é quadrado perfeito (o que geralmente sucede), a sua raiz quadrada é seguramente irracional e só pode ser calculada por aproximações sucessivas.

Assim, o conceito prático de aproximação é inseparável do conceito teórico de número irracional; ambos intervêm na mentalidade do analista, que se opõe, por vezes fortemente, à mentalidade do algebrista.

Resta-nos dizer que pelos métodos da álgebra moderna é possível construir uma teoria puramente algébrica das equações — sem recorrer, portanto, ao teorema fundamental. Todas as raízes de cada equação dada são introduzidas de maneira semelhante à dos números imaginários, isto é, como símbolos sobre os quais se opera segundo certas regras.

13. *Fórmulas de Viète-Girard; funções simétricas das raízes.* — Consideremos uma equação algébrica de grau n (>1) com coeficientes numéricos; será pois uma equação do tipo

$$(2) \quad a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n = 0,$$

em que, nos lugares de a_0, a_1, \dots , figuram constantes numéricas ($a_0 \neq 0$). Demonstra-se, a partir do teorema fundamental da álgebra, que o primeiro membro desta equação é equivalente a um produto da forma

$$(3) \quad a_0 (x - x_1)(x - x_2) \dots (x - x_n),$$

em que, nos lugares de x_1, x_2, \dots, x_n , estão representadas *todas* as raízes da equação. Pode, porém, acontecer que alguma raiz apareça repetida; chama-se *ordem de multiplicidade* duma raiz o número μ de vezes que ela figura na decomposição (3). Conforme $\mu = 2, 3, \dots$, assim a raiz se diz *dúpla, tripla*, etc.; se $\mu = 1$, a raiz diz-se *simples*. Por exemplo, a equação do 3.º grau em x

$$x^3 - 3x - 2 = 0$$

admite uma raiz simples (o número 2) e uma dúpla (o número -1), pois que se tem, como é fácil verificar,

$$x^3 - 3x - 2 \equiv (x - 2)(x + 1)(x + 1) \equiv (x - 2)(x + 1)^2.$$

Contando cada raiz múltipla de ordem μ por μ raízes simples, pode dizer-se que *toda a equação algébrica de grau n tem precisamente n raízes*. Mas trata-se

apenas de uma convenção de linguagem, que se revela cómoda para fins de exposição. É evidente que, se houver raízes múltiplas, o número das raízes não é na realidade n , mas sim inferior a n .

Da comparação de (2) com (3) deduzem-se relações simples entre as raízes e os coeficientes da equação, traduzidas pelas importantes fórmulas de Viète-Girard. No caso da equação do 2.º grau ($n=2$), essas fórmulas são

$$x_1 + x_2 = -\frac{a_1}{a_0}, \quad x_1 x_2 = \frac{a_2}{a_0};$$

no caso da equação do 3.º grau ($n=3$), tem-se

$$x_1 + x_2 + x_3 = -\frac{a_1}{a_0}, \quad x_1 x_2 + x_1 x_3 + x_2 x_3 = \frac{a_2}{a_0}, \quad x_1 x_2 x_3 = -\frac{a_3}{a_0};$$

e assim por diante. Em palavras: a soma das raízes é igual ao coeficiente do 2.º termo dividido pelo coeficiente do 1.º, com sinal trocado; a soma dos produtos das raízes tomadas duas a duas é igual ao coeficiente do 3.º termo dividido pelo coeficiente do 1.º; a soma dos produtos das raízes três a três é igual ao coeficiente do 4.º termo dividido pelo coeficiente do 1.º, com sinal trocado, etc.; finalmente, o produto das raízes é igual ao termo independente dividido pelo coeficiente do 1.º, multiplicado por $+1$ ou -1 , conforme n é par ou ímpar.

Limitemo-nos agora, para fixar ideias, ao caso da equação do 4.º grau e consideremos, por exemplo, a soma das raízes três a três, ou seja,

$$x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4;$$

se nesta expressão permutarmos entre si os símbolos x_1, x_2, x_3, x_4 , de qualquer modo que seja, obtém-se ainda, como é fácil ver, uma expressão equivalente à primeira — e portanto a *mesma função* das raízes. Exprime-se este facto dizendo que se trata duma *função simétrica*.

Portanto, *função simétrica* dos símbolos x_1, x_2, \dots, x_n (considerados como variáveis) é toda a função de x_1, x_2, \dots, x_n que se mantém inalterada quando se permutam entre si as suas variáveis de todos os modos possíveis. Por exemplo, a função $x_1 x_2 + x_3 x_4$ não é simétrica, porque se trocarmos x_2 com x_3 obteremos a função $x_1 x_3 + x_2 x_4$, distinta da primeira.

Pois bem, demonstra-se que, se x_1, x_2, \dots, x_n designam as raízes duma dada equação algébrica, toda a função racional simétrica de x_1, x_2, \dots, x_n , com coeficientes racionais, tem um valor que se pode calcular a partir dos coeficientes da equação, mediante uma função racional, com coeficientes ainda racionais (teorema das funções simétricas).

