I.1

INTRODUÇÃO ÀS MODERNAS TEORIAS ALGÉBRICAS

(Apenas o esboço dum curso de iniciação)

Página em branco

CAPÍTULO III

RESOLUBILIDADE POR MEIO DE RADICAIS
(1ª parte)

28. O teorema das funções simétricas

Consideremos a equação do 2.º grau

$$az^2 + bz + c = 0.$$

As raízes z_1, z_2 desta equação estão relacionadas com os coeficientes *a, b, c*, por meio das conhecidas fórmulas

$$z_1 + z_2 = -\frac{b}{a}, \quad z_1 z_2 = \frac{c}{a}.$$

Como se sabe, utilizando estas relações, torna-se possível calcular, por exemplo, a soma dos quadrados das raízes, o quadrado da diferença das raízes, etc., sem recorrer à formula resolvente da equação – efectuando sobre os coeficientes *a, b, c*, apenas operações racionais: adições, subtracções, multiplicações e divisões. Com efeito:

$$z_1^2 + z_2^2 = (z_1 + z_2)^2 - 2\, z_1 z_2 = \frac{b^2}{a^2} - 2\,\frac{c}{a} = \frac{b^2 - 2\,ac}{a^2}$$

$$(z_1 - z_2)^2 = (z_1 + z_2)^2 - 4\, z_1 z_2 = \frac{b^2}{a^2} - 4\,\frac{c}{a} = \frac{b^2 - 4\,ac}{a^2}$$

Mas note-se: a soma $z_1 + z_2$, o produto $z_1 z_2$, a soma dos quadrados $z_1^2 + z_2^2$, o quadrado da diferença $(z_1 - z_2)^2$, etc. são funções simétricas de z_1, z_2 (pensando z_1, z_2 como variáveis independentes). Ocorre então perguntar: Dada uma função simétrica (racional) das raízes duma equação algébrica, será sempre possível exprimir *racionalmente* essa função nos coeficientes da equação proposta?

Consideremos, em geral, a equação algébrica de grau n:

$$f(z) \equiv a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n = 0$$

($a_0, a_1, \ldots, a_n$ – números complexos quaisquer).

Sendo $z_1, z_2, \ldots, z_n$ as raízes desta equação (oportunamente repetidas quando múltiplas), tem-se, como é sabido,

$$f(z) \equiv a_0 (z - z_1)(z - z_2) \cdots (z - z_n).$$

Designemos por s_1 a soma das raízes, por s_2 a soma dos produtos das raízes duas a duas, por s_3 a soma dos produtos das raízes três a três, ..., por s_n o produto das n raízes; isto é, em símbolos:

$$s_1 = \sum z_1 = z_1 + z_2 + \cdots + z_n,$$

$$s_2 = \sum z_1 z_2 = z_1 z_2 + z_1 z_3 + \cdots + z_1 z_n + \cdots + z_{n-1} z_n,$$

$$s_3 = \sum z_1 z_2 z_3 = z_1 z_2 z_3 + z_1 z_2 z_4 + \cdots + z_{n-2} z_{n-1} z_n,$$

....

$$s_n = \sum z_1 z_2 \cdots z_n = z_1 z_2 \cdots z_n.$$

Imediatamente se reconhece que $s_1, s_2, \ldots, s_n$ são funções simétricas de $z_1, z_2, \ldots, z_n$ – chamadas precisamente as *funções simétricas elementares* das raízes (pensando estas como variáveis independentes). Os valores de tais funções são dados, a partir dos coeficientes da equação, pelas formulas notáveis

$$s_1 = -\frac{a_1}{a_0}, \quad s_2 = \frac{a_2}{a_0},$$

$$s_3 = -\frac{a_3}{a_0}, \ \ldots \ \ldots, \ s_n = (-1)^n \frac{a_n}{a_0}.$$

Pois bem, nos tratados de Álgebra Superior[1] costuma demonstrar-se o seguinte teorema:

Toda a função racional inteira e simétrica (com os coeficientes inteiros) de n variáveis $z_1, z_2, \ldots, z_n$ *pode exprimir-se como função racional inteira (com coeficientes inteiros) das funções simétricas elementares de* $z_1, z_2, \ldots, z_n$.

Para ver como, na prática, se consegue efectivamente exprimir uma dada função racional inteira e simétrica de $z_1, z_2, \ldots, z_n$ como função racional inteira de $s_1, s_2, \ldots, s_n$, convém introduzir algumas convenções prévias.

a) Dados dois monónimos não semelhantes, nas variáveis $z_1, z_2, \ldots, z_n$

$$A = a\, z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n}, \quad B = b\, z_1^{\beta_1} z_2^{\beta_2} \cdots z_n^{\beta_n}$$

diremos que *A tem uma ordem superior* à de *B*, quando a primeira das diferenças $\alpha_1 - \beta_1, \alpha_2 - \beta_2, \ldots, \alpha_n - \beta_n$ que não é nula, é positiva. Dois monómios semelhantes dir-se-ão de *igual ordem*.

b) Dada uma função racional inteira $\varphi(z_1, z_2, \ldots, z_n)$ (que supomos já reduzida à forma dum polinómio inteiro em $z_1, z_2, \ldots, z_n$, sem termos semelhantes nem termos nulos), chamaremos *primeiro termo de* φ ao termo de ordem mais elevada do polinómio que representa φ. Facilmente se demonstra que, *se* φ *é uma função racional inteira e simétrica de* $z_1, z_2, \ldots, z_n$ *e se o seu primeiro termo é*

$$a\, z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n}$$

então deve ser

$$\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_n .$$

Seja então $U = \varphi(z_1, z_2, \ldots, z_n)$ uma função racional inteira e simétrica de $z_1, z_2, \ldots, z_n$ e seja

$$a\, z_1^{\alpha_1} z_2^{\alpha_2} \cdots z_n^{\alpha_n}$$

(1) – Veja-se Prof. VICENTE GONÇALVES, *Curso de Álgebra Superior,* 2.º vol.

o seu primeiro termo. Consideremos o produto

$$P = a\, s_1^{\alpha_1 - \alpha_2}\, s_2^{\alpha_2 - \alpha_3} \cdots s_n^{\alpha_n}.$$

Desde logo se reconhece que P é uma função simétrica (racional inteira) de $z_1, z_2, \ldots, z_n$. Além disso, é fácil provar que o primeiro termo de P resulta idêntico ao primeiro termo de U. Então, a diferença $U - P$, que representaremos por U_1, será ainda uma função racional inteira e simétrica de $z_1, z_2, \ldots, z_n$, *cujo primeiro termo terá uma ordem inferior à do primeiro termo de U.* Aplicando a U_1 o que se disse para U, vê-se que a função U_1 é, por sua vez, redutível à forma $U_1 = P_1 + U_2$, em que P_1 representa um produto de potências de $s_1, s_2, \ldots, s_n$ e U_2 uma função racional inteira e simétrica de $z_1, z_2, \ldots, z_n$ cujo primeiro termo é de ordem inferior ao do primeiro termo de U_1. Procedendo assim, sucessivamente, chegar-se-á por força a uma função identicamente nula:

$$U - P = U_1, \quad U_1 - P_1 = U_2, \ldots, \quad U_r - P_r = 0.$$

Destas igualdades resultará, finalmente,

$$U = P + P_1 + P_2 + \cdots + P_r,$$

sendo $P, P_1, \ldots, P_r$ monómios em $s_1, s_2, \ldots, s_n$.

Assim, o valor de U será dado por uma função $F(s_1, s_2, \ldots, s_n)$ racional inteira em $s_1, s_2, \ldots, s_n$, *função que terá os coeficientes inteiros, se o mesmo acontecer a respeito de* $\varphi(z_1, z_2, \ldots, z_n)$.

Como exemplo, consideremos a função simétrica

$$U = (z_1 z_2 + z_3 z_4)(z_1 z_3 + z_2 z_4)(z_1 z_4 + z_2 z_3).$$

Reduzindo esta função à forma de polinómio, virá:

$$U = \sum z_1^3 z_2 z_3 z_4 + \sum z_1^2 z_3^2 z_4^2,$$

em que os somatórios se supõem extendidos a todos os termos que se deduzem dos termos escritos, efectuando sobre os índices as substituições de S_4. O primeiro termo de U é, manifestamente,

$$z_1^3\, z_2\, z_3\, z_4 \quad (\alpha_1 = 3,\ \alpha_2 = \alpha_3 = \alpha_4 = 1).$$

Ponhamos então

$$\begin{aligned} P &= s_1^{3-1}\, s_2^{1-1}\, s_3^{1-1}\, s_4^{1} = s_1^2\, s_4 \\ &= (z_1 + z_2 + z_3 + z_4)^2\, z_1\, z_2\, z_3\, z_4 . \end{aligned}$$

Ter-se-á, efectuando os cálculos:

$$U_1 = U - P = \sum z_1^2\, z_2^2\, z_3^2 - 2 \sum z_1^2\, z_2^2 z_3\, z_4 .$$

O primeiro termo de U_1 é

$$z_1^2\, z_2^2\, z_3^2 \quad (\alpha_1 = \alpha_2 = \alpha_3 = 2,\ \alpha_4 = 0).$$

Ponhamos

$$P_1 = s_1^{2-2}\, s_2^{2-2}\, s_3^2\, s_4^0 = s_3^2 .$$

Virá

$$U_2 = U_1 - P_1 = -\,4 \sum z_1^2\, z_2^2\, z_3\, z_4 .$$

Ponhamos agora

$$P_2 = -\,4\, s_2\, s_4 .$$

Virá, finalmente

$$U_2 - P_2 = 0,$$

e assim poderemos escrever

$$U = P + P_1 + P_2 = s_1^2\, s_4 + s_3^2 - 4\, s_2\, s_4 .$$

Dada uma equação algébrica $f(z)=0$ de raízes $z_1, z_2, \ldots, z_n$, chama-se *discriminante* D dessa equação o quadrado do determinante de VANDERMONDE em $z_1, z_2, \ldots, z_n$:

$$D = V^2 = \prod_{i>k}^{n} (z_i - z_k)^2 .$$

Imediatamente se reconhece que D é uma função simétrica de $z_1, z_2, \ldots, z_n$ (o que já não se pode dizer de V, que pertence ao grupo alternante, A_n).

Para a equação do segundo grau

$$z^2 + bz + c = 0 ,$$

tem-se

$$D = (z_2 - z_1)^2 = s_1^2 - 4 s_2 = b^2 - 4c .$$

Para a equação do 3.º grau

$$z^3 + bz^2 + cz + d = 0 ,$$

tem-se, pelo método das funções simétricas,

$$\begin{aligned} D &= (z_3 - z_2)^2 (z_3 - z_1)^2 (z_2 - z_1)^2 \\ &= 18\, bcd - 4b^3 d + b^2 c^2 - 4c^3 - 27d^2 . \end{aligned}$$

É fácil ver que: *condição necessária e suficiente para que uma equação algébrica tenha raízes múltiplas é que o seu discriminante seja nulo*. Aqui a origem do termo "*discriminante*".

O teorema das funções simétricas pode ser estabelecido com maior generalidade:

Toda a função simétrica racional (com coeficientes racionais) de $z_1, z_2, \ldots, z_n$ pode exprimir-se como função racional (com coeficientes racionais) das funções simétricas elementares de $z_1, z_2, \ldots, z_n$.

Seja com efeito $u = \varphi(z_1, z_2, \ldots, z_n)$ uma função simétrica racional de $z_1, z_2, \ldots, z_n$. Visto que se trata duma função racional, podemos escrever

$$u = \frac{v}{w},$$

sendo v, w duas funções racionais inteiras em $z_1, z_2, \ldots, z_n$. Representando por $v_1 (= v), v_2, \ldots, v_m$, as funções que se obtém a partir de v efectuando todas as possíveis substituições sobre as variáveis (funções conjugadas de v), e por $w_1 (= w), w_2, \ldots, w_m$ as funções correspondentes obtidas a partir de w, virá, atendendo a que φ é simétrica

$$u = \frac{v_1}{w_1} = \frac{v_2}{w_2} = \cdots = \frac{v_m}{w_m},$$

donde

$$v_1 = u\, w_1, \quad v_2 = u\, w_2, \ldots, \quad v_m = u\, w_m,$$

e portanto

$$v_1 + v_2 + \cdots + v_m = u(w_1 + w_2 + \cdots + w_m),$$

ou seja

$$u = \frac{v_1 + v_2 + \cdots + v_m}{w_1 + w_2 + \cdots + w_m}.$$

Mas $v_1 + v_2 + \cdots + v_m$ é, manifestamente, uma função simétrica de $z_1, z_2, \ldots, z_n$ e, portanto, racionalmente exprimível em $s_1, s_2, \ldots, s_n$; outro tanto se diga a respeito de $w_1 + w_2 + \cdots + w_m$. Fica portanto provado, como pretendiamos, que a função u é racionalmente exprimível nas funções simétricas elementares de $z_1, z_2, \ldots, z_n$. Observe-se ainda, como complemento, que, se os coeficientes da função $u = \varphi(z_1, z_2, \ldots, z_n)$ forem racionais, serão também racionais os coeficientes da função racional que exprime u mediante $s_1, s_2, \ldots, s_n$.

