

PORTUGALIAE MATHEMATICA

Revista editada
por
ANTÓNIO MONTEIRO
com
a cooperação de
HUGO RIBEIRO, J. PAULO, M. ZALUAR NUNES

VOLUME 2
1941

FACULDADE DE CIÊNCIAS
LISBOA — PORTUGAL

Publicação subsidiada pelo Instituto para a Alta Cultura

PROBLEMAS RELATIVOS A FUNÇÕES RACIONAIS DAS RAÍZES DUMA EQUAÇÃO ALGÉBRICA

POR

JOSÉ SEBASTIÃO E SILVA ¹

1. Nova demonstração do teorema de Lagrange. O teorema de Lagrange, que se estabelece na teoria da resolubilidade algébrica, pode enunciar-se do seguinte modo:

Se uma função racional ψ das n variáveis x_1, x_2, \dots, x_n fica invariante para as substituições do grupo a que pertence outra função φ , também racional, das mesmas variáveis, pode a primeira exprimir-se racionalmente na segunda, e nos coeficientes da equação cujas raízes são x_1, x_2, \dots, x_n .

Com auxílio do teorema de que nos ocuparemos no § 2, respeitante a funções racionais duma só raiz duma equação algébrica, pode ainda afirmar-se que se fôr m o número dos valores distintos que toma φ , quando se trocam entre si, de todos os modos possíveis, as suas variáveis, existe um polinómio inteiro $p(X)$, de grau quando muito igual a $m-1$, cujos coeficientes são funções simétricas de x_1, x_2, \dots, x_n , e tal que $\psi = p(\varphi)$.

Nós vamos proceder por ordem inversa, demonstrando directamente a última proposição, e deduzindo desta o referido teorema.

Sejam, pois, $\varphi_1 = \varphi, \varphi_2, \dots, \varphi_m$, os valores (algébricos) diferentes, por que passa φ , quando, sobre as suas variáveis independentes, se efectuam tôdas as substituições do grupo simétrico; e, respectivamente, $\psi_1 = \psi, \psi_2, \dots, \psi_m$, os valores correspondentes, que podem não ser todos distintos, da função ψ , — entendendo-se que, se fôr s_h uma das substituições que transformam φ_1 , em φ_h , será também essa uma das substituições que mudam ψ_1 em ψ_h , qualquer que seja $h = 1, 2, \dots, m$.

Deve ainda supôr-se, que os sistemas de valores numéricos atribuídos às variáveis independentes serão apenas os que tornam as funções $\varphi_1, \varphi_2, \dots, \varphi_m$ numéricamente distintas, duas a duas; pois é obvio que, conquanto duas quaisquer destas funções não sejam, conforme a hipótese, idênticas entre si, é sempre possível determinar, pelo menos, um sistema de valores de x_1, x_2, \dots, x_n , para o qual duas dessas funções tomem o mesmo valor numérico. Por outro lado, existirá uma infinidade

¹ Bolseiro do Instituto para a Alta Cultura.

(com a potência do contínuo) de sistemas de valores de x_1, x_2, \dots, x_n , que tornam estas funções todas numericamente distintas.

Pósto isto, seja $p(X)$ um polinómio inteiro em X , de grau quando muito igual a $m - 1$ e de coeficientes a determinar pelas condições

$$(1) \quad \psi_i = p(\varphi_i) \quad (i = 1, 2, \dots, m).$$

Tomando para incógnitas os coeficientes do polinómio $p(X)$, as igualdades anteriores formam um sistema de Cramer, visto o determinante do sistema ser o determinante de Vandermonde, construído com as potências, de expoentes $0, 1, \dots, m - 1$, das funções $\varphi_1, \varphi_2, \dots, \varphi_m$, que, em virtude da hipótese estabelecida, só podem tomar valores numéricos diferentes entre si, dois a dois.

Resta, agora, demonstrar que os coeficientes do polinómio são funções simétricas de x_1, x_2, \dots, x_n . Para isso notemos que:

1.º Toda a substituição $s_{i,k}$ que muda φ_i em φ_k é também uma das que transformam ψ_i em ψ_k . Com efeito, será $s_{i,k} = s_k s_i^{-1} g$, sendo g uma substituição do grupo a que pertence a função φ . Mas, como s_i^{-1} muda ψ_i em ψ_1 , e s_k transforma ψ_1 em ψ_k , segue-se que $s_{i,k}$ faz passar de ψ_i para ψ_k , — como se tinha afirmado.

2.º Valores diferentes de φ , são convertidos em valores diferentes de φ , por efeito da mesma substituição. É isto uma consequência da propriedade, segundo a qual os dois produtos de substituições $s\sigma$ e $s'\sigma$ são diferentes, quando se tiver $s \neq s'$.

Vê-se, portanto, que uma substituição qualquer do grupo total, executada sobre as variáveis x_1, x_2, \dots, x_n , tem apenas, como resultado, alterar a ordem das equações (1), o que, evidentemente, não influi na solução do sistema. Os coeficientes do polinómio são, por conseguinte, funções simétricas de x_1, x_2, \dots, x_n , e dêste modo fica demonstrado o que pretendíamos.

No caso geral, para que ψ_j se possa exprimir racionalmente em ψ_k , é necessário que se tenha $j = k$. Porém, o mesmo não sucede, se o grupo a que pertence a φ é um sub-grupo invariante do grupo simétrico. Com efeito, sabe-se que, se fôr G o grupo a que pertence a $\varphi = \varphi_1$ e s_h uma substituição que transforme φ_1 em φ_h , será $s_h G s_h^{-1}$ o grupo das substituições que deixam invariante a função φ_h ($h = 1, 2, \dots, m$). Dêste modo, se G fôr um sub-grupo invariante do grupo simétrico, ter-se-á $s_h G s_h^{-1} = G$ e, portanto, a função ψ_h não é alterada por nenhuma substituição de G , o que torna possível exprimir racionalmente ψ_h em φ_1 , qualquer que seja $h = 1, 2, \dots, m$. Devemos notar que o polinómio por meio do qual se exprime ψ_h em função de φ_1 não é, em geral, o mesmo que permite exprimir ψ_k em função de φ_1 , quando $h \neq k$; porém, se

fôr $\psi_h = p(\varphi_1)$, ter-se-á também $\psi_{h,k} = p(\psi_k)$, sendo $\psi_{h,k}$ a função em que é transformada ψ_h por qualquer substituição que mude φ_1 em φ_k ($h, k = 1, 2, \dots, m$).