Assim, por exemplo, na equação do 3.º grau, a soma dos quadrados das raízes é uma função simétrica de x_1, x_2, x_3 , que pode ser calculada do seguinte modo, a partir dos coeficientes a_0, a_1, a_2, a_3 :

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= (x_1 + x_2 + x_3)^2 - 2(x_1 x_2 + x_1 x_3 + x_2 x_3) = \\ &= \left(-\frac{a_1}{a_0}\right)^2 - 2\frac{a_2}{a_0} = \frac{a_1^2 - 2a_0 a_2}{a_0^2} \end{aligned}$$

Deste teorema deduz-se em particular que «toda a função racional simétrica das raízes (de coeficientes racionais) é *racionalmente conhecida*, quer dizer, o seu valor pertence ao corpo gerado pelos coeficientes da equação».

14. *Substituições e grupos de substituições; grupo de Galois duma equação.* — Retomemos o exemplo da função

$$x_1 x_2 + x_3 x_4,$$

há pouco considerada. Suponhamos que nos lugares de x_1, x_2, x_3, x_4 colocamos, respectivamente, $x_4 x_3 x_2 x_1$; diz então que sobre aqueles elementos se efectuou uma *substituição* (ou *permutação*), que pode ser indicada pelo símbolo

$$\begin{pmatrix} x_4 & x_3 & x_2 & x_1 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix},$$

em que, por cima de cada elemento indicado na linha inferior, figura aquele que o vai substituir. Designemos esta substituição por τ ; efectuando em $x_1 x_2 + x_3 x_4$ a substituição σ , obtém-se a função $x_4 x_3 + x_2 x_1$, idêntica à primeira — o que se exprime dizendo que tal função é *invariante* para σ . Análogamente se reconhece que a mesma função é ainda invariante para a substituição

$$\theta = \begin{pmatrix} x_2 & x_1 & x_3 & x_4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix},$$

mas não, por exemplo, para a substituição

$$\rho = \begin{pmatrix} x_1 & x_3 & x_2 & x_4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix}.$$

Dum modo geral, diz-se que se efectua uma *substituição sobre n elementos* x_1, x_2, \dots, x_n , quando nos lugares destes se colocam os mesmos elementos numa ordem geralmente diversa, sem omissão nem repetição. O número total de substituições possíveis sobre n elementos será então igual a $n! = 1 \times 2 \times 3 \times \dots \times n$. Por exemplo, as substituições possíveis sobre três elementos x_1, x_2, x_3 são:

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix}, \begin{pmatrix} x_2 & x_3 & x_1 \\ x_1 & x_2 & x_3 \end{pmatrix}, \begin{pmatrix} x_3 & x_1 & x_2 \\ x_1 & x_2 & x_3 \end{pmatrix}, \begin{pmatrix} x_2 & x_1 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix}, \begin{pmatrix} x_1 & x_3 & x_2 \\ x_1 & x_2 & x_3 \end{pmatrix} \text{ e } \begin{pmatrix} x_3 & x_2 & x_1 \\ x_1 & x_2 & x_3 \end{pmatrix}.$$

A primeira destas substituições deixa inalterados todos os elementos sobre que incide; dá-se-lhe o nome de *substituição idêntica* ou *identidade* e representa-se por I.

Dadas duas substituições S, T, sobre os mesmos elementos, chama-se *produto* destas substituições na ordem por que estão escritas, e representa-se por ST, a substituição que resulta de efectuar *primeiro* T e *depois* S. No exemplo das substituições σ, θ , atrás consideradas, ter-se-á:

$$\sigma \theta = \begin{pmatrix} x_4 & x_3 & x_2 & x_1 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix} \cdot \begin{pmatrix} x_2 & x_1 & x_3 & x_4 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix} = \begin{pmatrix} x_3 & x_4 & x_2 & x_1 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix};$$

com efeito: θ substitui x_1 por x_2 , σ substitui x_2 por x_3 , logo $\sigma\theta$ substitui x_1 por x_3 , etc. Análogamente, será

$$\theta \sigma = \begin{pmatrix} x_4 & x_3 & x_1 & x_2 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix} \neq \sigma \theta,$$

o que mostra desde já que o *produto de substituições não obedece à lei comutativa*. Pode porém acontecer em particular que, dadas duas substituições S, T, se tenha $ST = TS$; diz-se então que S e T são *permutáveis*.

