I.1

INTRODUÇÃO ÀS MODERNAS TEORIAS ALGÉBRICAS

(Apenas o esboço dum curso de iniciação)

Página em branco

CAPÍTULO IV

RESOLUBILIDADE POR MEIO DE RADICAIS

(2ª parte)

39. Redutibilidade dos polinómios. Corpos algebricamente fechados

Seja $f(z)$ um polinómio em z de grau n e de coeficientes situados num dado corpo Δ.

Diz-se que $f(z)$ *é redutível em* Δ, quando existem pelo menos dois polinómios $p(z)$, $q(z)$, de coeficientes ainda em Δ, ambos de grau *superior* a 0 e *inferior* a n, tais que

$$f(z) \equiv p(z) \cdot q(z).$$

Se esta hipótese se não verifica, diz-se que $f(z)$ é *irredutível* em Δ. Por sua vez a equação $f(z) = 0$ diz-se *redutível* ou *irredutível* em Δ, consoante o polinómio $f(z)$ é redutível ou irredutível em Δ.

Consideremos, por exemplo, o polinómio de coeficientes racionais

$$x^4 - x^2 - 2.$$

As suas raízes são, como é fácil reconhecer, os números i, $-i$, $\sqrt{2}$, $-\sqrt{2}$. Ter-se-á pois a decomposição em factores lineares:

$$x^4 - x^2 - 2 \equiv (x - i)\,(x + i)\,(x - \sqrt{2})\,(x + \sqrt{2}).$$

Vê-se então que, a respeito do corpo **Ra**, o referido polinómio admite a seguinte decomposição em factores irredutíveis:

$$x^4 - x^2 - 2 \equiv (x^2 + 1)\,(x^2 - 2)\,.$$

Passando porém ao corpo $\mathbf{Ra}(i)$, o factor x^2+1 torna-se redutível

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

Finalmente, no corpo $\mathbf{Ra}(i, \sqrt{2})$ o polinómio em questão decompõe-se nos factores irredutíveis $x+i$, $x-i$, $x+\sqrt{2}$, $x-\sqrt{2}$, todos do primeiro grau.

Dum modo geral, um polinómio $f(z)$ diz-se *completamente redutível* num corpo Δ, quando é decomponível num produto de factores todos do primeiro grau, de coeficientes em Δ. Por sua vez, um dado corpo Ω diz-se *algebricamente fechado*, quando todo o polinómio de coeficientes em Ω é completamente redutível em Ω (ou, e que vem a dar no mesmo, quando toda a equação algébrica de coeficientes em Ω admite pelo menos uma raiz em Ω). Assim, por exemplo, o corpo complexo é algebricamente fechado: é este, precisamente, o facto afirmado pelo "Teorema fundamental da Álgebra" ou "Teorema de D'Alembert". Mas já o corpo real não é algebricamente fechado.

Chama-se *número algébrico* todo o número que é raiz de alguma equação algébrica de coeficientes racionais. É fácil provar que o conjunto A de todos os números algébricos é um corpo algebricamente fechado, e, *portanto, o mínimo corpo algebricamente fechado existente*. Com efeito, seja

$$f(z) = z^n + \gamma_1 z^{n-1} + \gamma_2 z^{n-2} + \cdots + \gamma_n = 0$$

uma qualquer equação de coeficientes em A e sejam

$$p_1(u_1) = 0,\ p_2(u_1) = 0,\ \ldots,\ p_n(u_n) = 0\,,$$

equações de *coeficientes racionais*, que admitam como raízes respectivamente,

$$\gamma_1, \gamma_2, \cdots, \gamma_n .$$

Ora, eliminando as incógnitas $u_1, u_2, \ldots, u_n$ entre a equação

$$z^n + u_1 z^{n-1} + u_2 z^{n-2} + \cdots + u_n = 0$$

e as equações

$$p_1(u_1) = 0, p_2(u_2) = 0, \ldots, p_n(u_n) = 0,$$

chega-se necessariamente a uma equação algébrica, $F(z) = 0$, de *coeficientes racionais*, que admitirá, entre outras, as raízes da equação inicial, $f(z) = 0$, o que prova a afirmação feita.

Demonstra-se também facilmente que o conjunto dos números algébricos tem a potência do *numerável*. Como, por outro lado, o conjunto dos números complexos tem, notoriamente, a potência do *contínuo*, segue-se que existem números não algébricos – os quais são chamados *números transcendentes*.

Em 1873, HERMITE demonstrou a transcendência do número *e* e, nove anos depois, LINDEMANN conseguiu demonstrar[1] a transcendência de π. O facto de π ser um número transcendente implica a impossibilidade de resolver o famoso problema da quadratura do círculo por meio da régua e do compasso.