Em tudo o que segue, e quaisquer que sejam as convenções que se introduzam, cumulativamente, em cada caso particular, representaremos por $F(x) = 0$ a equação algébrica, cujas raízes são x_1, x_2, \dots, x_n .

Notemos, agora, que a demonstração apresentada indica, ao mesmo tempo, um processo para calcular os coeficientes do polinómio $p(X)$. Estes coeficientes aparecem, inicialmente, sob a forma de fracções, cujos termos são do tipo Au^p , em que A representa uma função simétrica de x_1, x_2, \dots, x_n e u o determinante de Vandermonde construído com as potências de expoente $0, 1, \dots, n-1$ daquelas variáveis; as fracções podem, pois, simplificar-se, de modo que os seus termos se reduzam a funções simétricas das variáveis.

Como exemplo de aplicação, determinemos o polinómio que, a partir do produto de duas raízes quaisquer da equação do 3.º grau

$$x^3 + px^2 + qx + r = 0$$

permite achar a soma das mesmas raízes. Teremos, representando por a, b e c as raízes da equação, e por A, B e C os coeficientes do polinómio,

$$\begin{cases} a + b = A(ab)^2 + B(ab) + C, \\ a + c = A(ac)^2 + B(ac) + C, \\ b + c = A(bc)^2 + B(bc) + C, \end{cases}$$

donde

$$\begin{aligned} A &= \frac{bc^2 - ac^2 + ab^2 - b^2c + a^2c - a^2b}{a^2bc^3 - ab^2c^3 + ab^3c^2 - a^2b^3c + a^3b^2c - a^3bc^2} \\ &= -\frac{(a-b)(a-c)(b-c)}{abc(a-b)(a-c)(b-c)} = \frac{1}{r}, \end{aligned}$$

e, análogamente, $B = -\frac{q}{r}$, $C = 0$.

O polinómio procurado será, portanto, $Y = \frac{X^2 - qX}{r}$.

2. Funções racionais duma só raiz. Suponhamos que são da seguinte forma, as funções φ e ψ a que nos referimos no § 1:

$$\begin{aligned} \varphi(x_1, x_2, \dots, x_n) &\equiv R(x_i), \\ \psi(x_1, x_2, \dots, x_n) &\equiv S(x_i), \end{aligned}$$

sendo $R(x)$ e $S(x)$ funções racionais de x que se conservam finitas quando se substitui a variável x por qualquer das raízes da equação $F(x) = 0$. Ter-se-á, evidentemente, $\varphi_i \equiv R(x_i)$ e $\psi_i \equiv S(x_i)$, qualquer que seja $i = 1, 2, \dots, n$.

Supondo agora que a equação $F(x) = 0$ não admite raízes múltiplas¹ pode afirmar-se, atendendo ao que foi estabelecido no § 1, que, *entre as funções $R(x_i)$ e $S(x_i)$, existe a relação*

$$S(x_i) = p[R(x_i)], \quad \text{para } i = 1, 2, \dots, n,$$

sendo $p(X)$ um polinómio inteiro em x , de coeficientes racionalmente conhecidos e de grau quando muito igual a $n-1$ (tem-se neste caso $m=n$).

É este um resultado já conhecido, que obtemos aqui por uma forma diferente da usual.

A equação cujas raízes são $R(x_1), R(x_2), \dots, R(x_n)$ é uma transformada de Tschirnhausen da equação $F(x) = 0$; o mesmo diremos a respeito da equação que tem como raízes $S(x_1), S(x_2), \dots, S(x_n)$. Pode então formular-se o resultado anterior de modo diferente, dizendo que *as raízes de qualquer transformada de Tschirnhausen da equação $F(x) = 0$ se podem escrever sob a forma dum polinómio inteiro $p(x)$, de coeficientes racionalmente conhecidos e de grau não superior a $n-1$, tomando para variável independente a raiz correspondente, de outra transformada de Tschirnhausen da mesma equação*. Não deixaremos de notar que, entre as transformadas de Tschirnhausen duma equação algébrica, se encontra a própria equação.

Seja Δ o menor corpo a que pertencem todos os coeficientes de equação $F(x) = 0$. Representemos por $\Delta(x_i)$ o corpo que se obtém pela adjunção a Δ da raiz x_i , e por $\Delta[x]$ o domínio da integridade constituído por todos os polinómios inteiros em x , de coeficientes situados em Δ , sendo x uma indeterminada. Seja por outro lado \mathfrak{H} o anel de classes resto $\frac{\Delta(x)}{\mathfrak{p}}$ em que \mathfrak{p} é o ideal gerado pelo polinómio $F_1(x)$, irredutível em Δ , que admite a raiz x_i . É claro que \mathfrak{H} é constituído por todos os polinómios inteiros em x , de coeficientes situados em Δ e de grau inferior a n_i , sendo n_i o grau da equação $F_1(x) = 0$.

Tendo em vista o resultado anterior, pode dizer-se que *existe um isomorfismo entre $\Delta(x_i)$ e \mathfrak{H} , que faz corresponder a cada elemento $R(x_i)$ de $\Delta(x_i)$ um elemento $p(x_i)$ de \mathfrak{H} , tal que $R(x_i) = p(x_i)$* . Estabelecemos assim, por via construtiva, um resultado já conhecido e susceptível de generalização².

3. Funções que mudam para tôdas as substituições do grupo simétrico. Seja φ uma função racional das n variáveis x_1, x_2, \dots, x_n , que

¹No caso de a equação $F(x) = 0$ admitir raízes múltiplas, pode passar-se para outra equação $F_1(x) = 0$, cujas raízes sejam tôdas raízes simples, numéricamente iguais às da primeira, — o que só introduz operações racionais.