A escolha do termo *produto* para designar o resultado da operação assim definida entre substituições tem carácter convencional e subordina-se a razões de comodidade; poderiam usar-se para o mesmo efeito outros termos, tais como *resultante*, *composição* ou mesmo *soma*, mas o primeiro é realmente preferível. Esta *multiplicação* obedece a várias regras de cálculo semelhantes às que regem a multiplicação ordinária entre números. Assim:

- a) Trata-se duma operação uniforme e associativa.
- b) Existe uma substituição (a *identidade*, I) tal que

$$SI = IS, \text{ qualquer que seja a substituição S.}$$

c) Para toda a substituição S existe uma outra — chamada *substituição inversa* de S e representável por S^{-1} — tal que

$$SS^{-1} = S^{-1}S = I.$$

Está-se a ver que a substituição inversa S^{-1} é aquela que produz efeito inverso ao de S ; isto é, se S substitui x_i por x_k , S^{-1} substitui x_k por x_i , de modo que, efectuando S^{-1} a seguir a S sobre x_i , obtém-se de novo x_i , qualquer que seja $i = 1, 2, \dots, n$, o que significa que tudo é reposto nos lugares primitivos. Por exemplo, tem-se

$$\begin{pmatrix} x_2 & x_3 & x_1 \\ x_1 & x_2 & x_3 \end{pmatrix}^{-1} = \begin{pmatrix} x_3 & x_1 & x_2 \\ x_1 & x_2 & x_3 \end{pmatrix}.$$

Daqui resulta ainda que, dadas duas substituições S, T sobre os mesmos elementos, existe sempre uma (e uma só) substituição X tal que

$$XS = T,$$

que é a substituição $X = TS^{-1}$, chamada *quociente à direita de T por S* . Análogamente, existirá uma (e uma só) substituição Y tal que $SY = T$, que é a substituição $Y = S^{-1}T$, chamada *quociente à esquerda de T por S* . Em geral é $TS^{-1} \neq S^{-1}T$.

Assim, a multiplicação entre substituições admite duas operações inversas — a *divisão à direita* e a *divisão à esquerda* —, que não coincidem pelo facto de a multiplicação não ser comutativa.

Tornemos ao exemplo da função $x_1x_2 + x_3x_4$. Vimos que as substituições σ, θ deixam inalterada esta função; é evidente *a priori* que o mesmo acontecerá com os produtos $\sigma\theta$ e $\theta\sigma$.

Dum modo geral, dada uma classe C de substituições sobre n elementos: x_1, x_2, \dots, x_n , diz-se que C é um *grupo* quando verifica a seguinte condição: o produto de duas substituições (distintas ou idênticas) pertencentes a C é sempre uma substituição pertencente a C . Assim, a totalidade das substituições que deixam inalterada uma dada função de x_1, x_2, \dots, x_n é um grupo (chamado *grupo dessa função*); em particular, se a função é simétrica, o seu grupo é constituído por todas as possíveis substituições sobre x_1, x_2, \dots, x_n (*grupo simétrico de grau n*). *Ordem do grupo* é o número das suas substituições. Por exemplo, as substituições:

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix}, \begin{pmatrix} x_2 & x_3 & x_1 \\ x_1 & x_2 & x_3 \end{pmatrix}, \begin{pmatrix} x_3 & x_1 & x_2 \\ x_1 & x_2 & x_3 \end{pmatrix}$$

formam um grupo de ordem 3, que não é visivelmente o grupo simétrico e a que pertence entre outras a função $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$.

Já vimos que as funções simétricas racionais (com coeficientes racionais) das raízes duma equação algébrica são racionalmente conhecidas a respeito dos coeficientes da equação. Pois bem, demonstra-se ainda o seguinte: *quando se conhece, além dos coeficientes da equação, o valor duma dada função racional assimétrica das raízes, tornam-se racionalmente conhecidas todas as outras funções racionais das raízes (com coeficientes racionais), que são invariantes para as substituições do grupo da primeira* (teorema de Lagrange). E pressente-se que o conhecimento desse valor constitui um progresso a caminho da resolução da equação.

São considerações deste tipo (devidas sobretudo a Vandermonde, Lagrange e Ruffini) que precedem historicamente a teoria de Galois, em que o conceito de grupo desempenha, a par do conceito de corpo, um papel fundamental.

Consideremos uma equação algébrica de coeficientes situados num dado corpo Ω (de números ou de funções). Chama-se *grupo de Galois* dessa equação a respeito de Ω um grupo G de substituições sobre as raízes da mesma, que verifica a seguinte condição: todas as funções racionais das raízes, com coeficientes racionais, que se mantêm invariantes para as substituições de G (e só essas), têm o seu valor situado em Ω . É a estrutura particular deste grupo que decide se a equação é ou não resolúvel algebricamente a respeito de Ω ; no caso

Tornemos ao caso geral e suponhamos que, depois de efectuada sobre as variáveis x_1, x_2, \dots, x_n a transformação (α) , se efectua sobre as novas variáveis u_1, u_2, \dots, u_m uma segunda transformação linear

$$(\beta) \quad \begin{cases} u_1 = b_{11} t_1 + b_{12} t_2 + \dots + b_{1p} t_p \\ u_2 = b_{21} t_1 + b_{22} t_2 + \dots + b_{2p} t_p \\ \vdots \\ u_m = b_{m1} t_1 + b_{m2} t_2 + \dots + b_{mp} t_p \end{cases}$$

ou, abreviadamente,

$$u_k = \sum_{j=1}^p b_{kj} t_j, \quad k = 1, 2, \dots, m,$$

cuja matriz

$$\mathbf{B} = [b_{ij}]$$

é do tipo $m \times p$, isto é, formada de m linhas e p colunas.