40. Teorema fundamental da irredutibilidade. Componentes dum número num dado corpo

Na teoria de GALOIS, desempenha um papel fundamental o seguinte teorema:

Sejam $f(z)$, $g(z)$ dois polinómios de coeficientes situados num mesmo corpo Δ. Se $g(z)$ é irredutível em Δ e se $f(z)$ admite pelo menos uma raiz de $g(z)$, então $f(z)$ admite todas as raízes de $g(z)$.

---

(1) – Para uma demonstração simplificada destes factos, veja-se VALIRON, "Théorie des fonctions", pag. 104.

Demonstração:

Seja $d(z)$ o máximo divisor comum de $f(z)$ e $g(z)$. Visto que os coeficientes de $d(z)$ se obtém a partir dos coeficientes de $f(z)$ e $g(z)$ efectuando apenas operações racionais, tais coeficientes serão ainda elementos de Δ. Suponhamos que existe uma raiz α comum a $f(z)$ e a $g(z)$: então α será também raiz de $d(z)$ e portanto o grau de $d(z)$ será necessariamente superior a zero. Como, por outro lado, $d(z)$ é um divisor de $g(z)$ de coeficientes em Δ, e $g(z)$ é irredutível em Δ, segue-se que o grau de $d(z)$ só poderá ser igual ao de $g(z)$ e que, portanto, $d(z)$ é, quando muito, o produto de $g(z)$ por um factor constante. Logo $f(z)$ será divisível por $g(z)$ e admitirá assim todas as raízes de $g(z)$, q. e. d.

Como consequência deste teorema, podemos agora demonstrar que:

Se $f(z)=0$ é uma equação de grau n, irredutível em Δ, e se α é uma raiz de $f(z)=0$, condição necessária e suficiente para que resulte

$$(12) \qquad c_1\alpha^{n-1} + c_2\alpha^{n-2} + \cdots + c_{n-1}\alpha + c_n = 0,$$

sendo $c_1, c_2, \ldots, c_n$ elementos de Δ, é que se tenha

$$c_1 = c_2 = \cdots = c_n = 0.$$

A condição é manifestamente suficiente. Suponhamos agora que se verifica a igualdade (12), sendo $c_1, c_2, \ldots, c_n$ elementos de Δ. Então, o polinómio

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

de coeficientes em Δ, admite a raiz α de $f(z)$. Mas $f(z)$ é irredutível em Δ. Logo, segundo o teorema anterior, $p(z)$ admitirá as n raízes de $f(z)$, e, como o grau de $p(z)$ é inferior a n, segue-se, pelo princípio das identidades, que

$$c_1 = c_2 = \cdots = c_n = 0.$$

Posto isto, sejam Δ e Ω dois corpos numéricos tais que

$$\Delta \subset \Omega .$$

Diz-se, em tal hipótese, que Δ é um *subcorpo de* Ω ou que Ω é uma *extensão* de Δ.

Por outro lado, se existir um número α capaz de gerar o corpo Ω a partir de Δ, isto é, um número a tal que

$$\Omega = \Delta(\alpha),$$

dir-se-á que Ω é uma *extensão simples* de Δ e ao número α chamar-se-á *elemento primitivo*, *elemento gerador* ou *elemento base* de Ω a respeito de Δ.

Diremos ainda que $\Delta(\alpha)$ é uma extensão *algébrica* de Δ, se α for raiz de alguma equação algébrica de coeficientes em Δ. Caso contrário, diremos que $\Delta(\alpha)$ é uma extensão *transcendente* de Δ.

Por exemplo, o corpo $\mathbf{Ra}(\sqrt{2})$ é uma extensão algébrica simples do corpo **Ra**, extensão que admite como elemento primitivo um qualquer dos seus elementos não contidos em **Ra**. Analogamente, o corpo $\mathbf{Ra}(\sqrt{2}, \sqrt{3})$ é (por exemplo) uma extensão algébrica simples do corpo $\Delta = \mathbf{Ra}(\sqrt{2})$, admitindo como elemento primitivo, a respeito de Δ, o número $\sqrt{3}$ ou qualquer outro dos seus elementos não situados em Δ. Por outro lado, o corpo $\mathbf{Ra}(\sqrt{2}, \sqrt{3})$ é uma extensão algébrica simples do corpo **Ra**, pois que se tem, como veremos adiante,

$$\mathbf{Ra}(\sqrt{2}, \sqrt{3}) = \mathbf{Ra}(\sqrt{2} + \sqrt{3}).$$

Consideremos então, em geral, um corpo numérico Ω, extensão algébrica simples dum corpo Δ:

$$\Omega = \Delta(\alpha),$$

e seja $f(z) = 0$ a equação irredutível em Δ que admite como raiz o elemento primitivo α. Os elementos de Ω são, como já sabemos, todos os números exprimíveis em α mediante funções racionais com os coeficientes em Δ. Mas, segundo o estabelecido no número 31,

todo o número ζ exprimível na raiz α de $f(z)$, mediante uma função racional ϕ de coeficientes em Δ, é susceptível da representação

$$\zeta = c_1\alpha^{n-1} + c_2\alpha^{n-2} + \cdots + c_{n-1}\alpha + c_n, \tag{13}$$

sendo n o grau da equação $f(z) = 0$ e estando os coeficientes $c_1, c_2, \ldots, c_n$ situados em Δ.