29. Equações resolventes. Transformações de TSCHIRNHAUS

Seja ainda $f(z) = 0$ uma equação algébrica de raízes $z_1, z_2, \dots, z_n$, e seja $u = \varphi(z_1, z_2, \dots, z_n)$ uma qualquer função racional de $z_1, z_2, \dots, z_n$. Representando por $u_1 (= u)$, $u_2, \dots, u_m$ as funções conjugadas de u, podemos afirmar que *toda a função $R(u_1, u_2, \dots, u_m)$ racional e simétrica em $u_1, u_2, \dots, u_m$ será ainda, por intermédio destas variáveis, uma função racional e simétrica de $z_1, z_2, \dots, z_n$*. Com efeito, visto que $u_1, u_2, \dots, u_m$ são as funções conjugadas de u, toda a substituição sobre os zz se traduz numa substituição sobre os uu, o que não altera, evidentemente, o valor da função $R(u_1, u_2, \dots, u_m)$, suposta simétrica em $u_1, u_2, \dots, u_m$.

Posto isto, consideremos a equação cujas raízes são, precisamente, $u_1, u_2, \dots, u_m$; isto é, a equação

$$g(z) \equiv (z - u_1)(z - u_2) \cdots (z - u_m) = 0.$$

Pondo $\qquad S_1 = \sum u_1,\ S_2 = \sum u_1 u_2,\ \dots,\ S_m = u_1 u_2 \cdots u_m,$

podemos escrever

$$g(z) \equiv z^m - S_1 z^{m-1} + S_2 z^{m-2} - \cdots + (-1)^m S_m = 0.$$

Ora, visto que $S_1, S_2, \dots, S_m$ são funções simétricas racionais dos uu, serão também, pelo que foi dito há pouco, funções simétricas racionais dos zz, e portanto racionalmente exprimíveis nos coeficientes da equação $f(z) = 0$.

A resolução de uma tal equação $g(z) = 0$ pode, por vezes, facilitar a resolução da proposta, $f(z) = 0$. Deste ponto de vista, a equação $g(z) = 0$ dir-se-à uma *resolvente* da equação, $f(z) = 0$.

Seja, por exemplo, a equação do 4.° grau

$$z^4 + bz^3 + cz^2 + dz + e = 0,$$

cujas raízes designaremos por z_1, z_2, z_3, z_4. Propunhamo-nos construir a equação que tem por raízes as conjugadas da função $u = z_1 z_2 + z_3 z_4$. Ora as conjugadas de u são:

$$u_1 (= u), \quad u_2 = z_1 z_3 + z_2 z_4, \quad \mathrm{u}_3 = z_1 z_4 + z_2 z_3.$$

Virá então:

$$S_1 = \sum u_1 = \sum z_1 z_2 = c;$$

$$S_2 = \sum u_1 u_2 = \sum z_1 z_2 z_3 = s_1 s_3 - 4 s_4 = bd - 4e.$$

Quanto a S_4, já o seu valor foi calculado como exemplo no número precedente:

$$S_4 = b^2 e + d^2 - 4ce.$$

A equação procurada será pois:

$$\rho(u) \equiv u^3 - cu^2 + (bd - 4e)u + 4ce - b^2 e + d^2 = 0$$

chamada a resolvente de FERRARI da proposta.

Suponhamos que se calculou uma raiz desta equação; é claro que podemos supor escolhidas as notações z_1, z_2, z_3, z_4, de modo que essa raiz seja precisamente $u_1 = z_1 z_2 + z_3 z_4$. Podemos então determinar o produto $z_1 z_2$ (ou o produto $z_3 z_4$) mediante uma equação do 2.° grau; tem-se, com efeito,

$$z_1 z_2 z_3 z_4 = e$$

donde

$$z_1 z_2 + z_3 z_4 = z_1 z_2 + \frac{e}{z_1 z_2} = u_1,$$

ou seja

$$(z_1 z_2)^2 - u_1 (z_1 z_2) + e = 0,$$

equação do 2.° grau em $z_1 z_2$, de coeficientes conhecidos. Uma qualquer das raízes desta equação pode ser tomada como valor de $z_1 z_2$ e a outra, portanto, como valor de $z_3 z_4$. Uma vez determinado o produto $z_1 z_2$, a soma $z_1 + z_2$ determina-se imediatamente por via racional, atendendo a que é

$$z_1 z_2 (z_3 + z_4) + z_3 z_4 (z_1 + z_2) = \sum z_1 z_2 z_3 = -d,$$

ou seja (visto que $z_1 + z_2 + z_3 + z_4 = -b$):

$$z_1 z_2 [-b-(z_1+z_2)] - \frac{e}{z_1 z_2}(z_1+z_2) = -d,$$

equação do primeiro grau em $z_1 + z_2$, de coeficientes já conhecidos. Calculados os valores $z_1 z_2$ e $z_1 + z_2$, a determinação das raízes z_1, z_2 reduz-se à resolução duma equação do segundo grau. Analogamente se determinam z_3, z_4. (É de notar como a escolha das notações z_1, z_2, z_3, z_4 vai sendo feita gradualmente, *à posteriori*).

Tornemos a considerar a equação de grau n qualquer, $f(z)=0$. Uma função racional $u = \varphi(z_1, z_2, \ldots, z_n)$ das n raízes desta equação pode, em particular, reduzir-se à função racional duma só raiz (por exemplo, de z_1) deixando as outras variáveis de figurar explicitadamente na expressão de u. Mais precisamente, pode acontecer que se tenha

$$\varphi(z_1, z_2, \ldots, z_n) \equiv R(z_1),$$

sendo R o símbolo duma função racional.

Neste caso, as funções conjugadas de $\varphi(z_1, z_2, \ldots, z_n)$ serão, manifestamente

$$u_1 = R(z_1),\ u_2 = R(z_2), \ldots,\ u_n = R(z_n).$$

Por isso, a equação

$$g(u) \equiv (u-u_1)(u-u_2)\cdots(u-u_n) = 0$$

terá o mesmo grau da proposta, $f(z)=0$, com a qual está relacionada por meio da fórmula de transformação $u = R(z)$. Diz-se então que $g(u)=0$ é uma *transformada de TSCHIRNHAUS* de $f(z)=0$.

Um caso particular das transformações de TSCHIRNHAUS é a *transformação homográfica*

$$u = \frac{az+b}{cz+d}$$

(com $ad \neq bc$), estudada nos cursos clássicos de Álgebra Superior.

Como exemplo, propunhamo-nos construir a equação que tem por raízes os quadrados das raízes da equação do terceiro grau

$$z^3 + bz^2 + cz + d = 0 .$$

Trata-se de efectuar a transformação $u = z^2$ sobre a equação dada. As raízes da equação procurada serão, neste caso, z_1^2, z_2^2, z_3^3. Ora

$$\sum z_1^2 = s_1^2 - 2s_2 = b^2 - 2c ,$$

$$\sum z_1^2 z_2^2 = s_2^2 - 2s_1 s_3 = c^2 - 2bd ,$$

$$z_1^2 z_2^2 z_3^2 = d^2 .$$

A equação transformada será pois

$$u^3 - (b^2 - 2c)\, u^2 + (c^2 - 2bd)\, u - d^2 = 0 .$$

30. Teorema de LAGRANGE

Seja $u = \varphi(z_1, z_2, \ldots, z_n)$ uma função racional de $z_1, z_2, \ldots, z_n$, pertencente a um grupo G de substituições sobre as variáveis independentes, e seja $v = \psi(z_1, z_2, \ldots, z_n)$ uma outra função racional de $z_1, z_2, \ldots, z_n$, a qual resulte invariante para todas as substituições do grupo G. Note-se bem: não se exclui a possibilidade de a função ψ ser invariante para outras substituições, além das que pertencem a G. Representando por G' o grupo a que pertence ψ, a nossa hipótese consiste apenas em supor $G' \supset G$, podendo ou não ser $G' = G$.

Ora bem, um teorema de LAGRANGE garante-nos *que, em tais condições, v é exprimível como função racional de u e das funções simétricas elementares de $z_1, z_2, \ldots, z_n$.*

Mais precisamente, nós podemos afirmar que, *se for m o número dos conjugados de φ, poderá escrever-se v sob a forma dum polinómio inteiro em u*

$$v = c_1 u^{m-1} + c_2 u^{m-2} + \cdots + c_{m-1} u + c_m ,$$

de grau inferior a m, e cujos coeficientes $c_1, c_2, \ldots, c_m$ são funções simétricas de $z_1, z_2, \ldots, z_n$.

Para demonstrar este facto, designemos por $u_1 (= u), u_2, \dots, u_m$ as funções conjugadas de u, e por $v_1 (= v), v_2, \dots, v_m$, as funções correspondentes que se obtém a partir de v. Visto que o grupo G' da função $v = \varphi(z_1, z_2, \dots, z_n)$ não coincide necessariamente com G, pode acontecer que as funções $v_1, v_2, \dots, v_m$ não sejam todas distintas; mas tal não prejudica em nada a marcha dos raciocínios que vamos desenvolver. (Como se tem $G' \supset G$, é claro que toda a classe lateral $\theta G'$ de G' em S_n, conterá a classe lateral θG de G em S_n).

Posto isto, procuremos determinar os coeficientes $c_1, c_2, \dots, c_m$, por meio das condições

$$(6) \qquad \begin{cases} v_1 = c_1 u_1^{m-1} + c_2 u_1^{m-2} + \cdots + c_{m-1} u_1 + c_m, \\ v_2 = c_1 u_2^{m-1} + c_2 u_2^{m-2} + \cdots + c_{m-1} u_2 + c_m, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ v_m = c_1 u_m^{m-1} + c_2 u_m^{m-2} + \cdots + c_{m-1} u_m + c_m. \end{cases}$$

Ora, temos aqui um sistema de equações lineares em $c_1, c_2, \dots, c_m$, cujo determinante, Δ, é (àparte o sinal) o determinante de VANDERMONDE em $u_1, u_2, \dots, u_m$:

$$\Delta = \begin{vmatrix} u_1^{m-1} & u_1^{m-2} & \cdots & u_1 & 1 \\ u_2^{m-1} & u_2^{m-2} & \cdots & u_2 & 1 \\ \dots & \dots & \dots & \dots & \dots \\ u_m^{m-1} & u_m^{m-2} & \cdots & u_m & 1 \end{vmatrix} = \prod_{i<k}^{n} (u_i - u_k).$$

Condição necessária e suficiente para que tal sistema seja possível e determinado é, como se sabe, que $\Delta \neq 0$. Para que Δ fosse *identicamente* nulo (isto é, nulo para todos os sistemas de valores possíveis das variáveis $z_1, z_2, \dots, z_n$), seria necessário que duas, pelo menos, das funções $u_1, u_2, \dots, u_m$ fossem idênticas. Mas, por hipótese, as funções $u_1, u_2, \dots, u_m$ são todas distintas (funções conjugadas de u_1). Logo, o sistema é, em geral, possível e determinado: podemos, portanto, aplicando a regra de CRAMER, determinar $c_1, c_2, \dots, c_m$ em *função racional* de $u_1, u_2, \dots, u_m, v_1, v_2, \dots, v_m$, e portanto em *função racional* de $z_1, z_2, \dots, z_n$. É contudo necessário não perder de vista que a fórmula

$$v = c_1 u^{m-1} + c_2 u^{m-2} + \cdots + c_m$$

só será válida para aqueles sistemas de valores numéricos de $z_1, z_2, \ldots, z_n$ *que tornem distintos entre si os valores numéricos das* m *funções* $u_1, u_2, \ldots, u_m$ *– pois que, de contrário, resultará nulo o determinante* Δ.

Resta-nos provar que os coeficientes $c_1, c_2, \ldots, c_m$ são funções simétricas de $z_1, z_2, \ldots, z_n$. Para isso, basta observar que *toda a substituição* $\theta_{i,k}$ *sobre os zz que faça passar de* u_i para u_k *é também uma das que convertem* v_i *em* v_k. Com efeito, designando por θ_i, θ_k duas substituições que façam passar, respectivamente, de u_1 para u_i e de u_1 para u_k, ter-se-á

$$\theta_{i,k} = \theta_k \sigma \theta_i^{-1}, \quad \text{com } \sigma \in G;$$

mas θ_i^{-1} converte v_i em v_1, σ deixa v_1 invariante e θ_k converte v_1 em v_k – logo $\theta_{i,k}$ faz passar de v_i para v_k, como tinhamos afirmado.