Ora, efectuar sucessivamente as transformações (α) e (β) equivale a efectuar directamente uma transformação única que se obtém substituindo u_1, u_2, \dots, u_m nas fórmulas (α) pelas respectivas expressões em t_1, t_2, \dots, t_p dadas pelas fórmulas (β) . Pois bem, prova-se facilmente que a transformação assim obtida ainda é uma transformação linear:

$$(\gamma) \quad x_i = \sum_{j=1}^p c_{ij} t_j, \quad i = 1, 2, \dots, n,$$

determinada por uma matriz

$$\mathbf{C} = [c_{ij}]$$

do tipo $n \times p$, cujo elemento genérico c_{ji} é dado pela fórmula

$$c_{ij} = \sum_{k=1}^m a_{ik} b_{kj} = a_{i1} b_{1j} + a_{i2} b_{2j} + \dots + a_{im} b_{mj};$$

isto é: o elemento c_{ij} situado na linha i e na coluna j de C obtém-se multiplicando ordenadamente os elementos da linha i de A pelos elementos correspondentes da coluna j de B e somando os resultados obtidos ($i = 1, 2, \dots, n$; $j = 1, 2, \dots, p$). Posto isto, diz-se que a transformação (γ) é o *produto* de (α) por (β); e, ainda, que a matriz C é o *produto* de A por B , escrevendo-se

$$C = A \cdot B \quad \text{ou} \quad C = A B.$$

Por exemplo, se, a seguir à transformação (σ_1) atrás considerada $(x = 3u - v, y = u + 2v)$, efectuarmos esta segunda transformação:

$$(\sigma_2) \quad \begin{cases} u = \xi - 2\eta \\ v = 2\xi + \eta - \zeta, \end{cases}$$

obtem-se a transformação produto de (σ_1) por (σ_2) :

$$(σ_3) \quad \begin{cases} x = \xi - 7\eta + \zeta \\ y = 5\xi - 2\zeta. \end{cases}$$

cuja matriz podia ser calculada directamente por meio da regra anterior:

$$\begin{bmatrix} 3 & -1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} 1 & -2 & 0 \\ 2 & 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 & -7 & 1 \\ 5 & 0 & -2 \end{bmatrix}.$$

(Assim, para calcular o elemento da 2.^a linha e 3.^a coluna, multiplica-se ordenadamente a 2.^a linha da primeira matriz pela 3.^a coluna da segunda matriz, o que dá: $1 \times 0 + 2 \times (-1) = -2$, etc.).

Note-se desde já que o *produto assim definido entre matrizes é associativo mas não comutativo*. Exemplo:

$$\begin{bmatrix} 3 & -1 \\ 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ -1 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -2 & 6 \end{bmatrix} \neq \begin{bmatrix} 0 & 2 \\ -3 & 7 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 3 & -1 \\ 0 & 2 \end{bmatrix}$$

Duas matrizes A, B dizem-se *permutáveis* quando se tem $AB = BA$.

Entre as matrizes quadradas de ordem n tem especial interesse a matriz cujos elementos são todos nulos, excepto aqueles situados na *primeira diagonal* (formada pelos elementos com iguais índices de linha e de coluna). A essa matriz dá-se o nome de *matriz unidade* e representa-se por I. Ter-se-á pois

$$I = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} \quad (n \text{ linhas e } n \text{ colunas}).$$

A designação *matriz unidade* provém do seguinte facto, que é fácil verificar:

$$IA = AI, \text{ qualquer que seja } A \text{ (matriz quadrada de ordem } n).$$

Tornemos ao caso geral da transformação (α) atrás considerada; supondo $m = n$, diz-se que esta transformação é *reversível* quando, substituindo as variáveis x_1, x_2, \dots, x_n por constantes quaisquer, se obtém sempre um sistema de equações lineares em u_1, u_2, \dots, u_n , que admite uma, e uma só, solução. Nesta hipótese será possível resolver o sistema (α) em ordem às variáveis u_1, u_2, \dots, u_n como funções de x_1, x_2, \dots, x_n , obtendo-se uma nova transformação linear

$$(z') \quad v_i = a'_{i1} x_1 + a'_{i2} x_2 + \dots + a'_{in} x_n \quad (i = 1, 2, \dots, n),$$

que se diz *inversa* de (α) . «Condição necessária e suficiente para que a transformação (α) seja reversível (supondo sempre $m = n$) é que seja diferente de zero o determinante da sua matriz A». (V. *determinante* e *eliminação*). Verificada esta hipótese, a matriz A também se diz *reversível* e a matriz da transformação (α') inversa de (α) diz-se *matriz inversa* de A, representando-se por A^{-1} . Além disso, tem-se, como é fácil ver,

$$A^{-1}A = AA^{-1} = I,$$

propriedade esta que também pode ser utilizada directamente para definir *matriz reversível* e *matriz inversa*. Assim, o estudo das matrizes implica, em particular, o estudo dos sistemas de equações lineares (isto é, do 1.^o grau).