²Van der Waerden, «Moderne Algebra», pg. 89-90.

toma $n!$ valores distintos $\varphi_1, \varphi_2, \dots, \varphi_{n!}$, quando se permutam de todos os modos possíveis as suas variáveis, isto é, uma função que pertence ao grupo constituído pela substituição identidade. Supõe-se neste § que a equação $F(x) = 0$ não admite raízes múltiplas. A equação que tem como raízes os valores $\varphi_1, \varphi_2, \dots, \varphi_{n!}$ é, como se sabe, uma resolvente de Galois da equação $F(x) = 0$ ¹. É evidente que qualquer outra função racional ψ das mesmas variáveis ficará invariante para as substituições do grupo a que pertence φ , visto que êsse grupo se reduz à identidade. Então pode afirmar-se que: *tôda a função racional das raízes da equação $F(x) = 0$ se pode exprimir em função duma das raízes duma sua resolvente de Galois, por meio dum polinómio inteiro, de coeficientes racionalmente conhecidos e de grau inferior a $n!$.*

Seja $p(X)$ o polinómio que permite exprimir $\psi = \psi_1$ em função de $\varphi = \varphi_1$; será também $p(X)$ o polinómio por meio do qual se exprime ψ_h em função de φ_h , qualquer que seja $h = 1, 2, \dots, n!$. Notemos porém que, neste caso, o grupo a que pertence a função φ , ou seja o grupo 1, é um sub-grupo invariante do grupo simétrico, o que nos habilita a afirmar que também ψ_h se pode exprimir em função de φ_1 , por meio dum polinómio, diferente, em geral, de $p(X)$. *Pode, pois, substituir-se no enunciado anterior a expressão «em função duma das raízes» por esta outra «em função de qualquer das raízes».* Obtém-se, dêste modo, à parte a forma, a conhecida proposição, enunciada primeiro por Abel, e demonstrada mais tarde por Galois no princípio da célebre memória sobre a resolubilidade algébrica.

Recordaremos de passagem que, se fôr Δ um corpo a que pertençam os coeficientes de $F(x) = 0$, o corpo $\Delta(x_1, x_2, \dots, x_n)$, obtido pela adjunção a Δ de tôdas as raízes de $F(x) = 0$, é idêntico ao corpo simples $\Delta(\varphi_1)$, obtido pela adjunção a Δ de uma das raízes, φ_1 , da resolvente de Galois da equação $F(x) = 0$: é isto uma consequência da última proposição estabelecida.

Devemos ainda notar que a função ψ pode em particular ter a forma $\psi(x_1, x_2, \dots, x_n) = x_1$; isto é, *as raízes da equação $F(x) = 0$ podem exprimir-se em função racional de qualquer das raízes duma sua resolvente de Galois.* Sejam $s_1 = 1, s_2, \dots, s_\mu$, em que $\mu = (n-1)!$, as substituições que trocam entre si, de todos os modos possíveis, as variáveis x_2, x_3, \dots, x_n , deixando fixa a variável x_1 , e sejam $\varphi_1, \varphi_2, \dots, \varphi_\mu$ os valores correspondentes da função φ : ter-se-á $\psi_1 = \psi_2 = \dots = \psi_\mu$, o que significa que existem μ polinómios diferentes, de grau inferior a $n!$, que permitem exprimir x_1 em função de $\varphi = \varphi_1$.

¹ Prof. A. de Mira Fernandes, «Grupos de substituições e resolubilidade algébrica», pág. 9-11.

4. **Funções simétricas dum determinado conjunto de raízes.** Um caso particular notável, que engloba o considerado no § 2, e do qual nos vamos ocupar pormenorizadamente, é aquêlê em que as funções φ e ψ se reduzem a funções simétricas de p das variáveis x_1, x_2, \dots, x_n , sendo $p < n$, e não figurando, por isso, explicitamente, as restantes variáveis. Serve de exemplo a função

$$\varphi(x_1, x_2, \dots, x_n) = x_1 + x_2 + \dots + x_p,$$

que podíamos pôr sob a forma

$$\varphi(x_1, x_2, \dots, x_n) = x_1 + x_2 + \dots + x_p + 0 \cdot x_{p+1} + \dots + 0 \cdot x_n.$$

Dum modo geral, ter-se-á, neste caso,

$$\varphi(x_1, x_2, \dots, x_n) = \Phi(x_1, x_2, \dots, x_p),$$

$$\psi(x_1, x_2, \dots, x_n) = \Psi(x_1, x_2, \dots, x_p),$$

sendo Φ e Ψ funções simétricas racionais de p variáveis.

As conseqüências que, do teorema demonstrado, resultam para êste caso, são de muito fácil dedução. *Em particular, se fôr $f_1(x) = 0$ a equação que tem como raízes x_1, x_2, \dots, x_p , e supondo que são entre si diferentes, dois a dois, os valores numéricos de $\varphi_1, \varphi_2, \dots, \varphi_m$, [neste caso é $m = \binom{n}{p}$], podemos afirmar que os coeficientes da equação $f_1(x) = 0$ são funções racionais inteiras de φ_1 , de coeficientes racionalmente conhecidos e de grau inferior a m .*

Os coeficientes da mesma equação podiam achar-se, como é sabido, utilizando o sistema

$$\begin{cases} F(x_1) = 0, \\ F(x_2) = 0, \\ \vdots \\ F(x_p) = 0, \\ \Phi(x_1, x_2, \dots, x_p) = 0, \end{cases}$$

o qual conduz, precisamente, à equação $f_1(x) = 0$, quando, na eliminação, tenha havido o cuidado de sujeitar os símbolos x_1, x_2, \dots, x_n , à condição de representarem, *de facto*, raízes algèbricamente distintas¹. Importa notar que, empregando êste processo, os coeficientes de $f_1(x) = 0$ vêm geralmente sob a forma de funções racionais fraccionárias dos coeficientes da equação $F(x) = 0$, não sendo, então, necessário que os valores numéricos de $\varphi_1, \varphi_2, \dots, \varphi_m$ sejam entre si diferentes, dois a dois, *mas apenas que o valor de φ_1 não coincida numèricamente com nenhum dos valores das restantes funções.*

Recordaremos ainda um outro processo que, no caso geral, se usa

¹ Comberousse, *Algèbre Supérieure*, 5.^a edição, II, pg. 454-455.

para determinar uma função racional (geralmente fraccionária), por meio da qual se possa exprimir ψ em φ . Consiste êste processo em construir a função $\lambda(X) = K(X) \left(\frac{\psi_1}{X - \varphi_1} + \frac{\psi_2}{X - \varphi_2} + \dots + \frac{\psi_m}{X - \varphi_m} \right)$, sendo $K(X) \equiv \prod_{i=1}^{i=m} (X - \varphi_i)$; e determinar, em seguida, ψ , a partir de φ , empregando a fórmula $\psi = \frac{\lambda(\varphi)}{K'(\varphi)}$.