Vê-se portanto que o efeito de uma qualquer substituição sobre os *zz* consiste, quando muito, em alterar a ordem das equações (6), o que, evidentemente, não influi na solução do sistema. Os coeficientes $c_1, c_2, \ldots, c_m$ são, por conseguinte, funções simétricas racionais de $z_1, z_2, \ldots, z_n$ e, como tais, racionalmente exprimíveis nas funções simétricas elementares de $z_1, z_2, \ldots, z_n$, mas que se podem reduzir a tais, dividindo-os pela função

$$V = \prod_{i>k}^{n} (z_i - z_k).$$

Como exemplo de aplicação, consideremos o seguinte problema: *Conhecido o produto de duas raízes da equação*

$$z^3 + bz^2 + cz + d = 0,$$

determinar, por meio de operações racionais, a soma das mesmas raízes. É visível que as duas funções

$$\varphi(z_1, z_2, z_3) \equiv z_1 z_2, \quad \psi(z_1, z_2, z_3) \equiv z_1 + z_2,$$

pertencem ao mesmo grupo: o subgrupo de S_3 constituído pelas substituições I, (1 2). Aplicando o processo indicado, virá então

$$\begin{cases} z_1 + z_2 = c_1 (z_1 z_2)^2 + c_2 (z_1 z_2) + c_3 \\ z_1 + z_3 = c_3 (z_1 z_3)^2 + c_2 (z_1 z_3) + c_3 \\ z_2 + z_3 = c_1 (z_2 z_3)^2 + c_2 (z_2 z_3) + c_3 \end{cases}$$

donde

$$c_1 = - \frac{(z_1^2 - z_2^2) z_3 - (z_1^2 - z_3^2) z_2 + (z_2^2 - z_3^2) z_1}{(z_1 z_2 - z_1 z_3)(z_1 z_2 - z_2 z_3)(z_1 z_3 - z_2 z_3)} =$$

$$= - \frac{(z_1 - z_2)(z_1 - z_3)(z_2 - z_3)}{z_1 z_2 z_3 (z_1 - z_2)(z_1 - z_3)(z_2 - z_3)} = \frac{1}{d},$$

e, analogamente,

$$c_2 = - \frac{c}{d}, \quad c_3 = 0.$$

O polinómio procurado será portanto

$$v = \frac{u^2 - cu}{d}.$$

Note-se que se podia chegar mais rapidamente a este resultado, por considerações elementares. Se apresentamos aqui este exemplo, é apenas com o objectivo de ilustrar a anterior demonstração de caracter geral.

31. Consequências do Teorema de LAGRANGE

Dada uma função racional $u = \varphi(z_1, z_2, \ldots, z_n)$, pode acontecer que todas as conjugadas de u pertençam a um mesmo grupo. Já sabemos que tal acontece, se, e só se, o grupo G a que pertence φ é um subgrupo *invariante* de S_n. Nesta hipótese, é claro que, segundo o teorema de LAGRANGE, dadas duas quaisquer funções, u_i, u_k, será possível exprimir u_i em u_k mediante um polinómio

$$u_i = c_1 u_k^{m-1} + c_2 u_k^{m-2} + \cdots + c_{m-1} u_k + c_m ,$$

de coeficientes $c_1, c_2, \ldots, c_m$ racionalmente exprimíveis nas funções simétricas elementares de $z_1, z_2, \ldots, z_n$.

Uma outra consequência imediata do teorema de LAGRANGE é esta:

Toda a função racional $Z = \Phi(z_1, z_2, \ldots, z_n)$ *pertencente ao grupo alternante* A_n *é susceptível da representação*

$$Z = M + N\,V,$$

em que M, N representam funções simétricas de $z_1, z_2, \ldots, z_n$ *e em que*

$$V = \prod_{i>k}^{n} (z_i - z_k).$$

Com efeito, a função V (pertencente por definição ao grupo A_n) admite apenas duas conjugadas: V e $-V$. Designando por Z e Z' as conjugadas de Z, tem-se, como é fácil reconhecer

$$M = \frac{1}{2}(Z + Z')\,, \quad N = \frac{1}{2}(Z - Z')/V.$$

Em particular, se $M = 0$, será $Z' = -Z$, e a função Z dir-se-á *hemisimétrica* (tal como V).

Consideremos agora o caso das funções pertencentes ao grupo $\mathscr{T}$. Tal é, por exemplo, toda a função u da forma

$$u = a_1 z_1 + a_2 z_2 + \cdots + a_n z_n ,$$

sendo $a_1, a_2, \ldots, a_n$ constantes numéricas todas distintas entre si. (Qualquer substituição distinta de I altera esta função; o número das suas conjugadas é pois $n!$ – índice de $\mathscr{T}$ em S_n).

Visto que toda a função de $z_1, z_2, \ldots, z_n$ se mantém invariante para a substituição I, segue-se, pelo teorema de LAGRANGE, *que toda a função racional de* $z_1, z_2, \ldots, z_n$ *é racionalmente exprimível numa qualquer função pertencente ao grupo idêntico e nas funções simétricas elementares de* $z_1, z_2, \ldots, z_n$.

Em particular, as funções racionais $u = \varphi(z_1, z_2, \dots, z_n)$ e $v = \psi(z_1, z_2, \dots, z_n)$ podem reduzir-se a funções duma só variável:

$$\varphi(z_1, z_2, \dots, z_n) \equiv \Phi(z_1), \quad \psi(z_1, z_2, \dots, z_n) \equiv \Psi(z_1).$$

Pode mesmo acontecer que se tenha

$$\Phi(z_1) \equiv z_1 .$$

Neste caso, as conjugadas de $u = \Phi(z_1)$ serão $z_1, z_2, \dots, z_n$ e as de $v = \Psi(z_1)$, serão $\Psi(z_1), \Psi(z_2), \dots, \Psi(z_n)$.

Ora, se for $f(z) = 0$ uma equação algébrica de raízes $a_1, a_2, \dots, a_n$, ter-se-á, segundo o teorema demonstrado

$$\Psi(\alpha_i) = c_1 \alpha_i^{n-1} + c_2 \alpha_i^{n-2} + \cdots + c_{n-1} \alpha_i + c_n$$

$(i = 1, 2, \dots, n)$, sendo $c_1, c_2, \dots, c_n$ racionalmente exprimíveis nos coeficientes de $f(z) = 0$.

Note-se bem: $\Psi(z)$ é uma função racional *qualquer* de z, portanto da forma

$$\Psi(z) \equiv \frac{N(z)}{D(z)}, \tag{7}$$

em que $N(z)$, $D(z)$ designam polinómios inteiros em z, de grau *qualquer.* Ora, como acabamos de ver, o valor de $\Psi(z)$ para $z = \alpha_i$, sendo α_i uma raiz qualquer da equação $f(z) = 0$, pode sempre ser dado mediante um polinómio inteiro em z:

$$P(z) \equiv c_1 z^{n-1} + c_2 z^{n-2} + \cdots + c_{n-1} z + c_n ,$$

de grau inferior a n.

(Impõe-se naturalmente a restricção de $\Psi(z)$ não se tornar infinita para nenhum dos valores $\alpha_1, \alpha_2, \dots, \alpha_n$).

Este facto pode ser estabelecido mesmo directamente:

Seja $\Psi(z)$ uma função da forma (7). Começaremos por mostrar que, para $z = \alpha_i$, é possível substituir os polinómios $N(z)$, $D(z)$, por dois polinómios $\upsilon(z)$, $\delta(z)$, de grau inferior a n. Tem-se, com efeito, representando por $q(z)$ e $\upsilon(z)$, respectivamente, o cociente e o resto da divisão de $N(z)$ por $f(z)$:

$$N(z) \equiv q(z) \cdot f(z) + \upsilon(z),$$

donde, atendendo a que $f(\alpha_i) = 0$:

$$N(\alpha_i) = \upsilon(\alpha_i) \qquad (i = 1, 2, \ldots, n),$$

sendo o grau de $\upsilon(z)$ inferior ao de $f(z)$ o portanto inferior a n, de acordo com o que tinhamos dito. Analogamente para $D(z)$.

Posto isto, podemos provar que, na fracção algébrica,

$$\frac{\upsilon(z)}{\delta(z)}$$

o denominador $\delta(z)$ pode ser substituído (para $z = \alpha_i$) por um polinómio $\delta_1(z)$ do grau inferior ao de $\delta(z)$. Tem-se, com efeito, representando por $q_1(z)$ e $\delta_1(z)$, respectivamente, o cociente e o resto da divisão de $f(z)$ por $\delta(z)$

$$\frac{f(z)}{\delta(z)} \equiv q_1(z) + \frac{\delta_1(z)}{\delta(z)},$$

donde, supondo que $f(z)$ e $\delta(z)$ não têm raízes comuns:

$$0 = q_1(\alpha_i) + \frac{\delta_1(\alpha_i)}{\delta(\alpha_i)} \quad (i = 1, 2, \ldots, n),$$

o que dá

$$\frac{\upsilon(\alpha_i)}{\delta(\alpha_i)} = -\frac{\upsilon(\alpha_i) \cdot q_1(\alpha_i)}{\delta_1(\alpha_i)} \quad (i = 1, 2, \ldots, n),$$

sendo o grau de $\delta_1(z)$ inferior ao de $\delta(z)$, por ser o resto da divisão de $f(z)$ por $\delta(z)$.

E assim, abaixando sucessivamente o grau do denominador, acabaremos por reduzi-lo a uma constante ficando deste modo a função racional $\Psi(z)$ substituída por um polinómio inteiro em z, cujo grau podemos tornar inferior a n, conforme o que dissemos.

Exemplos:

a) Seja a equação do segundo grau $x^2 - 5 = 0$, cujas raízes costumam ser designadas pelos símbolos $\sqrt{5}$, $-\sqrt{5}$. Qualquer que seja a função racional $\Phi(x)$, cociente de 2 polinómios $p(x)$, $q(x)$ de coeficientes racionais (com $q(\sqrt{5}) \neq 0$), será sempre possível determinar dois números racionais *a, b,* tais que

$$\frac{p(\sqrt{5})}{q(\sqrt{5})} = a + b\sqrt{5}.$$

Este facto pode ser estabelecido mesmo elementarmente, atendendo a que é $(\sqrt{5})^m = 5^p$ ou $(\sqrt{5})^m = 5^p\sqrt{5}$ (com p inteiro), consoante m é par ou ímpar; e recordando, por outro lado, o conhecido processo de racionalização de denominadores.

b) Toda a expressão do tipo $\Phi(\sqrt{-1})$, sendo Φ um símbolo de função racional de coeficientes racionais e $\sqrt{-1}$ uma qualquer das raízes da equação $z^2 + 1 = 0$, pode reduzir-se à forma $a + b\sqrt{-1}$ (ou $a + bi$, pondo $i = \sqrt{-1}$), com *a, b* racionais.

c) Seja agora a equação do terceiro grau $z^3 - 2 = 0$. Representando uma qualquer das raízes desta equação por $\sqrt[3]{2}$, é claro que toda a expressão do tipo $\Phi(\sqrt[3]{2})$, sendo ainda Φ símbolo de função racional de coeficientes racionais, pode reduzir-se à forma

$$a(\sqrt[3]{2})^2 + b\sqrt[3]{2} + c,$$

com *a, b, c* racionais. É recomendável verificar como, aplicando o anterior processo, se consegue efectuar neste caso a racionalização de denominadores.

32. Generalização do teorema de LAGRANGE

O teorema de LAGRANGE pode ser generalizado do seguinte modo:

Sejam $u = \varphi(z_1, z_2, \ldots, z_n)$, $v = \Phi(z_1, z_2, \ldots, z_n)$ duas funções racionais de $z_1, z_2, \ldots, z_n$, cujos grupos representaremos respectivamente por G, G', e seja $w = \chi(z_1, z_2, \ldots, z_n)$ uma terceira função racional de $z_1, z_2, \ldots, z_n$, que fique invariante para todas as substituições comuns a G e G', isto é, cujo grupo H contenha $G \cap G'$. *Em tais condições, podemos afirmar que w é exprimível como função racional de u, de v e das funções simétricas elementares de $z_1, z_2, \ldots, z_n$; mais precisamente, podemos afirmar que w é susceptível da representação*:

$$w = c_1 v^{m-1} + c_2 v^{m-2} + \cdots + c_{m-1} v + c_m,$$

sendo m o número das conjugadas de v em G e $c_1, c_2, \ldots, c_m$ funções racionais de u e das referidas funções simétricas elementares.