Por exemplo, a transformação

$$\begin{cases} x = 3u - v \\ y = 5u - 2v \end{cases}, \text{ de matriz } \begin{bmatrix} 3 & -1 \\ 5 & -2 \end{bmatrix},$$

é reversível, sendo a sua inversa a transformação

$$\begin{cases} u = 2x - y \\ v = 5x - 3y \end{cases}, \text{ de matriz } \begin{bmatrix} 2 & -1 \\ 5 & -3 \end{bmatrix};$$

tem-se, com efeito:

$$\begin{bmatrix} 3 & -1 \\ 5 & -2 \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 \\ 5 & -3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Entre as matrizes dum mesmo tipo também se define de maneira natural uma adição. Dadas duas de tais matrizes A, B, chama-se *soma* de A com B e representa-se por $A + B$ a matriz em que cada elemento é a soma dos elementos homólogos de A e de B. Por exemplo:

$$\begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix} + \begin{bmatrix} 0 & 3 \\ -2 & 1 \end{bmatrix} = \begin{bmatrix} 2+0 & -1+3 \\ 1-2 & 3+1 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ -1 & 4 \end{bmatrix}.$$

A adição assim definida entre matrizes é manifestamente *associativa* e *comutativa*. Além disso, dadas duas matrizes A, B, existe sempre uma terceira X (e só uma) tal que

$$A + X = B;$$

é claro que cada elemento de X é a diferença entre o elemento homólogo de B e o elemento homólogo de A; diz-se então que X é a diferença entre B e A e escreve-se $X = B - A$.

Finalmente, demonstra-se que, entre matrizes quadradas da mesma ordem, a multiplicação é *distributiva* a respeito da adição (*à direita* e *à esquerda*); isto é, tem-se

$$A(B + C) = AB + AC, \quad (B + C)A = BA + CA,$$

sendo A, B, C matrizes quadradas da mesma ordem.

É ainda costume definir uma terceira operação — a *multiplicação de números por matrizes* — em que um dos dados é um número e o outro uma matriz. Chama-se *produto dum dado número k por uma dada matriz A*, e representa-se por kA , a matriz cujos elementos são os produtos dos elementos homólogos de A por k. Exemplo:

$$(-3) \cdot \begin{bmatrix} -2 & 0 & 3 \\ 5 & \frac{1}{2} & \sqrt{3} \end{bmatrix} = \begin{bmatrix} 6 & 0 & -9 \\ -15 & -\frac{3}{2} & -3\sqrt{3} \end{bmatrix}.$$

Mas tornemos agora atrás. O conceito de transformação linear foi introduzido começando por considerar uma função qualquer

$$\Phi(x_1, x_2, \dots, x_n)$$

e falando em substituir as variáveis x_1, x_2, \dots, x_n por novas variáveis u_1, u_2, \dots, u_m , segundo a transformação linear

$$(\alpha) \quad x_i = a_{i1}u_1 + a_{i2}u_2 + \dots + a_{im}u_m \quad (i = 1, 2, \dots, n).$$

É claro que, feita a referida mudança de variáveis, se obtém uma nova função

$$\Psi(u_1, u_2, \dots, u_m) \equiv \Phi\left(\sum_{k=1}^m a_{1k}u_k, \sum_{k=1}^m a_{2k}u_k, \dots, \sum_{k=1}^m a_{nk}u_k\right),$$

a qual se diz *transformada* da primeira por meio de (α) . Tem particular interesse o caso em que a função $\Phi(x_1, x_2, \dots, x_n)$ é expressa por um polinómio em x_1, x_2, \dots, x_n ; neste caso a expressão resultante será ainda um polinómio nas variáveis u_1, u_2, \dots, u_m de grau *não superior* ao do primeiro; o grau do novo polinómio será igual ao do primeiro se a transformação (α) for reversível (supondo $m = n$). Há pois certas propriedades de cada polinómio que se mantêm *invariantes* para certas transformações lineares.

Mais particularmente ainda interessa o caso dos polinómios *homogêneos*, isto é, dos polinómios cujos termos têm todos o mesmo grau (v. *formas algébricas*).

16. Importância e evolução dos estudos de álgebra linear. — A álgebra linear tem por objecto não só o estudo das transformações lineares e matrizes ⁽¹⁾, mas

⁽¹⁾ Primitivamente, a álgebra linear consiste no estudo dos sistemas de equações do 1.º grau (também chamadas lineares), donde o adjectivo *linear* aplicado a este ramo da álgebra. De resto, o conceito de equação linear evolui e alarga-se no âmbito da moderna análise funcional.

ainda o comportamento das expressões algébricas perante tais transformações (incluindo os respectivos *invariantes*). Estas doutrinas encontram numerosas aplicações em vários campos da matemática, pura e aplicada: primeiramente, em geometria analítica e projectiva (transformações geométricas, teoria das cônicas e das quadricas, etc.), depois em álgebra superior (transformações de equações), em aritmética superior (representação dos números inteiros complexos), em análise (teoria dos máximos e dos mínimos, etc.) e, finalmente, em geometria superior (sobretudo em geometrias de Riemann). Estas últimas aplicações têm um especial significado, atendendo ao uso que se faz das geometrias de Riemann na física moderna; aqui a álgebra linear intervém sob a forma bem mais elaborada da *álgebra tensorial*, que é a parte algébrica do *cálculo tensorial* (ou *absoluto*), criado pelos italianos Ricci e Levi-Civita e que, nas mãos de Einstein, se revelou um instrumento formal indispensável para o tratamento da teoria da relatividade (v. *tensor*).