Nós vamos adaptar êste processo à determinação dos valores de $\psi_1, \psi_2, \dots, \psi_\mu$, no caso em que se tenha, numéricamente,

$$\begin{aligned} \varphi_1 &= \varphi_h & (h=2, 3, \dots, \mu), \\ \varphi_1 &\neq \varphi_h & (h=\mu+1, \mu+2, \dots, m). \end{aligned}$$

É claro que, em tal caso, não são funções racionais dos coeficientes da equação $F(x) = 0$ os valores procurados, mas são-no, com certeza, os coeficientes da equação $\eta(Y) \equiv \prod_{i=1}^{i=\mu} (Y - \psi_i)$. Vejamos como determinar êsses coeficientes. Para isso, notemos que qualquer dêles se pode considerar função racional das raízes x_1, x_2, \dots, x_n ; sejam, nessas condições, $\eta_1(Y) = \eta(Y), \eta_2(Y), \dots, \eta_r(Y)$, em que $r = \binom{m}{\mu}$, as formas diferentes que toma o polinómio $\eta(Y)$, quando, sôbre aquelas variáveis, se executam tôdas as substituições do grupo simétrico; e $\chi_1(X) = \chi(X), \chi_2(X), \dots, \chi_r(X)$ as formas correspondentes, que toma o polinómio $\chi(X) \equiv \prod_{i=1}^{i=\mu} (X - \varphi_i)$, para as mesmas substituições. Então os coeficientes do polinómio

$$\theta(X, Y) \equiv K(X) \left[\frac{\eta_1(Y)}{\chi_1(X)} + \frac{\eta_2(Y)}{\chi_2(X)} + \dots + \frac{\eta_r(Y)}{\chi_r(X)} \right]$$

serão funções simétricas de x_1, x_2, \dots, x_n e, portanto, funções racionais dos coeficientes da equação $F(x) = 0$. Finalmente, é fácil ver que

$$\eta_1(Y) \equiv \frac{\mu! \theta(\varphi_1, Y)}{K^{(\mu)}(\varphi_1)},$$

tendo-se $K^{(\mu)}(\varphi_1) \neq 0$, visto que φ_1 é uma raiz da equação $K(X) = 0$, de grau de multiplicidade igual a μ .

Não se deve perder de vista que êste resultado é válido no caso geral, isto é, quaisquer que sejam as funções racionais φ e ψ das variáveis x_1, x_2, \dots, x_n . Em particular, podem, por êste processo, ser determinados os coeficientes da equação $f_1(x) = 0$ atrás considerada.

A título de curiosidade, vamos indicar processos especiais, para cada um dos dois casos seguintes:

1.º A função Φ reduz-se ao produto das p variáveis. Suponhamos que se aplicou a transformação $y = t - x$, à equação $F(x) = 0$, deixando t indeterminado, e se construiu a equação $P_t(X) = 0$ cujas raízes são os produtos das raízes p a p da transformada $F(t - y) = 0$. Nestas condições, a equação $P_t(X) = 0$, que tem por coeficientes funções de t , define X como função implícita, pluriforme de t , cujos $\binom{n}{p}$ ramos estão incluídos na expressão geral seguinte:

$$X_{i_1, i_2, \dots, i_p}(t) = (t - x_{i_1})(t - x_{i_2}) \dots (t - x_{i_p}),$$

em que i_1, i_2, \dots, i_p representam p quaisquer dos números $1, 2, \dots, n$.

Pondo, por comodidade, $X_{i_1, i_2, \dots, i_p}(t) \equiv X_i(t)$, e escrevendo esta função sob a forma $X_i(t) \equiv \alpha_0 + \alpha_1 t + \dots + \alpha_{p-1} t^{p-1} + t^p$, virá

$$\alpha_i = \frac{X_i^{(i)}(0)}{i!} \quad (i = 0, 1, 2, \dots, p-1).$$

Ora, como facilmente se conclui, as grandezas $\alpha_0, \alpha_1, \dots, \alpha_{p-1}$, são à parte um factor comum, os coeficientes da equação $f_1(x) = 0$, que admite soluções iguais às da equação $X_i(t) = 0$. Por outro lado, os números derivados $X'_i(0), X''_i(0), \dots, X_i^{(p-1)}(0)$, funções racionais de $\varphi_1 = (-1)^p x_1 x_2 \dots x_p$, podem calcular-se do seguinte modo: determinando $\frac{dX}{dt}$, a partir da equação $P_t(X) = 0$, pela regra das funções implícitas;

deduzindo da função $\frac{dX}{dt}$, as restantes funções derivadas, e fazendo, no final, em todas aquelas funções, $t = 0$ e $X = \varphi_1$. Assim ficará o problema resolvido.

Para que seja eficaz este processo, é apenas necessário que se tenha, numericamente, $\varphi_1 \neq \varphi_h$ ($h = 2, 3, \dots, m$).

Se esta condição não fôr satisfeita, e se tiver

$$\begin{aligned} \varphi_1 &= \varphi_h & (h = 2, 3, \dots, \mu), \\ \varphi_1 &\neq \varphi_h & (h = \mu + 1, \mu + 2, \dots, m), \end{aligned}$$

as derivadas parciais, em relação a X e a t , da função $P_t(X)$, que podemos pôr sob a forma $P_t(X) \equiv \pi(X, t)$, serão, para $t = 0$ e $X = \varphi_1$, todas nulas, até à ordem $\mu - 1$, inclusivé, como se pode verificar, e a equação que se obtém, desenvolvendo o primeiro membro da igualdade

$$\left[\frac{\partial \pi}{\partial X} \cdot \frac{dX}{dt} + \frac{\partial \pi}{\partial t} \right]_{\substack{X=\varphi_1 \\ t=0}}^{(\mu)} = 0,$$

e tomando $X'_i(0)$ para incógnita, será, deste modo, uma equação algébrica de grau μ , que permite calcular aquêl número derivado. É desneces-

sário indicar como se acham os restantes números derivados. Interessa, apenas, notar que o problema terá agora μ soluções, e é evidente que os coeficientes da equação $f_1(x) = 0$ já não são, neste caso, funções racionais de ρ_1 .