Sejam, com efeito, $v_1 (= v)$, $v_2, \ldots, v_m$ as funções conjugadas de v em G (note-se bem: em G não em S_n) e sejam $w_1 (= w)$, $w_2, \ldots, w_m$ as funções correspondentes obtidas a partir de w. Consideremos então o seguinte sistema de equações lineares em $c_1, c_2, \ldots, c_m$:

$$(8) \qquad w_i = c_1 v_i^{m-1} + c_2 v_i^{m-2} + \cdots + c_{m-1} v_i + c_m \quad (i = 1, 2, \ldots, m).$$

Discorrendo como no número precedente, chega-se à conclusão de que este sistema é possível e determinado, desde que se evitem os valores numéricos de $z_1, z_2, \ldots, z_n$ que tornam iguais os valores de duas quaisquer das funções $v_1, v_2, \ldots, v_m$. Tal sistema permite pois, em geral, determinar os coeficientes $c_1, c_2, \ldots, c_m$, em função racional dos vv e dos ww, e portanto em função racional dos zz.

Seja agora θ uma substituição qualquer do grupo G. Já sabemos (n.° 26) que a substituição θ, efectuada sobre os zz, se traduz numa substituição $\overline{\theta}$ sobre os vv. Podemos portanto concluir, por um raciocínio análogo ao do número precedente, que o efeito de uma tal substituição θ consistirá, quando muito, numa alteração da ordem das equações (8), o que, obviamente, não influe na solução do sistema. Por outras palavras: os coeficientes $c_1, c_2, \ldots, c_m$ são funções racionais de $z_1, z_2, \ldots, z_n$, que se mantêm invariantes para todas as substituições de G, *grupo a que pertence a função u.* Então, segundo o teorema de LAGRANGE, os coeficientes $c_1, c_2, \ldots, c_n$, poderão exprimir-se racionalmente em u e nas funções simétricas elementares de $z_1, z_2, \ldots, z_n$, q.e.d.

33. Noção de corpo numérico

É evidente que, efectuando operações racionais (adições, subtracções, multiplicações e divisões) a partir de números racionais, os resultados obtidos serão ainda, necessariamente, números racionais. Mais precisamente: representando por **Ra** o conjunto dos números racionais, tem-se que a soma, a diferença, o produto e o cociente de dois quaisquer elementos de **Ra** (sendo o divisor diferente de 0) é ainda elemento de **Ra**. Exprime-se este facto dizendo que o conjunto **Ra** é *racionalmente fechado* ou *fechado a respeito das operações racionais.*

Mas tal propriedade não é exclusiva do conjunto **Ra**: também o conjunto **R**, dos números reais, e o conjunto **K**, dos números complexos (para não citar outros) são racionalmente fechados, como imediatamente se reconhece. Mas já, por exemplo, o conjunto **P**, dos números positivos, não é racionalmente fechado, visto que a diferença de dois elementos de **P** pode não pertencer a **P**.

Costuma chamar-se *corpo* ou *domínio de racionalidade* todo o conjunto de números racionalmente fechado e constituído por mais de um elemento.

Corpo numérico é pois todo o conjunto Ω de números, dotado dos seguintes caracteres: 1) tem mais de um elemento; 2) dados dois quaisquer elementos a, b de Ω, também $a+b$, $a-b$, ab, a/b (supondo neste último caso $b \neq 0$) são elementos de Ω.

Esta definição pode ainda ser simplificada: *Para que um conjunto Ω, constituído por vários números, seja um corpo, é necessário e suficiente que, dados dois elementos a, b quaisquer de Ω, se tenha sempre $a-b \in \Omega$, $a/b \in \Omega$ (sendo $b \neq 0$).* Com efeito, uma vez verificadas estas condições, tem-se representando por c um elemento não nulo de Ω:

$$0 = c - c \in \Omega\,, \quad 1 = c/c \in \Omega\,.$$

Então, dados dois elementos a, b quaisquer de Ω (com $b \neq 0$) tem-se que $0 - b$ e $1/b$ também serão elementos de Ω e, portanto, visto que $a + b = a + (-b)$, $a \cdot b = a : (1/b)$, também $a + b$ e $a \cdot b$ pertencerão a Ω.

Observemos agora que o *mínimo corpo numérico existente é o corpo racional*, **Ra**. Com efeito, qualquer outro corpo numérico contém **Ra**, pois que, contendo 1, conterá todo o número natural $m = 1 + 1 + \cdots + 1$ (m vezes) e portanto o cociente m/n de todo o par de números naturais (com $n \neq 0$), bem como o simétrico $-m/n$.

Um exemplo não trivial de corpo é o conjunto de todos os números da forma $a + b\sqrt{2}$, com a, b racionais. A diferença ou o cociente de dois números desta forma é ainda, manifestamente, um número da mesma forma.

É fácil demonstrar que *a intersecção de dois ou mais corpos (em número qualquer, finito ou infinito) é ainda um corpo*. Com efeito, dados vários corpos Ω_i, se forem a, b dois números pertencentes à intersecção $\bigcap_i \Omega_i$, a diferença a-b deverá pertencer a cada um desses corpos Ω_i e portanto à intersecção de todos eles, e o mesmo acontecerá a respeito do cociente a/b (supondo $b \neq 0$).

Posto isto, seja M um conjunto *qualquer* de números. Haverá pelo menos um corpo numérico que contém M: o corpo complexo, **K**. Ora, a intersecção de todos os corpos que contêm M será ainda, em virtude do resultado precedente, um corpo que contém M: designemo-lo por Ω. É claro que Ω será o *mínimo* corpo que contém M: diz-se então que Ω é o corpo *gerado* por M (ou pelos elementos de M). Observemos ainda que Ω *é o conjunto de todos os números que se obtêm por meio de operações racionais efectuadas um número finito de vezes sobre elementos de M ou sobre os resultados de tais operações.*

Consideremos agora um corpo numérico Δ e um número α, qualquer. (Se $\alpha \notin \Delta$, a reunião Δ com α não será um corpo). Representa-se por $\Delta(\alpha)$ o corpo gerado por α e pelos elementos de Δ, e diz-se que $\Delta(\alpha)$ resulta da *adjunção* do número α ao corpo Δ. No caso de Δ coincidir com o corpo racional, é claro que $\Delta(\alpha)$ poderá ser gerado unicamente por α.

Analogamente, chama-se corpo resultante da *adjunção* de vários números $\alpha_1, \alpha_2, \ldots, \alpha_n$ a um corpo Δ, e representa-se por $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$, o corpo gerado por esses números e pelos elementos de Δ. É claro que o corpo $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$ pode ainda ser obtido pela adjunção sucessiva dos números $\alpha_1, \alpha_2, \ldots, \alpha_n$ a Δ, em qualquer ordem.

Exemplos:

Efectuando a adjunção de $\sqrt{2}$ ao corpo racional, **Ra**, obtém-se o corpo $\mathbf{Ra}(\sqrt{2})$, constituído por todos os números da forma $a+b\sqrt{2}$ com *a, b* racionais. Designemos por Δ este corpo; fazendo a adjunção de $\sqrt[3]{5}$ a Δ, obtém-se o corpo $\Delta(\sqrt[3]{5})$, constituído por todos os números da forma $a + b\sqrt[3]{5} + c(\sqrt[3]{5})^2$, com $a, b, c \in \Delta$. Ponhamos ainda $\Omega = \Delta\sqrt[3]{5}$; fazendo a adjunção de log 3 ao corpo Ω, obtém-se o corpo $\Omega(log\ 3)$, constituído por todos os números da forma $\varphi(log\ 3)$, sendo φ uma qualquer função racional de coeficientes em Ω. É claro que

$$\Omega(log\ 5) = \mathbf{Ra}(\sqrt{2}, \sqrt[3]{5}, log\ 3).$$

É ainda de observar que o corpo complexo resulta, precisamente, da adjunção do elemento $i = \sqrt{-1}$ ao corpo real.

Como exercício, recomenda-se a demonstração dos seguintes factos:

1) Para que se tenha $a+b\sqrt{2} = a' + b'\sqrt{2}$, com a, b, a', b' racionais, é necessário e suficiente que $a = b$; $a' = b'$.

2) O número $\sqrt{3}$ não pertence ao corpo $\mathbf{Ra}(\sqrt{2})$.

3) A intersecção de $\mathbf{Ra}(\sqrt{2})$ com $\mathbf{Ra}(\sqrt{3})$ é o corpo **Ra**.

4) Condição necessária e suficiente para que se tenha $a+b\sqrt{3} = = a' + b'\sqrt{3}$, com $a, b, a', b' \in \mathbf{Ra}(\sqrt{2})$ é que resulta $a=a'$, $b=b'$.

34. Funções pertencentes a um grupo em sentido restrito

Até aqui, falando das raízes, $z_1, z_2, \ldots, z_n$, duma equação algébrica de grau *n,* temos tratado tais raízes como variáveis independentes. Todavia, nos casos concretos, dada uma equação algébrica

$$f(z) = a_0 z^n + a_1 z^{n-1} + \cdots + a_n = 0,$$

de coeficientes *numéricos determinados*, as raízes de tal equação (que designaremos agora por $\alpha_1, \alpha_2, \ldots, \alpha_n$) serão *números determinados* e não *variáveis*. Seja $u = \varphi(z_1, z_2, \ldots, z_n)$ uma função racional das *variáveis independentes* $z_1, z_2, \ldots, z_n$ e sejam $u_1(= u), u_2, \ldots, u_m$ as funções conjugadas de u; suponhamos, além disso, que, substituindo $z_1, z_2, \dots, z_n$ pelas raízes $\alpha_1, \alpha_2, \dots, \alpha_n$ da equação considerada, vêm para $u_1, u_2, \dots, u_n$ valores *finitos e determinados*:

$$\beta_1 = \varphi_1(\alpha_1, \alpha_2, \dots, \alpha_n),$$
$$\beta_2 = \varphi_2(\alpha_1, \alpha_2, \dots, \alpha_n), \dots$$
$$\beta_m = \varphi_m(\alpha_1, \alpha_2, \dots, \alpha_n).$$

Por comodidade de linguagem, continuaremos a dizer que β_1 é uma função racional de $\alpha_1, \alpha_2, \dots, \alpha_n$ (muito embora os $\alpha\alpha$ sejam constantes) e que $\beta_1, \beta_2, \dots, \beta_m$ são as *funções conjugadas* de β_1.

Por outro lado, diremos que duas funções das raízes são *formalmente iguais*, quando (e só quando) essas funções resultam idênticas, *abstraindo do valor numérico dos* $\alpha\alpha$, *isto é, tratando mentalmente os símbolos* $\alpha_1, \alpha_2, \dots, \alpha_n$ como *variáveis independentes*.

Ora pode acontecer que duas funções das raízes sejam *formalmente* distintas, sendo *numericamente* iguais.

Seja, por exemplo, a equação recíproca

$$x^4 - 2x^3 - 2x + 1 = 0,$$

cujas raízes designaremos por $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. É claro que podemos supor estas notações já escolhidas de modo que se tenha $\alpha_1 \alpha_2 = 1$, $\alpha_3 \alpha_4 = 1$ (pois que se trata duma equação recíproca). Deste modo, a função das raízes

$$\varphi(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \equiv \alpha_1 \alpha_2$$

ficará *formalmente* invariante para as substituições do grupo $G = \{I, (1\ 2), (3\ 4), (1\ 2)\ (3\ 4)\}$, e só para essas; podemos mesmo dizer que tal função pertence formalmente ao grupo G. Há todavia substituições fora de G que deixam a função $\alpha_1 \alpha_2$ *numericamente* invariante: tal é, por exemplo, a substituição (1 3) (2 4), que muda $\alpha_1 \alpha_2$ em $\alpha_3 \alpha_4$, tendo-se, *numericamente*, $\alpha_1 \alpha_2 = \alpha_3 \alpha_4 = 1$, embora *formalmente* (isto é, pensando os $\alpha\alpha$ como variáveis independentes) se tenha $\alpha_1 \alpha_2 \not\equiv \alpha_3 \alpha_4$. O mesmo acontecerá, de resto, com qualquer função de forma $m\alpha_1 \alpha_2 + n\alpha_3 \alpha_4$, sendo m, n coeficientes numéricos distintos.

Pois bem, tornando ao caso geral, diremos que uma dada função racional $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ das raízes da equação considerada pertence, *em sentido restrito*, a um dado grupo G, quando se verificam as duas seguintes condições: 1) a função $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ pertence *formalmente* ao grupo G; 2) os valores numéricos $\beta_1, \beta_2, \ldots, \beta_m$ das funções conjugadas de φ são todos distintos sobre si.