Por sua vez, o cálculo matricial constitui uma técnica operatória que transcede nitidamente os quadros da aritmética tradicional e cujo emprego está a difundir-se cada vez mais pela sua comodidade e pelo seu poder sugestivo. Os engenheiros, os técnicos estatísticos, etc., fazem hoje uso corrente do cálculo de matrizes.

A álgebra linear é essencialmente uma criação dos ingleses Cayley e Sylvester, do francês Hermite e do alemão Kronecker (século XIX).

Mais modernamente, a álgebra linear tornou-se um dos aspectos — precisamente o aspecto finito — da *análise funcional linear*, que tem numerosas aplicações, especialmente no campo da física atómica.

Os estudos de álgebra linear desenvolvem-se hoje segundo a orientação axiomática, no âmbito vastíssimo dos espaços vectoriais abstractos e das álgebras ou sistemas hipercomplexos (v. *estruturas algébricas* e *vector*).

III. Álgebra moderna. — Actualmente os estudos de álgebra subordinam-se, na maior parte, à *orientação abstracta, formal* ou *axiomática*, que é um dos traços dominantes das matemáticas modernas (v. *axiomática*).

Não quer isto dizer que as matemáticas tradicionais, e em particular a álgebra, não tivessem já carácter abstracto. Os números e as figuras geométricas são, já de si, entes abstractos por excelência. E o conceito de variável é a expressão genuína do abstractismo matemático, que estende para além de todos os limites a faculdade humana de «dar o mesmo nome a coisas diferentes» — diferentes pela *substância*, que não pela *forma*. Mas trata-se agora de um nível superior de abstracção, de um plano mais elevado de racionalização.

A álgebra clássica tinha já mostrado que, na sua essência, os raciocínios algébricos abstraem da natureza intrínseca dos elementos sobre os quais inicialmente se opera — os números —, para visarem exclusivamente as operações que os relacionam e, acima de tudo, as *propriedades formais dessas operações*. Mas, presentemente, o formalismo — aquela faculdade de dar o mesmo nome a coisas idênticas só na forma — é exercido em escala muito mais ampla: *agora são os domínios operatórios e as próprias operações que se tornam variáveis*.

Na breve exposição precedente sobre álgebra clássica deixámos esboçada a génese deste processo de generalização. Viu-se ali como os conceitos de adição, multiplicação, etc., primeiro definidos entre números, se transferem depois naturalmente para o campo das expressões algébricas; chamámos em particular a atenção para a analogia flagrante entre o cálculo dos polinómios e o cálculo dos números inteiros, entre o cálculo das funções racionais e o cálculo dos números racionais. Durante séculos os domínios operatórios ficarão assim normalmente constituídos: ou por números ou por funções numéricas. Em particular, as equações algébricas, cuja teoria é o objecto central de toda a álgebra clássica — sua remota origem e seu último fim —, têm invariavelmente os coeficientes situados num corpo de números (equações numéricas) ou num corpo de funções (equações literais). Paralelamente, o problema central da aritmética (ou *teoria dos números*) fica sendo o estudo das equações de Diofanto, de preferência sob a forma da teoria das congruências, que, no caso do módulo primo, apresenta analogias profundas, surpreendentes, com a teoria das equações algébricas, à qual, de resto, aparece intimamente associada com os métodos geniais de Gauss e de Galois (v. *congruência*).

Mas, assim como tinha obrigado a um alargamento do conceito de número com a introdução dos números irracionais, dos números negativos e dos números imaginários, é o próprio estudo das equações algébricas que irá provocar a rotura dos quadros, levando a criar uma espécie de *cálculo* sobre entidades que não são números nem funções numéricas — as *substituições*. Com efeito, entre estas novas entidades é definida uma *operação* que apresenta certas *analogias formais* com a multiplicação ordinária entre números (diferentes de zero), o que induziu a dar-lhe esse *mesmo nome* de *multiplicação*. Os grupos de substituições, que, por obra de Galois, se inserem na base da teoria algébrica das equações, aparecem assim como o primeiro exemplo importante de domínios operatórios, situados nitidamente fora da linha tradicional.

Mas um vigoroso impulso convergente para a superação dos esquemas tradicionais vem da escola dos algebristas ingleses do século XIX, cuja nota preponderante é a da originalidade e da independência mental. No breve período que vai de 1830 a 1850 assistimos ao aparecimento de novos, inusitados ramos da matemática: a álgebra da lógica com Boole (v. *álgebras de Boole* em *estruturas algébricas*), a álgebra dos vectores e dos quaterniões com Hamilton (v. *vector*), a álgebra das transformações lineares e das matrizes com Cayley.