Nota — Para construir a equação cujas raízes são os produtos das raízes, p a p , duma equação dada, vários processos podem indicar-se. Não apresentaremos, contudo, nenhum desses processos, porque não vemos nisso interesse especial; limitamo-nos a observar que os coeficientes de tal equação podem achar-se directamente, aplicando a teoria das funções simétricas.

2.º A função simétrica das p raízes reduz-se à soma das mesmas raízes.

Suponhamos que se aplicou à equação $F(x) = 0$ a transformação definida por $y = \frac{1}{\frac{1}{x} - t}$, em que t é um parâmetro variável, e se cons-

truiu a equação $S_i(X) = 0$, que tem como raízes as somas das raízes, p a p , da equação transformada. A equação $S_i(X) = 0$ define X como função implícita, pluriforme de t , com $\binom{n}{p}$ ramos, incluídos na seguinte expressão

$$X_{i_1, i_2, \dots, i_p}(t) \equiv \frac{1}{\frac{1}{x_{i_1}} - t} + \frac{1}{\frac{1}{x_{i_2}} - t} + \dots + \frac{1}{\frac{1}{x_{i_p}} - t}.$$

Fazendo, por comodidade, $X_{1,2,\dots,p}(t) \equiv X_1(t)$, será

$$X_1^{(i)}(0) = \frac{1}{i!} (x_1^{i+1} + x_2^{i+1} + \dots + x_p^{i+1}) \quad (i = 0, 1, 2, \dots, p-1).$$

Ora, como é sabido, a partir das funções simétricas do tipo $\sum_{k=1}^p x_k^i$, para $i = 0, 1, \dots, p$, podem determinar-se todos os coeficientes da equação $f_1(x) = 0$. Por outra parte, os números derivados $X_1'(0)$, $X_1''(0)$, \dots , $X_1^{(p-1)}(0)$, podem calcular-se por um processo inteiramente análogo ao que foi indicado, para fim semelhante, no caso anterior.

Também aqui é necessário e suficiente que se tenha

$$\varphi_1 \neq \varphi_h \quad (h = 2, 3, \dots, m),$$

para que o processo não seja ilusório.

Na hipótese de ser

$$\begin{aligned} \varphi_1 &= \varphi_h & (h = 2, 3, \dots, \mu), \\ \varphi_1 &\neq \varphi_h & (h = \mu + 1, \mu + 2, \dots, m), \end{aligned}$$

ajusta-se a este caso, mutatis mutandis, tudo o que, em circunstância idêntica, se disse para o caso anterior.

Nota — Os coeficientes da equação que tem como raízes as somas das raízes, p a p , duma dada equação, podem calcular se directamente pelo método das funções simétricas.

Todavia, convém notar que, neste caso, basta saber calcular o termo conhecido da equação, por isso que os restantes coeficientes se deduzem, facilmente, da expressão daquêlê. Com efeito, imaginemos que, sujeitando a equação $F(x) = 0$ à transformação $y = \frac{u}{p} - x$, sendo u variável, se obtém a equação $R_u(y) = 0$, cujos coeficientes serão funções de u . Considerando a função

$$\begin{aligned}\theta(y_1, y_2, \dots, y_n) &\equiv \left(\frac{u}{p} - x_1\right) + \left(\frac{u}{p} - x_2\right) + \dots + \left(\frac{u}{p} - x_p\right) \\ &\equiv u - (x_1 + x_2 + \dots + x_p)\end{aligned}$$

e designando por $\theta_1 = \theta, \theta_2, \dots, \theta_m$ os valores distintos da função θ , para tôdas as substituições do grupo simétrico, será evidentemente $\theta_1 \cdot \theta_2 \dots \theta_m$, produto daquelas funções, o termo conhecido da equação cujas raízes são as somas das raízes, p a p , da equação $R_u(y) = 0$. Então, representando por $\tau(u)$ êsse produto (que é, manifestamente, função de u), será a igualdade $\tau(u) = 0$ a equação que tem como raízes as somas das raízes, p a p , da equação $F(x) = 0$.

Assim, por exemplo, quaisquer que sejam os coeficientes da equação do 4.º grau $x^4 + Ax^3 + Bx^2 + Cx + D = 0$ cujas raízes designaremos por a, b, c, d , ter-se-á, sempre $(a + b)(a + c)(a + d)(b + c)(b + d)(c + d) = \Sigma a^3 b^2 cd + 2 \Sigma a^3 bcd + + 3 \Sigma a^2 b^2 c^2 + 4 \Sigma a^2 b^2 cd = A(BC - AD) - C^2$; por isso, dada a equação $f(x) \equiv x^4 + kx^3 + px^2 + qx + r = 0$, que se transforma na equação

$$y^4 - \frac{1}{3!} f''' \left(\frac{u}{2} \right) y^3 + \frac{1}{2!} f'' \left(\frac{u}{2} \right) y^2 - f' \left(\frac{u}{2} \right) y + f \left(\frac{u}{2} \right) = 0,$$

quando se faz $y = \frac{u}{2} - x$, será

$$\frac{1}{6} f''' \left(\frac{u}{2} \right) \left[\frac{1}{2} f'' \left(\frac{u}{2} \right) f' \left(\frac{u}{2} \right) - \frac{1}{6} f''' \left(\frac{u}{2} \right) \cdot f \left(\frac{u}{2} \right) \right] - \left[f' \left(\frac{u}{2} \right) \right]^2 = 0$$

a equação cujas raízes são as somas das raízes, duas a duas, da equação $f(x) = 0$.