A necessidade desta convenção faz-se sentir na aplicação do teorema de LAGRANGE. Suponhamos que a função $\beta = \varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ pertence em sentido restrito a um grupo G, e seja $\gamma = \psi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ uma segunda função racional dos $\alpha\alpha$ que fique *formalmente* invariante para todas as substituições de G. Então, segundo o teorema de LAGRANGE, existirão m números $c_1, c_2, \ldots, c_m$, racionalmente exprimíveis nos coeficientes da equação considerada, tais que

$$\gamma = c_1 \beta^m + c_2 \beta^{m-1} + \cdots + c_{m-1} \beta + c_m .$$

Note-se porém que, no caso de φ pertencer ao grupo G apenas formalmente, e não em sentido restrito, não seria lícito chegar a esta conclusão, pois que em tal hipótese, não sendo os números $\beta_1, \beta_2, \ldots, \beta_m$ todos distintos entre si, o determinante de VANDERMONDE em $\beta_1, \beta_2, \ldots, \beta_m$ resultaria nulo (reveja a demonstração do teorema de LAGRANGE).

Assim, por exemplo, tornando ao caso da equação recíproca precedente, não será possível exprimir a soma $\alpha_1 + \alpha_2$ como função racional (com coeficientes racionais) do produto $\alpha_1 \alpha_2$ e dos coeficientes da equação, embora as funções $\alpha_1 + \alpha_2$, $\alpha_1 \alpha_2$ pertençam formalmente ao mesmo grupo. De resto, como é fácil ver, as somas $\alpha_1 + \alpha_2$, $\alpha_3 + \alpha_4$, têm por valores numéricos $1 + \sqrt{3}$, $1 - \sqrt{3}$. (Já no número 29, a propósito de resolventes, vimos como se pode calcular a soma $z_1 + z_2$ de duas raízes de uma equação do quarto grau, uma vez conhecido o produto $z_1 z_2$ dessas raízes; ora, é fácil ver que tal processo é inaplicável, quando se tenha, *numericamente*, $z_1 z_2 = z_3 z_4$).

O que dissemos para o teorema de LAGRANGE estende-se, *tatis mutandis*, à sua generalização.

Posto isto, podemos demonstrar um facto de importância capital para o que segue: *Se as raízes* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *da equação* $f(z) = 0$ *são todas simples, é sempre possível, dado um grupo G qualquer de* *substituições sobre os* $\alpha\alpha$*, construir uma função racional das raízes (com coeficientes racionais) que pertença a G em sentido restrito.*

Suponhamos pois que a equação $f(z)=0$ não admite *raízes múltiplas*. Começaremos por mostrar como se constrói uma função racional dos $\alpha\alpha$ pertencente em sentido restrito ao grupo $\mathscr{T}$. Consideremos o polinómio inteiro em t:

$$p(t) \equiv \alpha_1 + \alpha_2 t + \alpha_3 t^2 + \cdots + \alpha_n t^{n-1}.$$

Efectuando sobre os $\alpha\alpha$ uma substituição $\theta \neq I$, qualquer que ela seja, obtém-se um polinómio distinto de $p(t)$, pois que, por hipótese, os números $\alpha_1, \alpha_2, \ldots, \alpha_n$ são todos diferentes, e, segundo o *princípio das identidades,* dois polinómios são idênticos, se, e só se, tem iguais os coeficientes dos termos do mesmo grau. Sejam então $p_1(=p), p_2, \ldots, p_\upsilon$ todos os polinómios que se obtém a partir de p efectuando sobre os $\alpha\alpha$ todas as possíveis substituições: será então $\upsilon = n!$. Consideremos agora o determinante de VANDERMONDE em $p_1(t), p_2(t), \ldots, p_\upsilon(t)$:

$$V(t) = \prod_{i>k}^{\upsilon} [p_i(t) - p_k(t)].$$

Visto que os polinómios $p_i(t)$ são todos distintos entre si dois a dois, o polinómio $V(t)$, *não será identicamente nulo*, e admitirá portanto um *número finito* de raízes, o que quer dizer que existem *infinitos valores inteiros* de t que não o anulam. Seja t_0 um desses valores; ter-se-á pois

$$V(t_0) \neq 0,$$

o que equivale a dizer que os números $p_1(t_0), p_2(t_0), \ldots, p_\upsilon(t_0)$ são todos distintos. Mas tem-se

$$p(t_0) = \alpha_1 + \alpha_2 t_0 + \alpha_3 t_0^2 + \cdots + \alpha_n t_0^{n-1};$$

logo $p(t_0)$ será uma função racional dos $\alpha\alpha$ (de coeficientes inteiros) que, em virtude de que foi dito, pertence, em sentido restrito ao grupo $\mathscr{T}$.

Ponhamos para brevidade $\pi_i = p_i(t_0)$ $(i = 1, 2, \ldots, \upsilon)$. É claro que $\pi_1, \pi_2, \ldots, \pi_\upsilon$ são as funções conjugadas de π_1 – tantas quantos os elementos de S_n; pois que, dada uma destas conjugadas, π_i, existe *uma, e só uma substituição* θ_i que faz passar de π_1 para π_i.

Seja agora:

$$G = \{I, \sigma_2, \ldots, \sigma_r\}$$

um grupo qualquer de substituições sobre os $\alpha\alpha$, e sejam $\pi_1, \pi_2, \ldots, \pi_r$ as conjugadas de π_1 em G:

$$\begin{aligned} \pi_2 &= I\{\pi_1\}, \\ \pi_2 &= \sigma_2\{\pi_1\}, \ldots, \\ \pi_r &= \sigma_r\{\pi_1\}. \end{aligned}$$

Consideremos o polinómio em λ:

$$P(\lambda) = (\lambda - \pi_1)(\lambda - \pi_2) \cdots (\lambda - \pi_r).$$

Qualquer substituição σ de G (efectuada sobre os $\alpha\alpha$) traduz-se numa substituição sobre os $\pi\pi$ e não altera, portanto, o polinómio $P(\lambda)$. Por outro lado, qualquer substituição θ de S_n, não pertencente a G, altera o polinómio $P(\lambda)$, pois que, em tal hipótese, as funções dos $\alpha\alpha$

$$\theta\{\pi_1\}, \theta\{\pi_2\}, \ldots, \theta\{\pi_r\}$$

são todas distintas (mesmo numericamente) das funções $\pi_1, \pi_2, \ldots, \pi_r$. (Efectuar a substituição θ em $\pi_1, \pi_2, \ldots, \pi_r$ equivale a efectuar directamente em π_1 as substituições da classe lateral θG, de G em S_n). Vê-se, pois que, designando por m o índice de G em S_n, se obtém, a partir de $P(\lambda)$, m polinómios, todos distintos entre si,

$$P_1(\lambda), P_2(\lambda), \ldots, P_m(\lambda),$$

quando sobre os $\alpha\alpha$ se efectuam todas as substituições de S_n. Então, discorrendo como anteriormente para os polinómio $p_i(t)$, chega-se à conclusão de que existe pelo menos um inteiro λ_0, para o qual os números $P_i(\lambda_0)$ são todos distintos. Ponhamos então $\beta = P(\lambda_0)$; ter-se-á

$$\beta = (\lambda_0 - \pi_1)(\lambda_0 - \pi_2) \cdots (\lambda_0 - \pi_r).$$

Em virtude do que foi dito, β será uma função racional dos $\alpha\alpha$, pertencente a G em sentido restrito.

35. Grupo de GALOIS duma equação

Observamos, em primeiro lugar, que, fazendo intervir a noção de corpo numérico, o teorema das funções simétricas é susceptível do seguinte complemento:

Designe Ω um corpo de números e seja $u = \varphi(z_1, z_2, \ldots, z_n)$ uma função racional e simétrica de $z_1, z_2, \ldots, z_n$ com os coeficientes em Ω. Nestas condições, a função racional $F(s_1, s_2, \ldots, s_n)$, que exprime u nas funções simétricas elementares $s_1, s_2, \ldots, s_n$, terá também os coeficientes em Ω.

A demonstração deste complemento é imediata, desde que se examine o processo geral atrás indicado para o cálculo das funções simétricas.

Um complemento análogo pode ser enunciado para o teorema de LAGRANGE, em qualquer das suas formas.

Posto isto, sejam $f(z) = 0$ uma equação algébrica de coeficientes racionais e $\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ uma função racional (com coeficientes racionais) das raízes desta equação. Se a função φ é simétrica, o seu valor numérico não pode deixar de ser racional, pois que, segundo o teorema das funções simétricas, esse valor é racionalmente exprimível nos coeficientes da equação, e estes, por hipótese, são racionais. Suponhamos porém que a função φ não é simétrica: podemos nós concluir daí que o seu valor não é racional? Sabe-se bem que não: basta que as raízes $\alpha_1, \alpha_2, \ldots, \alpha_n$ sejam todas racionais, para que o valor de φ também o seja. Mesmo fora deste caso trivial, pode acontecer, *excepcionalmente*, que o valor numérico duma função assimétrica das raízes seja racional. Seja, por exemplo, a equação

$$z^3 + pz + q = 0.$$

Consideremos a função assimétrica das raízes

$$V = (z_3 - z_2)\,(z_3 - z_1)\,(z_2 - z_1)\,.$$

O valor de V será, segundo a expressão indicada no número 28, dada pela fórmula

$$V = \sqrt{D} = \sqrt{-4p^3 - 27q^2}\,.$$

Ora, pode acontecer, em casos particulares, que $\sqrt{D}$ seja racional; tal é, por exemplo, o caso da equação

$$z^3 - 9z + 9 = 0\,,$$

para a qual se tem $V = \sqrt{9^3} = +\,27$, sem que as raízes sejam racionais, como se pode verificar.

Consideremos agora, mais geralmente, um corpo numérico Ω, qualquer, e uma equação algébrica $f(z) = 0$, de coeficientes em Ω. Dada uma função racional das raízes desta equação

$$\beta = \varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)\,,$$

cujos coeficientes sejam elementos de Ω, é claro que, se tal função pertencer ao grupo S_n (isto é, se for *simétrica*), o seu valor numérico, β, será ainda um elemento de Ω. Mas esta propriedade não é, necessariamente, um privilégio do grupo simétrico, S_n.

Diremos que um dado grupo G de substituições sobre os $\alpha\alpha$ é um grupo *admissível* da equação $f(z) = 0$, *a respeito do corpo* Ω, quando toda a função racional dos $\alpha\alpha$ com os coeficientes em Ω, que fique formalmente invariante para as substituições de G, tenha o seu valor numérico em Ω.

Imediatamente se reconhece que o grupo simétrico é sempre um grupo admissível. Por outro lado, é fácil ver que *condição necessária e suficiente para que G seja um grupo admissível da equação $f(z) = 0$, a respeito do corpo Ω, é que exista uma função racional (com coeficientes racionais) das raízes da equação, pertencente ao grupo G em sentido restrito e cujo valor numérico esteja em Ω.*

Com efeito, se for $\beta = \varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ uma tal função, qualquer função racional das raízes, com os coeficientes em Ω, que fique invariante para as substituições de G, poderá, segundo o teorema de LAGRANGE, exprimir-se como função racional (com os coeficientes em Ω) de β e dos coeficientes da equação e o seu valor numérico pertencerá portanto a Ω.

Mais ainda: podemos demonstrar o seguinte

TEOREMA – *A intersecção de dois grupos admissíveis da equação $f(z) = 0$, a respeito do corpo Ω, é ainda um grupo admissível de $f(z) = 0$ a respeito de Ω.*

Sejam, com efeito, G, H dois grupos admissíveis de $f(z) = 0$ em relação a Ω, e sejam φ, ψ duas funções racionais das raízes, com coeficientes racionais, que pertençam em sentido restrito respectivamente a G e a H. (Segundo a análise do número precedente existem sempre duas tais funções). Seja, por outro lado, χ uma função racional das raízes, com coeficientes racionais, pertencente ao grupo $G \cap H$. Ora, segundo o teorema de LAGRANGE generalizado, a função χ poderá exprimir-se racionalmente em φ, ψ e nos coeficientes de $f(z) = 0$. Mas tanto os valores de φ e de ψ, como os coeficientes de $f(z) = 0$, pertencem por hipótese a Ω. logo, também o valor de χ pertencerá a Ω, o que significa que a intersecção $G \cap H$ é um grupo admissível da equação $f(z) = 0$ a respeito do corpo Ω, q.e.d..

Sejam então $G_1, G_2, \ldots, G_\mu$ os grupos admissíveis de $f(z) = 0$, a respeito do corpo Ω. (Eles são necessariamente em número finito, visto serem subconjuntos de S_n).

Consideremos o grupo

$$\begin{aligned} G &= G_1 \cap G_2 \cap \cdots \cap G_\mu \\ &= ((G_1 \cap G_2) \cap \cdots) \cap G_\mu . \end{aligned}$$

Em virtude do teorema precedente, G será ainda um grupo admissível de $f(z)$ a respeito de Ω: será pois um dos grupos $G_1, G_2, \ldots, G_\mu$ e precisamente o *menor* de todos eles. Chamar-lhe-emos *grupo de GALOIS* da equação $f(z) = 0$, a respeito do corpo Ω. Portanto:

Grupos de GALOIS da equação $f(z)=0$ a respeito do corpo Ω é o mínimo grupo admissível de $f(z)=0$ a respeito de Ω.