A criação e o aprofundamento de novos domínios algorítmicos, obra executada ao longo de todo o século passado e no princípio deste, conduz a uma tal abundância de teorias e de resultados que se torna difícil ou mesmo impossível dominá-los em toda a sua extensão. Já não há uma só *álgebra*; existem agora várias *álgebras*, ou, melhor, várias *estruturas algébricas* ⁽¹⁾. Este facto, semelhante ao que se verifica ao mesmo tempo com o pluralismo geométrico, é apenas um aspecto dum fenómeno muito mais extenso, que chegará a instalar-se no campo da própria lógica, último reduto das verdades absolutas.

Mas há que sistematizar, ordenar, racionalizar: *há que restabelecer a unidade no caos da pluralidade*. É preciso que, das várias, infinitas álgebras possíveis, se construa uma ciência una, que seja de novo a Álgebra, ressurgida e transfigurada.

Esta síntese, que é hoje uma realidade, à qual se aplica a designação de *álgebra moderna* ou *álgebra abstracta*, já tinha sido esboçada pelos referidos algebristas ingleses, que abriram o caminho, introduzindo o conceito abstracto de *operação binária* (ou *lei de composição*) e fazendo uso do método axiomático. Mas o trabalho de unificação da álgebra segundo esta via foi executado sobretudo pela moderna escola alemã, começando com Dedekind e Hilbert, prosseguindo com Steinitz e atingindo a fase da maturidade, entre 1920 e 1930, com Emil Artin (actualmente na América) e com a matemática Emmy Noether.

Examinemos um pouco mais de perto a natureza destas concepções. Consideremos um conjunto U constituído por entidades de natureza qualquer (um conjunto de números, um conjunto de funções, um conjunto de matrizes, um conjunto de frases, um conjunto de conjuntos, etc.); chama-se *operação binária* ou *lei de composição* definida entre os elementos de U qualquer processo que faça corresponder, a cada par de elementos a, b de U (os *dados*), um determinado elemento c de U (o *resultado* da operação aplicada aos elementos a, b). Por exemplo, a adição definida entre matrizes dum mesmo tipo faz corresponder a cada par A, B de tais matrizes (*parcelas*) a matriz $C = A + B$ (*soma de A com B*). Por vezes consideram-se mais geralmente operações binárias em que um dos dados pertence a um conjunto Ω distinto de U , enquanto o outro dado e o resultado pertencem ainda ao conjunto U (*leis de composição externas*); exemplo típico de tais operações é a multiplicação de vectores por escalares (v. *vector*), de que é um caso particular a multiplicação de matrizes por números.

Quando num dado conjunto se definem uma ou mais operações binárias (internas ou externas), de modo a serem verificadas certas propriedades, diz-se que o conjunto está *algebrizado* ou que nele foi introduzida uma *estrutura algébrica*, por meio de tais operações. O que interessa, do ponto de vista da álgebra, não é a natureza dos elementos sobre os quais se opera, nem sequer a maneira

⁽¹⁾ O termo *álgebra*, como substantivo comum, é hoje usado em sentido restrito para designar uma determinada espécie de estruturas algébricas, também denominadas *sistemas hipercomplexos*. (V. *estruturas algébricas*).

como se efectuam as operações (isto compete à *aritmética da estrutura*), mas unicamente as *propriedades formais das operações definidas* (por exemplo, a associatividade, a comutatividade, etc., nos casos em que se verifiquem). Entre essas propriedades são elegidas algumas como *propriedades fundamentais* (também chamadas *axiomas*), a partir das quais se deduzem logicamente todas as outras.

As estruturas algébricas são classificadas de acordo com as propriedades das operações que as definem; surgem assim várias *espécies de estruturas algébricas*, cada uma das quais caracterizada por um conjunto de axiomas e todas dispostas numa complicada hierarquia, em que certas espécies estão subdivididas noutras espécies, estas possivelmente noutras ainda e assim por diante.

Não faremos aqui a descrição pormenorizada das estruturas algébricas; esse estudo é transferido para outro lugar (v. *estruturas algébricas*). Mas podemos desde já assentar no seguinte conceito:

A álgebra moderna tem por objecto estudar as diferentes espécies de estruturas algébricas. (O trabalho do algebrista moderno assemelha-se um pouco ao do naturalista).

Para cada uma dessas espécies constrói-se uma correspondente teoria deductiva, que será um ramo da nova álgebra. Deste modo, o estudo de várias, infinitas estruturas algébricas é feito em comum, dentro duma mesma espécie; todos os resultados, todos os teoremas assim estabelecidos, serão pois válidos em cada uma dessas estruturas, restando, quando muito, fazer uma interpretação dos termos empregados.

Mesmo *a priori* se pode imaginar o que tal unificação representa como economia de pensamento e como potência criadora. Faz-se agora em grande escala, a respeito das matemáticas tradicionais, o que a álgebra clássica tinha feito a respeito da aritmética com a introdução do conceito de variável.