Para $k = 0$, a última equação toma a seguinte forma:

$$u^6 + 2pu^4 + (p^2 - 4r)u^2 - q^2 = 0,$$

resultado que oportunamente aproveitaremos.

5. Decomposição de polinómios em factores irreduzíveis; equações susceptíveis de abaixamento. Neste, e nos parágrafos seguintes, trataremos de aplicar, à resolução de alguns problemas conhecidos, os resultados anteriormente expostos.

Em virtude do que foi estabelecido, o conhecimento do valor duma função simétrica de p raízes da equação de grau n , $F(x) = 0$, torna geralmente possível substituir esta equação por duas outras, uma de grau p e a outra de grau $n - p$, cujos coeficientes sejam funções racionais daquêlê valor. Em particular, se o referido valor pertencer ao corpo Δ definido pelos coeficientes da equação $F(x) = 0$, esta será redutível.

Dum modo geral, pode afirmar-se que *é condição necessária para que uma equação seja redutível, que exista, pelo menos, uma função simétrica de p raízes dessa equação (sendo p qualquer dos números $1, 2, \dots, n-1$), cujo valor pertença ao corpo definido pelos coeficientes da mesma equação.*

Esta condição não é contudo suficiente. Com efeito, suponhamos que sendo p um divisor de n e $\mu = \frac{n}{p}$, se tem, numéricamente,

$\Phi(x_1, x_2, \dots, x_p) = \Phi[x_{kp+1}, x_{kp+2}, \dots, x_{(k+1)p}] = \alpha$ para $k = 1, 2, \dots, \mu - 1$. Então, o conhecimento de α não adianta nada, em geral, relativamente à decomposição de $F(x)$, em factores de coeficientes situados em Δ .

Em todos os restantes casos, porém, o polinómio $F(x)$ será, com certeza, decomponível em factores daquela natureza. Poderia, assim, formular-se uma condição necessária e suficiente para que uma equação algébrica seja redutível.

Se, verificando-se a última condição, não houver combinação alguma de p raízes de $F(x) = 0$, além das indicadas, para a qual a função Φ tome o valor numérico α , a equação $F(x) = 0$ será susceptível de abaixamento: a sua resolução torna-se, então, equivalente à de uma equação de grau μ (a resolvente), seguida (no caso de tal equação não admitir raízes múltiplas) da resolução de μ equações, $f_1(x) = 0, f_2(x) = 0, \dots, f_\mu(x) = 0$, todas de grau p , e tais que $f_1(x) \cdot f_2(x) \cdots f_\mu(x) = F(x)$. Estas μ equações estão em correspondência biunívoca com as raízes da resolvente, sendo os coeficientes de cada uma, funções racionais da raiz correspondente; por isso, tais coeficientes não pertencerão, geralmente, ao corpo definido pelos coeficientes da proposta.

O que acabamos de afirmar não é senão uma consequência do que, no § anterior, foi estabelecido a respeito do caso em que os valores de algumas das funções $\varphi_1, \varphi_2, \dots, \varphi_n$, coincidem numéricamente. Deve acrescentar-se que, se a resolvente admitir k raízes múltiplas, será ainda preciso resolver, depois dessa, k equações auxiliares; e que, se algumas destas admitirem também raízes múltiplas, se lhes deve aplicar o que se disse para a primeira; e assim sucessivamente. É manifesto que, à medida que se passa de umas para outras equações, o grau das mesmas baixará muito rapidamente.

No tipo de equações anteriormente consideradas, estão incluídas as equações recíprocas, e as equações a que faltam os termos de grau impar. No primeiro caso, tem-se, representando, numa ordem conveniente, por x_1, x_2, \dots, x_{2n} as raízes da proposta, diferentes de 1 e de -1 : $x_1 x_{2n} = x_2 x_{2n-1} = \dots = x_n x_{n+1} = 1$; o que permite formar, empregando apenas operações racionais, a equação que tem como raízes $x_1 + x_{2n}, x_2 + x_{2n-1}, \dots, x_n + x_{n+1}$. No segundo caso, será, adoptando a mesma

representação das raízes: $x_1 + x_{2n} = x_2 + x_{2n-1} = \dots = x_n + x_{n+1} = 0$; pode então passar-se imediatamente para a equação que tem como raízes $x_1 x_{2n} = -x_1^2, x_2 x_{2n-1} = -x_2^2, \dots, x_n x_{n+1} = -x_n^2$.

Posto isto, notemos que, se o polinómio $F(x)$ fôr decomponível no produto de dois polinómios $f_1(x)$ e $f_2(x)$, de coeficientes situados em Δ , o valor de *qualquer* função simétrica das raízes de $f_1(x)$, ou das raízes de $f_2(x)$, pertencerá também a Δ . O problema da decomposição de $F(x)$ em factores irreduzíveis pode então resolver-se, tendo em atenção esta e as anteriores considerações; sendo manifesto que, para tal fim, existirá uma infinidade de maneiras de proceder distintas, conducentes ao mesmo resultado. É claro que nem todos estes modos de proceder serão igualmente vantajosos: está naturalmente indicado o emprêgo de funções simétricas das p raízes ($p < n$) que coincidam ou com a soma ou com o produto dessas p raízes, e é fácil ver que, em tal caso, os processos não diferem, no fundo, dos conhecidos, em que se aplica o método dos coeficientes indeterminados.

Não iremos indicar pormenorizadamente, como se procede, para a resolução do referido problema. Limitar-nos-emos a dizer que, no caso em que se adopte como função simétrica a soma ou o produto, será necessário construir $n - 1$ equações, cada uma das quais tem como raízes as somas (ou os produtos) das raízes p a p da proposta ($p = 1, 2, \dots, n - 1$); procurar em seguida, raízes destas equações que pertençam a Δ ; fazer a decomposição de $F(x)$ a partir dessas raízes; repetir a operação indicada para cada um dos polinómios obtidos, e assim sucessivamente. Dêste modo, é-se levado, necessariamente, à decomposição de $F(x)$, em factores irreduzíveis. É claro que entre as equações consideradas se encontra a equação proposta. O problema complica-se, quando a raiz achada seja uma raiz múltipla, mas encontram-se atrás elementos que permitem resolver completamente esta dificuldade.