Como exemplo, consideremos de novo a equação $z^3-9z+9=0$. O grupo alternante A_3 é um grupo admissível desta equação para o corpo racional **Ra**, pois que, como vimos, a função V, pertencente a A_3 em sentido restrito, tem o valor numérico em **Ra**. Mas A_3 é o grupo gerado pela substituição (1 2 3): o seu único subgrupo, distinto de A_n, é o grupo $\mathscr{T}$. Mas $\mathscr{T}$ não é um grupo admissível da equação considerada, em relação a **Ra**, pois que, se o fosse, a função $\varphi(\alpha_1, \alpha_2, \alpha_3) \equiv \alpha_1$ teria valor racional: ora já dissemos que as raízes desta equação são irracionais. Logo é A_4 o grupo de GALOIS da equação considerada a respeito de **Ra**.

36. Pesquisa do grupo de GALOIS duma equação

Uma questão se põe, primeiro que tudo, na pesquisa do grupo de GALOIS:

Como fixar as notações $\alpha_1, \alpha_2, \ldots, \alpha_n$, antes de conhecer efectivamente as raízes (todas distintas por hipótese) da equação $f(z)=0$?

Um dos vários critérios que poderiam servir para este fim seria o seguinte: representar as raízes por $\alpha_1, \alpha_2, \ldots, \alpha_n$, segundo a ordem crescente dos módulos e, no caso das raízes equimodulares, segundo a ordem crescente dos argumentos, entre 0 e 2π. *Todavia, o mais cómodo ainda é deixar primeiro indeterminadas as notações* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *e fixá-las apenas no momento oportuno.*

Ora, para determinar o grupo de GALOIS da equação $f(z)=0$ a respeito dum dado corpo Ω, será preciso, naturalmente, procurar grupos admissíveis da equação para o corpo Ω. Como se consegue porém saber se um dado grupo H de substituições sobre os $\alpha\alpha$ é ou não um grupo admissível da equação a respeito de Ω? As considerações do número precedente indicam-nos o caminho a seguir.

Construa-se (pelo processo do n.° 34) uma função racional $\beta = \varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$, que pertença ao grupo H em sentido restrito, e considere-se a equação

$$g(u) = (u - \beta_1)(u - \beta_2) \cdots (u - \beta_m) = 0,$$

cujas raízes são as funções conjugadas de β. Conforme o que se viu no número 29, os coeficientes desta equação são racionalmente exprimíveis nos coeficientes da proposta, e, portanto, pertencentes a Ω. Então, dois casos se podem apresentar:

a) A equação $g(u) = 0$ não admite raízes em Ω.
b) A equação $g(u) = 0$ admite pelo menos uma raiz em Ω.

No primeiro caso, pode-se concluir desde logo que o grupo H não é admissível para Ω. Quanto ao segundo caso, *podemos supor as notações* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *fixadas de modo tal que uma das raízes de* $g(u)=0$ *pertencentes a* Ω *seja precisamente a raiz* $\beta = \varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$, e então podemos afirmar que o grupo H é um grupo admissível da equação $g(u) = 0$, a respeito de Ω.

Resta porém um ponto importante a esclarecer: Como se consegue saber se a equação $g(u) = 0$ admite ou não uma raiz em Ω?

O caso mais simples será aquele em que Ω é o corpo racional: trata-se então de saber se a equação $g(u)=0$ admite ou não raízes racionais, problema que ensinam a resolver todos os tratados clássicos de Álgebra Superior.

Nos casos em que Ω não seja o corpo racional, o problema complica-se, naturalmente. Dele nos ocuparemos só mais adiante.

Finalmente, podemos indicar o modo de achar o grupo de GALOIS da equação $f(z) = 0$, a respeito de Ω:

Apenas se tenha determinado um grupo admissível H, a respeito de Ω (e um destes grupos é sempre um grupo simétrico), bastará prosseguir a pesquisa entre os subgrupos de H. Então, se nenhum dos subgrupos máximos de H é admissível a respeito de Ω, H será manifestamente o grupo de GALOIS que se pretende determinar. Se, pelo contrário se encontra um subgrupo máximo K de H, que seja ainda admissível a respeito de Ω, repetir-se-à para K o que se fez para H. E assim sucessivamente. Deste modo, o grupo de GALOIS acabará seguramente por ser determinado com um número finito de operações.

Este método, tal como acabamos de o expor, resultaria excessivamente laborioso na prática. Há todavia considerações de ordem vária, que simplificam consideravelmente a pesquisa do grupo de GALOIS.

37. Equações do terceiro grau [1]. Equações cíclicas

Recordemos o método de TARTAGLIA para a resolução da equação geral do 3.° grau e vejamos se é possível descobrir nele alguma ideia que possa aplicar-se a classes mais extensas de equações.

Em primeiro lugar, sabe-se que é sempre possível, mediante uma transformação em $z + \lambda$, sendo λ a média aritmética das raízes, reduzir a equação geral do 3.° grau à forma

$$z^3 + pz + q = 0. \tag{9}$$

Ponhamos então $z = u + v$ e procuremos determinar u e v, de modo que a equação (9) seja verificada.

Virá, sucessivamente:

$$u^3 + v^3 + 3u^2v + 3uv^2 + p(u+v) + q = 0,$$
$$u^3 + v^3 + (3uv + p)(u+v) + q = 0.$$

A equação será portanto verificada, se pusermos

$$3uv = -p, \quad u^3 + v^3 = -q. \tag{10}$$

A primeira destas igualdades dá-nos

$$u^3 \cdot v^3 = -\frac{1}{27}p^3.$$

(1) – Para um estudo completo do assunto, veja-se Prof. VICENTE GONÇALVES, Curso de Álgebra Superior, 2.° Vol..

Os valores de u^3 e de v^3 serão pois as raízes da equação do segundo grau em ζ:

$$\zeta^2 - q\zeta - \frac{1}{27}p^3 = 0.$$

Para brevidade da expressão, designemos por A e B as raízes desta equação:

$$u^3 = A, \quad v^3 = B.$$

Então, deverá ter-se

$$z = u + v = \sqrt[3]{A} + \sqrt[3]{B}.$$

Mas existem três raízes cúbicas de A e três raízes cúbicas de B; somando cada determinação de $\sqrt[3]{A}$, com cada determinação de $\sqrt[3]{B}$, obtém-se ao todo *nove* valores para z, enquanto a equação (9) nos dá apenas *três*. Desfaz-se esta indeterminação, atendendo à primeira das igualdades (10). Então, se representarmos por u_1 uma das determinações de $\sqrt[3]{A}$, a determinação correspondente $\sqrt[3]{B}$ deverá ser

$$v_1 = -\frac{p}{3u_1}.$$

As restantes determinações de $\sqrt[3]{A}$, serão ρu_1, $\rho^2 u_1$, representando por ρ uma das raízes cúbicas primitivas da unidade, isto é, uma das raízes da equação

$$z^2 + z + 1 = 0.$$

(Poderá escolher-se, por exemplo:

$$\rho = \frac{-1 + \sqrt{3}\,i}{2}, \quad \sigma = \frac{-1 - \sqrt{3}\,i}{2} = \rho^2,$$

tendo-se, evidentemente,

$$1 + \rho + \rho^2 = 0).$$

As determinações de $\sqrt[3]{B}$ correspondentes a ρu_1, $\rho^2 u_1$, serão, respectivamente,

$$v_2 = -\frac{p}{3\rho u_1} = \rho^{-1} v_1 = \rho^2 v_1 ,$$

$$v_3 = -\frac{p}{3\rho^2 u_1} = \rho^{-2} v_1 = \rho v_1 ,$$

e assim, as três raízes de (9) serão:

$$z_1 = u_1 + v_1 , \quad z_2 = \rho u_1 + \rho^2 v_1 , \quad z_3 = \rho^2 u_1 + \rho v_1 .$$

Estas mesmas igualdades permitem-nos determinar u_1 e v_1 em função de z_1, z_2, z_3. Para obter u_1, basta multiplicar ordenadamente a segunda por ρ^2, a terceira por ρ e somar ordenadamente as três, atendendo a que é $1 + \rho + \rho^2 = 0$; virá

$$u_1 = \frac{1}{3} (z_1 + \rho^2 z_2 + \rho z_3) .$$

Analogamente, ter-se-á

$$v_1 = \frac{1}{3} (z_1 + \rho z_2 + \rho^2 z_3) .$$

Estudemos estas duas funções, do ponto de vista das substituições sobre os zz. A transposição (2 3) muda u_1 em v_1. Quanto às substituições do grupo alternante, A_4 distintas de I, observa-se que:

a) o ciclo (1 2 3) muda u_1 em

$$\frac{1}{3} (z_2 + \rho^2 z_3 + \rho z_1) = \frac{1}{3} \rho (z_1 + \rho^2 z_2 + \rho z_3) = \rho u_1 ;$$

b) o ciclo (1 3 2) muda u_1 em

$$z_3 + \rho^2 z_1 + \rho z_2 = \rho^2 u_1 .$$

Deste modo, a função u_1^3 será transformada pelo ciclo (1 2 3) na função

$$\rho^3\, u_1^3 = u_1^3$$

e, pelo ciclo (1 3 2), na função

$$\rho^6\, u_1^3 = u_1^3\ ;$$

numa palavra, ficará invariante para as substituições de A_3 (e só para essas), o que a torna racionalmente exprimível em $V = \sqrt{D}$ e nos coeficientes da equação proposta (n.° 31). Outro tanto se diga a respeito da função v_1^3.

Consideremos agora uma equação $f(z) = 0$, de grau n, de coeficientes contidos num dado corpo Δ. Diremos que esta equação é *cíclica* a respeito de Δ, quando for cíclico e transitivo um dos seus grupos admissíveis[(1)] a respeito de Δ.

Suponhamos pois que $f(z)=0$ é cíclica a respeito de Δ, e designe H um seu grupo admissível (a respeito de Δ) que seja cíclico e transitivo. Se for σ uma das substituições geradoras de H, é claro que σ só poderá ser formada por um n – ciclo, de contrário cada um dos ciclos em que se decompusesse daria lugar a um sistema de transitividade. Ter-se-á pois

$$\sigma = (i_1\, i_2\, \ldots\, i_n)\,,$$

em que $i_1, i_2, \ldots, i_n$ representam os elementos $1, 2, \ldots, n$ dispostos numa ordem determinada, sem omissão nem repetição. Mas nada nos impede de supor as notações $\alpha_1, \alpha_2, \ldots, \alpha_n$ (das raízes de $f(z)=0$ previamente escolhidas de modo que se tenha, precisamente, $i_1 = 1,\ i_2 = 2, \ldots,\ i_n = n$; e assim poderemos escrever, mais comodamente, $\sigma = (1\ 2\ \ldots\ n)$.

(1) – Segundo a terminologia corrente, a equação $f(z)=0$ diz-se cíclica a respeito de Δ, quando é cíclico e transitivo o seu grupo de GALOIS a respeito de Δ. Há contudo vantagem, do ponto de vista didáctico, em apresentar o conceito de "equação cíclica", tal como o definimos aqui.

Por outro lado, tem-se:

$$H = \{I, \sigma, \sigma^2, \dots, \sigma^{n-1}\}.$$

Posto isto, designemos por ω uma das raízes primitivas de índice n da unidade. Notemos, desde já, que o grupo H é ainda um grupo admissível de $f(z)=0$ a respeito do corpo ampliado $\Delta(\omega)$: com efeito, qualquer função racional dos $\alpha\alpha$, com coeficientes racionais, pertencente em sentido restrito a H, tem o valor numérico em Δ e portanto em $\Delta(\omega)$ (reveja cuidadosamente as considerações do n.° 35). Consideremos então a seguinte função das raízes

$$\beta = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3 + \cdots + \omega^{n-1}\alpha_n.$$

As funções conjugadas de β *em H,* obtém-se, como é sabido, executando as substituições de H sobre os $\alpha\alpha$, na expressão de β. Ponhamos:

$$\beta_1 = \beta, \quad \beta_2 = \sigma\{\beta\}, \quad \beta_3 = \sigma^2\{\beta\}, \dots, \beta_n = \sigma^{n-1}\{\beta\}$$

Ter-se-á, como é fácil verificar:

$$\begin{aligned}
\beta_1 &= \alpha_1 + \omega\alpha_2 + \cdots + \omega^{n-1}\alpha_n = \beta, \\
\beta_2 &= \alpha_2 + \omega\alpha_3 + \cdots + \omega^{n-1}\alpha_1 = \omega^{-1}\beta, \\
\beta_3 &= \alpha_3 + \omega\alpha_4 + \cdots + \omega^{n-1}\alpha_2 = \omega^{-2}\beta, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\beta_n &= \alpha_n + \omega\alpha_1 + \cdots + \omega^{n-1}\alpha_{n-1} = \omega\beta.
\end{aligned}$$

Daqui resulta imediatamente que

$$\beta_1^n = \beta_2^n = \cdots = \beta_n^n,$$

visto ser $(\omega^{-1})^n = 1$, $(\omega^{-2})^n = 1, \dots, \omega^n = 1$.