Um exemplo ajudará talvez a esclarecer este último ponto de vista. Os processos de resolução algébrica das equações do 2.º grau são conhecidos desde longa data (já os Babilónios os sabiam aplicar); porém, a completa unificação desses processos numa síntese breve e luminosa pode dizer-se que só foi conseguida com o emprego das letras no papel de coeficientes variáveis, que permitiu condensar sob a forma de *equação literal* ($ax^2 + bx + c = 0$) as infinitas equações numéricas do 2.º grau existentes e dar, *uma vez por todas*, a chave da sua resolução, naquela fórmula algébrica hoje tão familiar a estudantes do liceu. Anteriormente, em vez duma só regra, davam-se várias, enunciadas em linguagem comum, e para a sua justificação empregavam-se várias páginas de prolixas considerações geométricas — enquanto hoje a dedução da fórmula resolvente se faz, com rigor e clareza, em meia dúzia de linhas!

Ora, pois, a álgebra moderna realiza, num plano superior, uma semelhante unificação simplificadora. Por exemplo, a analogia que mencionámos entre a teoria da divisibilidade para números inteiros e a teoria da divisibilidade para polinómios (no sentido clássico) estende-se a infinitas estruturas algébricas, hoje denominadas *anéis euclidianos*, para as quais pode ser construída, *uma vez por todas*, uma *teoria geral da divisibilidade*, aplicável a qualquer dessas estruturas e susceptível ainda de várias generalizações, que formam um dos problemas centrais da *teoria dos anéis*.

Por sua vez, a analogia de que falámos entre a teoria clássica das equações algébricas e a teoria das congruências relativas a módulo primo não é fortuita: encontra-se hoje esclarecida na teoria geral das equações algébricas, construída para *corpos comutativos* de natureza qualquer.

E vários outros exemplos poderiam ser apresentados.

Em todas estas teorias abstractas a natureza íntima dos problemas é posta a claro com limpidez cristalina. E, como é natural, ao mesmo tempo que sintetiza, libertando o essencial do accidental, clarificando e definindo as ideias, a moderna orientação abstracta oferece ainda *novos métodos de investigação e demonstração*, que permitem distinguir o verdadeiro do falso, lá onde os métodos clássicos se revelavam impotentes, por falta duma armadura lógica adequada que desembaraçasse o espirito da massa inerte das fórmulas ou de considerações metafísicas nebulosas. Acontecia isto, em particular, a respeito da geometria

algébrica, onde certos teoremas, apreendidos por intuição, não tinham podido ser demonstrados rigorosamente.

Como se disse atrás, os novos métodos axiomáticos não são exclusivos da álgebra: estendem-se a todas as matemáticas modernas. A par das estruturas algébricas, tem-se desenvolvido o estudo das chamadas *estruturas topológicas* (v. *topologia*); e os casos mais interessantes, pela riqueza e importância dos resultados, são aqueles em que, num mesmo conjunto, aparecem associadas uma estrutura algébrica e uma estrutura topológica (por exemplo, uma adição, uma multiplicação e uma operação de *limite*). Tais *estruturas algébrico-topológicas* formam precisamente o objecto de estudo da moderna análise infinitesimal. Assim, álgebra e topologia, ramos independentes da *análise moderna* (também chamada *análise geral*), acabam por conjugar-se numa união fecunda — a nova síntese do discreto e do contínuo —, que é a matemática da hora em que vivemos, a matemática do futuro.

BIBLIOGRAFIA:

- L. E. DICKSON — *Modern algebraic theories*, Chicago, Nova Iorque e Boston, 1930.
F. ENRIQUES — *Le matematiche nella storia e nella cultura*, Bolonha (Zanichelli), 1938.
R. FRICKE — *Lehrbuch der Algebra*, Braunschweig, 1924-1928.
F. GOMES TEIXEIRA — *História das Matemáticas em Portugal*, publicada pela Academia das Ciências de Lisboa, 1934.
C. JORDAN — *Traité des substitutions et des équations algébriques*, Paris (Gauthier-Villars), 1870.
P. NUNES — *Obras*, vol. VI: *Libro de Álgebra en Arithmetica y Geometria*, nova edição, revista e anotada por uma comissão de sócios da Academia das Ciências de Lisboa, 1950.
W. W. ROUSE BALL — *Histoire des Mathématiques*, tradução francesa da 3.^a edição inglesa, Paris (Hermann), 1906.
J. A. SERRET — *Cours d'Algèbre supérieure*, 3.^a ed. Paris (Gauthier-Villars), 1866.
H. WEBER — *Lehrbuch der Algebra*, Braunschweig, 1898-1899.
H. G. ZEUTHEN — *Histoire des Mathématiques dans l'Antiquité et le Moyen Age*, tradução francesa da edição dinamarquesa, Paris (Gauthier-Villars), 1902.

Nota. — Quanto a bibliografia sobre *álgebra moderna* ver as respectivas indicações bibliográficas no artigo *estruturas algébricas* da ENCICLOPÉDIA DA VIDA CORRENTE.