6. Resolução de equações por meio de resolventes. Aplicando os resultados anteriormente expostos, é possível imaginar processos de resolução de equações algébricas, com emprêgo de equações auxiliares.

Assim, por exemplo, é possível resolver uma equação do 6.º grau, começando por determinar uma só raiz θ duma equação do 10.º grau, e resolvendo, em seguida, duas equações do 3.º, cujos coeficientes são funções racionais de $\sqrt{\theta}$. Com efeito, se transformarmos a equação do 6.º grau proposta, de modo que se anule o coeficiente do termo em x^5 , teremos, representando por $x_1, x_2, x_3, x_4, x_5, x_6$ as raízes da equação transformada: $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 0$; o que nos habilita a afirmar que a equação, cujas raízes são as somas das raízes $x_1, x_2,$

x_3, x_4, x_5, x_6 tomadas 3 a 3, é tal que, se admite a raiz α , admite igualmente a raiz $-\alpha$. Trata-se, pois, duma equação do 20.º grau a que faltam os termos de grau ímpar, e que pode, portanto, ser substituída por uma do 10.º grau. Dêste modo, determinada uma raiz da última equação, e extraída a sua raiz quadrada, podemos, atendendo ao que foi dito no § 4, construir duas equações do 3.º grau, cujas raízes são, no seu conjunto, $x_1, x_2, x_3, x_4, x_5, x_6$.

Chega-se a um resultado equivalente, se, em vez da transformação que produz o desaparecimento do termo em x_5 , se efectuar a transformação, pela qual o termo independente se torna igual ao coeficiente do primeiro termo; neste caso, como o produto das raízes da transformada é igual à unidade, a equação cujas raízes são os produtos das raízes daquela, tomadas três a três, é uma equação recíproca, que poderá, como anteriormente, ser substituída por uma do 10.º grau.

Para a equação do 4.º grau, haverá dois processos correspondentes. Sejam a, b, c, d , as raízes da equação do 4.º grau, privada do 2.º termo, $x^4 + px^2 + qx + r = 0$.

A equação que tem como raízes a soma das raízes, duas a duas, da anterior é, como se viu, $u^6 + 2pu^4 + (p^2 - 4r)u^2 - q^2 = 0$, que se transforma na equação $z^3 + 2pz^2 + (p^2 - 4r)z - q^2 = 0$, para $z = u^2$.

Esta última equação não é outra senão a resolvente que se obtém, quer pelo método de Descartes, quer (à parte uma transformação elemental) pelo método de Lagrange. O conhecimento duma das suas raízes basta para que a resolução da proposta se reduza à de duas equações do 2.º grau. Mas será ainda mais simples o modo de proceder, se, em vez de uma, se conhecerem as três soluções da resolvente. Com efeito, por ser $(a + b) + (a + c) + (a + d) = 2a + (a + b + c) = 2a$ e atendendo a que é a uma raiz *qualquer* da proposta, as raízes desta serão os valores de x , dados pela fórmula $x = \frac{1}{2}(\sqrt{z_1} + \sqrt{z_2} + \sqrt{z_3})$ para combinações convenientes das determinações de $\sqrt{z_1}, \sqrt{z_2}, \sqrt{z_3}$. Ora a maneira de combinar, convenientemente, os sinais das raízes quadradas, pode deduzir-se, tendo em vista as igualdades

$$\begin{aligned} a + b &= -(c + d), \\ a + c &= -(b + d), \\ a + d &= -(b + c), \end{aligned}$$

donde se conclui que, se forem α, β, γ os valores que conduzem à determinação de a , serão $\alpha, -\beta, -\gamma$ os que permitem achar $b, -\alpha$,

¹ É claro que $\alpha = a + b, \beta = a + c, \gamma = a + d$.

β , $-\gamma$ os que definem c e $-\alpha$, $-\beta$, γ os correspondentes a d . Em resumo, os valores a tomar, de cada vez, na aplicação da fórmula anterior, devem ser tais que o seu produto tenha o sinal de

$$(a+b)(a+c)(a+d) = a^2(a+b+c+d) + (bc+bd+cd)a + bcd \\ = abc + abd + acd + bcd,$$

portanto o sinal do coeficiente $-q$. Dêste modo se chega, mais uma vez, a um resultado conhecido.

Se, em vez da equação do 4.º grau privada do 2.º termo, se tivesse tomado como ponto de partida a equação do mesmo grau, com o termo independente igualado ao coeficiente do 1.º termo, chegar-se-ia a uma resolvente, que é a mesma que se obtém pelo método de Ferrari.

7. **Determinação duma raiz, conhecido apenas o módulo, a parte real ou o argumento.** Neste §, consideraremos, separadamente, cada um dos problemas seguintes:

1.º *Dado o módulo duma raiz, determinar a parte real dessa raiz.* No caso geral, isto é, quando se trate duma equação $F(z) = 0$, de coeficientes imaginários quaisquer, não será possível aplicar, à resolução dêste problema, os resultados anteriormente expostos. Fazendo $z = x + iy$, pode escrever-se $F(z) = \varphi(x, y) + i\psi(x, y)$, em que φ e ψ são funções inteiras, de coeficientes reais, das variáveis reais x e y . Seja, então, ρ , o módulo duma raiz, e consideremos o sistema, necessariamente possível,

$$\begin{cases} \varphi(x, y) = 0 \\ \psi(x, y) = 0 \\ x^2 + y^2 = \rho^2. \end{cases}$$

A eliminação de y entre a primeira equação e a última, por um lado; e entre a segunda e a última, por outro lado, conduz a um sistema de duas equações a uma só incógnita, ambas de grau $2n$, sendo n o da proposta, e que admitem, *geralmente*, uma só raiz comum, que é a parte real da raiz de módulo ρ , se êste fôr diferente dos módulos das outras raízes.

Não chegámos, portanto, a fazer uso do que foi estabelecido nos §§ anteriores; e o que se dá, no caso geral, em relação a êste problema, verifica-se igualmente, para os que vão ser considerados em seguida.

Porém, se os coeficientes da equação $F(x) = 0$ forem todos reais, a questão simplifica-se consideravelmente, tornando-se já possível a aplicação da matéria dos §§ anteriores, e haverá dois métodos diferentes, conforme se trate duma raiz real ou duma raiz imaginária.