Ponhamos $\beta^n = \gamma$. Segundo o que acabamos de ver, γ é uma função racional dos $\alpha\alpha$, de coeficiente em $\Delta(\omega)$, a qual se mantém formalmente invariante para todas as substituições de H. Ora H é um grupo admissível de $f(z) = 0$, a respeito de $\Delta(\omega)$. Logo, γ tem de ser um elemento de $\Delta(\omega)$. O valor de β pode pois ser deduzido de um elemento de Δ mediante uma extracção de raiz:

$$\beta = \sqrt[n]{\gamma} \quad (\text{tem-se } \gamma \in \Delta(\omega)).$$

Por outro lado, observemos que β é uma função racional das raízes, de coeficientes em $\Delta(\omega)$, pertencente em sentido restrito ao grupo $\mathscr{T}$ dentro de H (as suas conjugadas $\beta_1, \beta_2, \ldots, \beta_n$ em H são todas numericamente distintas). Mas, por sua vez, α_1 é uma função racional das raízes, de coeficientes racionais,

$$\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n) \equiv \alpha_1 + 0 \cdot \alpha_2 + \cdots + 0 \cdot \alpha_n,$$

pertencente ao grupo $\mathscr{T}$ dentro de H. Logo, segundo o teorema de LAGRANGE generalizado, poderá escrever-se

$$(11) \qquad \begin{cases} \alpha_1 = c_1 \beta_1^{n-1} + c_2 \beta_1^{n-2} + \cdots + c_{n-1} \beta_1 + c_n, \\ \alpha_2 = c_1 \beta_2^{n-1} + c_2 \beta_2^{n-2} + \cdots + c_{n-1} \beta_2 + c_n, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \alpha_n = c_1 \beta_n^{n-1} + c_2 \beta_n^{n-2} + \cdots + c_{n-1} \beta_n + c_n, \end{cases}$$

sendo os coeficientes $c_1, c_2, \ldots, c_n$ elementos de $\Delta(\omega)$. Com efeito, uma substituição qualquer de H executada sobre os $\alpha\alpha$ determina apenas uma substituição sobre os $\beta\beta$, e o seu efeito será, quando muito, o de alterar a ordem das equações (11), o que não influi sobre o valor dos *cc* deduzido dessas equações; os *cc* são pois funções racionais dos $\alpha\alpha$, de coeficientes em $\Delta(\omega)$, que se mantém formalmente invariantes para as substituições de H, donde se conclui que pertencem ao corpo $\Delta(\omega)$, atendendo à hipótese feita sobre H.

Veremos oportunamente que é mesmo possível eliminar a raiz primitiva ω, das expressões obtidas para os $\alpha\alpha$.

Em conclusão:

Se a equação $f(z)=0$ é cíclica a respeito de Δ, as raízes de $f(z)=0$ podem ser obtidas, efectuando apenas operações racionais e uma extracção de raiz, a partir de elementos de Δ.

Observe-se, entretanto, que toda a equação do terceiro grau é cíclica a respeito do corpo gerado pelos coeficientes e pela raiz quadrada do discriminante. Em particular, a equação $z^3 - 9z + 9 = 0$ é cíclica a respeito do corpo racional pois que, como vimos no n.° 35, a raiz quadrada do seu discriminante é ± 27, portanto racional.

38. Condição suficiente de resolubilidade por meio de radicais

Dada uma equação algébrica $f(z)=0$, de coeficientes contidos num dado corpo Δ, diz-se que tal equação *é resolúvel por meio de radicais* a respeito do corpo Δ, quando todas as suas raízes podem ser obtidas mediante operações racionais e extracções de raiz, efectuadas um número finito de vezes sobre elementos de Δ ou sobre os resultados de tais operações.

Em vez da locução "por meio de radicais", poderia usar-se esta outra "por meio de equações binómias", visto que o símbolo $\sqrt[n]{a}$ designa, como é sabido, uma qualquer das raízes da equação binómia

$$z^n - a = 0,$$

obtendo-se as restantes raízes da mesma equação multiplicando $\sqrt[n]{a}$ pelas potências duma raiz primitiva de índice n da unidade. Chama-se *extracção da raiz de índice n* de a, precisamente, a operação que consiste em passar de a para $\sqrt[n]{a}$.

Posto isto, designe G um grupo admissível da equação $f(z)=0$ a respeito do corpo Δ e seja

$$\beta = \varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

uma função racional, com coeficientes racionais, de $\alpha_1, \alpha_2, \ldots, \alpha_n$, pertencente em sentido restrito ao grupo G. (Já sabemos que é sempre possível determinar uma tal função). Ter-se-á então, naturalmente, $\beta \in \Delta$.

Seja agora H um subgrupo de G, distinto de G. Construída uma função racional das raízes

$$\gamma = \psi(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

com coeficientes racionais, pertencente em sentido restrito a H dentro de G (isto é, pertencente formalmente a H em G e tal que as suas conjugadas em G sejam todas numericamente distintas), já não podemos garantir que se tenha $\gamma \in \Delta$, a não ser que H seja ainda um grupo admissível de $f(z)=0$ a respeito de Δ.

Seja porém como for, nós podemos assentar nos seguintes factos:

I – *O grupo H é um grupo admissível da equação $f(z)=0$, a respeito do corpo $\Delta(\gamma)$.* Com efeito, qualquer função racional dos $\alpha\alpha$, com os coeficientes em Δ, que fique formalmente invariante para as substituições de H em G, pode, segundo o teorema de LAGRANGE generalizado, exprimir-se como função racional de γ, com os coeficientes em Δ e terá o valor numérico em $\Delta(\gamma)$.

II – *Representando por $\gamma_1(=\gamma), \gamma_2, \ldots, \gamma_m$ as conjugadas de γ em G, a equação*

$$g(z) \equiv (z-\gamma_1)\,(z-\gamma_2) \cdots (z-\gamma_m) = 0$$

terá os coeficientes em Δ. Com efeito, os coeficientes desta equação

$$-S_1 = -\sum \gamma_1, \quad S_2 = \sum \gamma_1 \gamma_2, \; \ldots \;, (-1)^n S_n = \\ = (-1)^n \gamma_1 \gamma_2 \ldots \gamma_n,$$

são, por intermédio dos $\gamma\gamma$, funções racionais dos $\alpha\alpha$ (com coeficientes racionais) que se mantêm formalmente invariantes para todas as substituições de G, uma vez que o efeito destas substituições é apenas permutar entre si os $\gamma\gamma$. Os valores numéricos de $S_1, S_2, \ldots, S_n$ serão pois elementos de Δ, em virtude da hipótese.

III – Já sabemos (n.° 26) que cada substituição θ de G sobre os $\alpha\alpha$ se traduz numa substituição $\overline{\theta}$ sobre os $\gamma\gamma$ e que, portanto, o grupo G dá assim origem a um grupo $\overline{G}$ de substituições sobre os $\gamma\gamma$. Seja então

$$\Gamma = \Phi(\gamma_1, \gamma_2, \ldots, \gamma_m)$$

uma qualquer função racional dos $\gamma\gamma$ (com os coeficientes em Δ) que se mantenha formalmente invariante para as substituições de $\overline{G}$. Executando sobre os $\alpha\alpha$ uma qualquer substituição de G, esta traduz-se numa substituição de $\overline{G}$ sobre os $\gamma\gamma$ e não altera portanto Φ. Logo Γ é, por intermédio dos $\gamma\gamma$, uma função racional dos $\alpha\alpha$ (com os coeficientes em Δ), que se mantém formalmente invariante para as substituições de G, tendo-se portanto

$$\Gamma \in \Delta.$$

Em resumo: toda a função dos $\gamma\gamma$, com os coeficientes em Δ, que se mantenha formalmente invariante para as substituições de $\overline{G}$, tem o valor numérico em Δ. Mas isto quer dizer precisamente que:
O grupo $\overline{G}$ é um grupo admissível da equação $g(z)=0$, a respeito do corpo Δ.

IV – Recordemos que, quando H é invariante em G, o grupo $\overline{G}$ é o chamado *grupo cociente*, G/H, cuja ordem é igual ao índice de H em G.
O caso mais simples será aquele em que o índice de H em G é um número primo. Mas então o grupo G/H admitirá, como únicos subgrupos, ele mesmo e a identidade, e *será portanto um grupo cíclico* (n.º 22). Com efeito, seja $\sigma(\neq I)$ um elemento de $\overline{G}$ e seja C o grupo cíclico gerado por σ; se C fosse distinto de $\overline{G}$, então $\overline{G}$ admitiria um subgrupo C, distinto dele mesmo e da identidade, o que é impossível.
Além disso, o *grupo $\overline{G}$ é transitivo*. Com efeito, dadas duas quaisquer conjugadas γ_i, γ_k de γ em G, designando por θ_i, θ_k duas substituições de G que façam passar, respectivamente, de γ_i para γ_k, a substituição

$$\theta_k\,\theta_i^{-1}$$

faz passar de γ_i para γ_k, e, portanto, a substituição

$$\overline{\theta}_k\,\overline{\theta}_i^{-1}$$

de $\overline{G}$ transforma γ_i em γ_k.

Em conclusão:

Se H é um subgrupo invariante de índice primo de G, a equação $g(z)=0$ é uma equação cíclica a respeito do corpo Δ, e pode portanto, segundo o que se disse no número precendente, resolver-se por meio de radicais a respeito de Δ.

Posto isto, suponhamos que o grupo G admite uma cadeia de subgrupos

$$G \supset H \supset K \supset \cdots \supset M \supset N \supset \mathscr{I},$$

começando em G e terminando no grupo idêntico, cada um dos quais, a partir do segundo, seja um *subgrupo invariante de índice primo do precedente*. Diz-se, em tal hipótese, que G é um grupo *resolúvel* ou *metacíclico*.

Sejam, por outro lado,

$$\gamma, \delta, \ldots, \eta, \zeta,$$

funções racionais dos $\alpha\alpha$, com coeficientes racionais, pertencentes em sentido restrito, respectivamente a H em G, K em $H, \ldots$, N em M, $\mathscr{I}$ em N; e sejam

$$h(z)=0, \quad k(z)=0, \ldots, n(z)=0, \quad \iota(z)=0,$$

as equações que admitem como raízes, respectivamente, as conjugadas de γ em G, de δ em $H, \ldots$, de η em M, de ζ em N.

Em virtude do que foi dito nas alíneas I), II) os coeficientes de $h(z)=0$ pertencerão ao corpo Δ, os de $k(z)=0$ ao corpo $\Delta(\gamma), \ldots$ os de $\iota(z)$ ao corpo $\Delta(\gamma, \delta, \ldots, n)$.

Por outro lado, em virtude do estabelecido nas alíneas III) e IV), a equação $h(z)=0$ será resolúvel por meio de radicais a respeito de Δ;

analogamente, a equação $k(z)$ será resolúvel por meio de radicais a respeito de $\Delta(\gamma)$, e portanto a respeito de Δ, visto que o elemento γ é raiz da equação $h(z)=0$. E assim sucessivamente. Podemos portanto concluir que a equação $\iota(z)=0$ é resolúvel por meio de radicais a respeito de Δ.[1]

Ora o elemento ζ, raiz da equação $\iota(z)=0$, pertence em sentido restrito ao grupo $\mathscr{T}$ em N. Logo, toda a função racional dos $\alpha\alpha$ (com coeficientes racionais), e em particular as funções $\alpha_1, \alpha_2, \ldots, \alpha_n$, poderão exprimir-se em ζ, mediante polinómios com os coeficientes em $\Delta(\gamma, \delta, \ldots, \eta)$. Mas isto significa precisamente que a equação $f(z)=0$ é resolúvel por meio de radicais a respeito de Δ.

Podemos pois assentar no seguinte resultado fundamental:

Condição suficiente para que uma equação algébrica $f(z)=0$ seja resolúvel por meio de radicais a respeito de um dado corpo Δ é que um seu grupo admissível a respeito de Δ seja um grupo metacíclico.

Já se disse que o mínimo grupo admissível da equação $f(z)=0$ a respeito do corpo Δ é chamado o grupo de GALOIS de $f(z)=0$ em relação a Δ. Pois bem, diz-se que a equação é *metacíclica* em relação a Δ, precisamente quando o seu grupo de GALOIS a respeito de Δ é metacíclico.

Segundo o que acaba de ser estabelecido, toda a equação metacíclica é resolúvel por meio de radicais. Veremos no capítulo seguinte que a recíproca desta proposição também é verdadeira; isto é, demonstraremos que as únicas *equações resolúveis por meio de radicais (a respeito de um determinado corpo Δ) são as equações metacíclicas (a respeito de Δ).*

Exemplos:

a) Como exemplo de aplicação da doutrina exposta, consideremos a equação

$$f(z) \equiv z^4 - 2z^3 + z^2 + 2z - 1 = 0,$$

cujas raízes representaremos por $\alpha_1, \alpha_2, \alpha_3, \alpha_4$.

---

(1) – O elemento ζ, raiz de $\iota(z)$ ficará portanto expresso mediante um número finito de radicais sobrepostos.

Comecemos por procurar grupos admissíveis desta equação a respeito do corpo **Ra**. Seja, por exemplo, o grupo

$$G=\{I,\,(1\,2),\,(3\,4),\,(1\,2)\,(3\,4),\,(1\,3)\,(2\,4),\,(1\,4)\,(2\,3),\,(1\,3\,2\,4),\,(1\,4\,2\,3)\},$$

subgrupo máximo de S_4, ao qual pertence, entre outras, a função

$$\beta=\alpha_1\,\alpha_2+\alpha_3\,\alpha_4\,.$$

Construamos a equação $g(z)=0$, que tem por raízes as conjugadas de β (resolvente de FERRARI da proposta).

Segundo o que foi estabelecido no n.° 29, ter-se-á

$$g(z)\equiv z^3-z^2-4=0\,.$$

Ora, fazendo a pesquiza das raízes racionais desta equação, encontra-se 2 como raiz, sendo as restantes raízes $g(z)$ as raízes da equação $z^2+z+2=0$, ambas imaginárias. Podemos então supor escolhidas as notações $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, de modo que a raiz 2 seja precisamente o valor numérico da função $\alpha_1\,\alpha_2+\alpha_3\,\alpha_4$, a qual pertencerá, em sentido restrito, ao grupo G – visto que as suas conjugadas (raízes de $g(z)=0$) são numericamente distintas. *O grupo G é pois um grupo admissível da equação proposta a respeito de* **Ra**.

Consideremos agora subgrupos máximos de G. Seja, por exemplo, o grupo

$$H=\{I,\,(1\;2),\,(3\;4),\,(1\;2)\,(3\;4)\},$$

ao qual pertence em G a função

$$\gamma=\alpha_1\,\alpha_2\,.$$

As conjugadas desta função em G são

$$\gamma_1=\alpha_1\,\alpha_2\,(=\gamma),\quad \gamma_2=\alpha_3\,\alpha_4$$

e a equação que admite γ_1, γ_2 como raízes será

$$h(z) = z^2 - (\gamma_1 + \gamma_2) z + \gamma_1 \gamma_2 = 0 .$$

Mas

$$\gamma_1 + \gamma_2 = \alpha_1 \alpha_2 + \alpha_3 \alpha_4 = \beta = 2,$$

$$\gamma_1 \gamma_2 = \alpha_1 \alpha_2 \alpha_3 \alpha_4 = -1$$

e portanto

$$h(z) \equiv z^2 - 2z - 1 .$$

A equação resolvente $h(z) = 0$ tem pois os coeficientes em **Ra**, conforme o previsto na teoria. Por outro lado, H é um subgrupo invariante de índice 2 de G, e, segundo a teoria, a equação $h(z) = 0$ deve ser cíclica a respeito de **Ra**, o que realmente acontece: toda a equação do segundo grau é cíclica, uma vez que o grupo simétrico S_2 é gerado pelo ciclo (1 2).

Podemos então escrever

$$\gamma_1 = 1 - \sqrt{2}\,, \quad \gamma_2 = 1 + \sqrt{2}\,.$$

Posto isto, consideremos o grupo

$$K = \{I,\ (3\ 4)\}\,,$$

subgrupo invariante de H, ao qual pertence em H a função

$$\delta = \alpha_1\,,$$

que tem por conjugadas em H

$$\delta_1 = \alpha_1\ (= \delta), \quad \delta_2 = \alpha_2\,.$$

A equação que admite δ_1, δ_2 como raízes será

$$K(z) \equiv z^2 - (\alpha_1 + \alpha_2)\, z + \alpha_1 \alpha_2 = 0\,.$$

Ora

$$\alpha_1 \alpha_2 = \gamma_1 = 1 + \sqrt{2}\,.$$

Quanto a $\alpha_1 + \alpha_2$, recordemos (n.° 29) que é

$$\alpha_1 \alpha_2 (\alpha_3 + \alpha_4) + \alpha_2 \alpha_3 (\alpha_1 + \alpha_2) = \sum \alpha_1 \alpha_2 \alpha_3 = 1,$$

ou seja

$$(1 + \sqrt{2})\,[2 - (\alpha_1 + \alpha_2)] + (1 - \sqrt{2})(\alpha_1 + \alpha_2) = 1,$$

donde

$$\alpha_1 + \alpha_2 = \frac{1 + 2\sqrt{2}}{\sqrt{2}} = 2 + \frac{\sqrt{2}}{2}\,.$$

A equação $k(z) = 0$ tem pois os coeficientes em $\mathbf{Ra}(\gamma) = \mathbf{Ra}(\sqrt{2})$. A sua resolução fornece-nos as raízes α_1, α_2 da proposta.

Finalmente, o único subgrupo de H (distinto de K) é o grupo idêntico, $\mathscr{T}$, ao qual pertence em K a função

$$\varepsilon = \alpha_3$$

cujas conjugadas em K são

$$\varepsilon_1 = \alpha_3 \;(= \varepsilon)\,, \quad \varepsilon_2 = \alpha_4\,.$$

A equação que admite ε_1, ε_2 como raízes é

$$\iota(z) \equiv z^2 - (\alpha_3 + \alpha_4)\, z + \alpha_3 \alpha_4 = 0\,,$$

equação de coeficientes em $\mathbf{Ra}(\sqrt{2})$, cuja resolução nos fornece as restantes raízes da proposta.

Utilizou-se, portanto, na resolução de $f(z) = 0$, a cadeia de grupos

$$G \supset H \supset K \supset \mathscr{T},$$

cada um dos quais, a partir do segundo, é subgrupo invariante de índice 2 do precedente.

Note-se como, neste caso, as raízes de $f(z) = 0$ se exprimem exclusivamente mediante radicais quadráticos. Isto habilita a concluir que tais raízes podem ser determinadas graficamente, por meio da régua e do compasso.

b) Só excepcionalmente o grupo de GALOIS duma equação a respeito de **Ra** não é o grupo simétrico. No caso da equação do quarto grau, de coeficientes racionais, se o discriminante da equação e as raízes da sua resolvente cúbica não forem racionais, o grupo de GALOIS da equação a respeito de **Ra** será S_4.

Mas o grupo S_4 é metacíclico. Com efeito, representando por V_4 o grupo do rectângulo e por N o grupo

$$\{I, (1\ 2)\ (3\ 4)\},$$

ter-se-á

$$S_4 \supset A_4 \supset V_4 \supset N \supset \mathscr{I},$$

sendo cada um destes grupos, a partir do segundo, subgrupo invariante de índice primo do precedente. Uma função pertencente a A_4 é, como já sabemos, $V = \sqrt{B}$; o seu valor calcula-se, portanto, mediante uma equação do segundo grau, o que está de acordo com o facto de ser 2 o índice de A_4 em S_4.

Por sua vez, a função

$$\beta = \alpha_1 \alpha_2 + \alpha_3 \alpha_4$$

pertence ao grupo V_4 em A_4. A equação que admite como raízes as conjugadas de β em A_4, será ainda a resolvente de FERRARI, que se apresenta portanto como equação cíclica a respeito do corpo numérico $\Delta = \mathbf{Ra}(\sqrt{D})$.

A função $\gamma = \alpha_1 \alpha_2$ pertence ao grupo N em V_4, tendo por conjugadas em V_4 as funções $\alpha_1 \alpha_2$, $\alpha_3 \alpha_4$.

Os coeficientes da equação

$$(z - \alpha_1 \alpha_2)(z - \alpha_3 \alpha_4) = 0$$

serão pois elementos do corpo $\mathbf{Ra}(\sqrt{D}, \beta)$.

Finalmente, a função $\delta = \alpha_1 - \alpha_2$, cujo quadrado é um elemento do corpo $\mathbf{Ra}(\sqrt{D}, \beta, \gamma)$, pertence ao grupo $\mathscr{T}$ em N, e portanto as raízes α_1, α_2, α_3, α_4 da equação proposta estarão todas contidas no corpo ampliado

$$\mathbf{Ra}(\sqrt{D}, \beta, \gamma, \delta).$$

As raízes α_1, α_2, α_3, α_4 ficarão pois expressas mediante um radical cúbico e três radicais quadráticos.

Página em branco

NOTAS FINAIS

A) *Sobre o teorema de LAGRANGE.*

O teorema de LAGRANGE generalizado pode ainda ser apresentado sob a seguinte forma, particularmente cómoda para a aplicação à teoria de GALOIS:

Consideremos uma equação algébrica $f(z)=0$, de raízes $\alpha_1, \alpha_2, \ldots, \alpha_n$, com os coeficientes num dado corpo Δ, e seja G um seu grupo admissível a respeito de Δ. Consideremos, por outro lado, uma função racional $\beta=\varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ das raízes desta equação, com os coeficientes em Δ e pertencente em sentido restrito a um grupo H em G. Nestas condições, qualquer outra função racional das raízes,

$$\gamma=\Psi(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

com os coeficientes em Δ, que fique formalmente invariante para as substituições de H, terá o valor em $\Delta(\beta)$.

A técnica da demonstração é inteiramente análoga à que seguimos nos n.os 30 e 32. Sejam $\beta_1(=\beta), \beta_2, \ldots, \beta_m$ as funções conjugadas de β em G, e

$$\gamma_1(=\gamma), \gamma_2, \ldots, \gamma_m$$

as funções correspondentes obtidas a partir de γ. Tomando para incógnitas $c_1, c_2, \ldots, c_m$, o determinante do sistema

$$(27) \qquad \gamma_i=c_1\beta_i^{m-1}+c_2\beta_i^{m-2}+\cdots+c_m \quad (i=1, 2, \ldots m),$$

é o determinante de VANDERMONDE em $\beta_1, \beta_2, \ldots, \beta_m$ e portanto $\neq 0$. Por outro lado, qualquer substituição θ de G sobre os $\alpha\alpha$ não faz mais do que produzir uma substituição sobre os $\beta\beta$ e a substituição correspondente sobre os $\gamma\gamma$, provocando assim, quando muito, uma alteração da ordem das equações (27). Os coeficientes $c_1, c_2, \dots, c_m$ são pois, por intermédio dos $\beta\beta$ e dos $\gamma\gamma$, funções racionais dos $\alpha\alpha$, com os coeficientes em Δ que se mantêm formalmente invariantes para as substituições de G. Mas G é, por hipótese, um grupo admissível da equação $f(z) = 0$ a respeito de Δ. Logo, tem-se

$$c_1, c_2, \dots, c_m \in \Delta,$$

o que prova a afirmação feita.

B) *Sobre as equações cíclicas.*

Nas considerações desenvolvidas no n.° 37 sobre a resolução algébrica da equação cíclica, há um ponto a rectificar. A função das raízes,

$$\beta = \sum_{k=1}^{n} \omega^{k-1} \alpha_k,$$

só pertencerá em sentido restrito ao grupo $\mathscr{T}$ em H, se for $\beta \neq 0$. Esta dificuldade pode ser removida do seguinte modo: se os $\alpha\alpha$ são todos distintos, existe necessariamente um expoente μ tal que

$$\sum_{k}^{n} \omega^{k-1} \alpha_k^{\mu} \neq 0;$$

com efeito, se assim não fosse, as equações

$$\omega^0 \alpha_1^r + \omega \alpha_2^r + \cdots + \omega^{n-1} \alpha_n^r = 0 \quad (r = 0, 1, \dots, n-1),$$

considerando $\omega^0, \omega, \dots, \omega^{n-1}$ como incógnitas, formariam um sistema determinado, tendo por única solução $\omega^0 = \omega = \cdots = \omega^{n-1} = 0$, o que é absurdo. Pode então tomar-se para valor de β o somatório

$$\sum_{k=1}^{n} \omega^{k-1} \alpha_k^{\mu},$$

em vez do primeiro. Deste modo se evita o inconveniente indicado, e todos os raciocínios podem seguir como foi dito no n.° 37.

Página em branco

ÍNDICE

INTRODUÇÃO ÀS MODERNAS TEORIAS ALGÉBRICAS

CAP. I – **Generalidades sobre conjuntos e transformações**

CAP. II – **Transitividade e Homomorfia**

CAP. III – **Resolubilidade por meio de radicais (1ª parte)**

CAP. IV – **Resolubilidade por meio de radicais (2ª parte)**