Se a raiz fôr imaginária, como o quadrado do módulo é igual ao produto da raiz pela sua conjugada, e a soma das duas, igual ao dôbro da parte real comum, o problema a resolver é o da determinação da

soma de duas raízes, a partir do seu produto, — caso particular de outro problema que já foi estudado com desenvolvimento no § 4.

Tratando-se duma raiz real, o cálculo da parte real ou do coseno do argumento equivale à determinação do sinal, uma vez que se considera conhecido o módulo. Então o problema reduz-se a este outro: determinar uma raiz, conhecido o seu quadrado; implícito noutro, de maior generalidade, e que consiste em, dada a potência de expoente n duma raiz, determinar essa raiz. Ora sabe-se que, sendo α raiz da equação $F(x) = 0$, existe uma função inteira $p(x)$, de coeficientes racionalmente conhecidos, e de grau quando muito igual a $n - 1$, tal que $\alpha = p(\alpha^n)$. O problema pode ainda resolver-se de outras maneiras.

2.º *Conhecida a parte real, determinar o módulo.* O problema só tem interesse quando a raiz fôr imaginária. Atendendo às observações anteriormente feitas, vê-se imediatamente que, no caso de a equação ter os coeficientes reais, se trata de determinar o produto de duas raízes, conhecida a sua soma.

3.º *Determinar o módulo ou a parte real, conhecido o argumento.* Só interessa, evidentemente, o caso em que a raiz é imaginária. Então, se a equação tem todos os coeficientes reais, dado o argumento ω duma raiz x_1 , e representando por x_2 a raiz conjugada, ter-se-á $\cos 2\omega = \frac{x_1^2 + x_2^2}{x_1 x_2}$. Como as funções de raízes $x_1 + x_2$ e $x_1 x_2$ pertencem ao

mesmo grupo que a função $\frac{x_1^2 + x_2^2}{x_1 x_2}$, será possível exprimi-las racionalmente nesta última, o que resolve o problema.

NOTAS

A) Na demonstração do § 1 supomos, inicialmente, que o polinómio $p(X)$ é de grau $m - 1$, e indicamos como se faz, nessa hipótese, a determinação dos coeficientes do polinómio $p(X)$, tomados para incógnitas dum sistema de equações lineares; mas nada impede, evidentemente, que o coeficiente do pressuposto primeiro termo, e, porventura, de alguns dos seguintes, venha a receber no resultado o valor zero, o que significa, afinal, que o polinómio não era de grau $m - 1$, como se tinha suposto, mas de grau inferior a êsse.

B) A demonstração que apresentamos no § 1 pode facilmente adaptar-se ao caso em que o grupo das substituições que deixam invariante a função φ esteja contido no grupo G de Galois da equação $F(x) = 0$, relativamente a um dado corpo Δ que contenha os coeficientes dessa equação. Basta, então, considerar os valores distintos $\varphi_1 = \varphi, \varphi_2, \dots, \varphi_\mu$, da

função φ , para tôdas as substituições de G , e os correspondentes valores $\psi_i = \psi, \psi_2, \dots, \psi_\mu$ da função ψ , para as mesmas substituições. Representando por $p(X)$ um polinómio inteiro em X do grau $\mu - 1$, tal que $\psi_i = p(\varphi_i)$, para $i = 1, 2, \dots, \mu$, é fácil ver que os coeficientes de tal polinómio são funções racionais de x_1, x_2, \dots, x_n , que permanecem invariantes para tôdas as substituições de G , o que¹ nos habilita a afirmar que tais coeficientes são esprimíveis racionalmente nos coeficientes da equação proposta. Chegamos, dêste modo, a um outro resultado conhecido.

C) Tôdas as vezes que, neste trabalho, nos referimos a funções racionais das raízes da equação $F(x) = 0$, é evidente que pressupomos a existência dum corpo qualquer, no qual estejam contidos, juntamente com os coeficientes daquela equação, os coeficientes da função considerada. Nestas condições, diremos, por comodidade, que uma função das variáveis independentes x_1, x_2, \dots, x_n é racional *em relação* a um dado corpo Δ , se constitui um elemento do corpo ampliado $\Delta(x_1, x_2, \dots, x_n)$; análogamente, diremos que tal função é inteira *em relação* a Δ , se fôr um elemento do domínio de integridade $\Delta[x_1, x_2, \dots, x_n]$.

Então, se fôr Δ um corpo a que pertençam os coeficientes da equação $F(x) = 0$, e $\Phi(x_1, x_2, \dots, x_r)$ uma função racional (em relação a Δ) das raízes x_1, x_2, \dots, x_r , sendo $r \leq n$, pode considerar-se Φ como função exclusiva da variável x_1 , $\Phi = R(x_1)$, de coeficientes situados no corpo ampliado $\Delta_1 = \Delta(x_2, x_3, \dots, x_r)$, — o que permite afirmar que Φ é função racional de x_1 , em relação a Δ_1 . Dêste modo, a função $R(x_1)$ poderá, em virtude da proposição do § 2, ser substituída por uma função de x_1 inteira em relação a Δ_1 , e de grau inferior a n . Por outro lado, como os coeficientes de $R(x_1)$ são funções racionais das raízes x_2, x_3, \dots, x_r , pode, a cada uma dessas funções, aplicar-se o que se disse para a função Φ , o que leva a substituir os coeficientes de $R(x_1)$ por funções inteiras duma das raízes x_2, x_3, \dots, x_r , de grau inferior a n e de coeficientes expressos racionalmente nas restantes raízes. Continuando a raciocinar dêste modo, chega-se inevitavelmente à conclusão de que é possível substituir a função Φ por uma função inteira das variáveis x_1, x_2, \dots, x_r , de grau inferior a n em relação a cada uma dessas variáveis, e de coeficientes situados em Δ .

Êste resultado constitui uma conhecida generalização do teorema do § 2².

Original recebido na Redacção em Novembro de 1940

¹ Prof. A. de Mira Fernandes, obra já citada, Tomo II, pág. 14, Teorema I.

² Serret, «Cours d'Algèbre Supérieure», pág. 408-412.