Deste modo, para cada elemento ζ de Ω, existirá um sistema $(c_1, c_2, \ldots, c_n)$ de n elementos de Δ que o representará segundo a fórmula (13). E podemos acrescentar que tal sistema é único, para cada $\zeta \in \Omega$. Com efeito, se for

$$c_1\alpha^{n-1} + c_2\alpha^{n-2} + \cdots + c_{n-1}\alpha + c_n =$$

$$= c'_1\alpha^{n-1} + c'_2\alpha^{n-2} + \cdots + c'_{n-1}\alpha + c'_n,$$

ter-se-á

$$(c_1 - c'_1)\alpha^{n-1} + (c_2 - c'_2)\alpha^{n-2} + \cdots + (c_n - c'_n) = 0$$

e portanto, em virtude do teorema precedente,

$$c_1 = c'_1, \quad c_2 = c'_2, \ \ldots, \quad c_n = c'_n,$$

visto ser $f(z) = 0$ irredutível em Δ, por hipótese.

É então natural chamar aos números $c_1, c_2, \ldots, c_n$ *componentes* (ou coordenadas) *em* Δ *do número* ζ a respeito do elemento base α. Fica portanto assim estabelecida uma correspondência biunívoca entre os elementos de Ω e os sistemas de n elementos de Δ; do mesmo modo que fica estabelecida uma correspondência biunívoca entre os pontos do espaço $\mathbf{R}_3$ e os sistemas de três números reais, uma vez fixado um referencial cartesiano.

Consideremos, por exemplo, o número $\sqrt{8} - \sqrt{3}$, pertencente ao corpo $\Omega = \mathbf{Ra}(\sqrt{2}, \sqrt{3})$. Representando por α o elemento $\sqrt{2} + \sqrt{3}$ de Ω, ter-se-á, como é fácil verificar

$$\sqrt{2} = \frac{1}{2}\left(\alpha - \frac{1}{\alpha}\right), \quad \sqrt{3} = \frac{1}{2}\left(\alpha + \frac{1}{\alpha}\right),$$

donde

$$\sqrt{8}-\sqrt{3}=2\sqrt{2}-\sqrt{3}=\frac{1}{2}\alpha-\frac{3}{2}\cdot\frac{1}{\alpha}.$$

Por outro lado, a equação irredutível em **Ra** que admite α como raiz é

$$z^4-10z^2+1=0.$$

Virá então

$$\sqrt{8}-\sqrt{3}=\frac{1}{2}\alpha+\frac{3}{2}(\alpha^3-10\alpha)=\frac{3}{2}\alpha^3-7\alpha.$$

Serão pois 3/2, 0, 7, 0 as coordenadas racionais de $\sqrt{8}-\sqrt{3}$ a respeito do elemento base $\sqrt{2}+\sqrt{3}$.

Como aplicação da doutrina exposta, procuremos um modo de resolver o seguinte problema:

Sendo ρ *uma raiz duma equação algébrica de coeficientes racionais e* $f(z)$ *um polinómio de coeficientes em* $\mathbf{Ra}(\rho)$, *determinar as raízes de* $f(z)$ *que porventura existam no corpo* $\mathbf{Ra}(\rho)$.

Seja então $g(z)$ o polinómio irredutível em **Ra** que admite ρ como raiz e designe m o grau deste polinómio. Em virtude dos resultados precedentes, cada raiz z da equação

$$f(z)\equiv z^n+a_1z^{n-1}+\cdots+a_n=0,$$

existente no corpo $\mathbf{Ra}(\rho)$, será da forma

$$z=x_1\rho^{m-1}+x_2\rho^{m-2}+\cdots+x_{m-1}\rho+x_m, \tag{14}$$

sendo $x_1, x_2, \ldots, x_m$ números racionais. Então, substituindo z por esta expressão em $f(z)=0$, obter-se-á, depois de efectuadas todas as possíveis simplificações, uma igualdade do tipo:

$$P_1\rho^{m-1}+P_2\rho^{m-2}+\cdots+P_{m-1}\rho+P_m=0, \tag{15}$$

em que $P_0, P_1, \ldots, P_m$ designam polinómios inteiros em $x_1, x_2, \ldots, x_m$, com coeficientes racionais. Ora, visto que $g(z)$ é irredutível em **Ra**, a igualdade (15) será verificada se, e só se, resultar simultaneamente

$$P_1 = 0, P_2 = 0, \ldots, P_m = 0.$$

Mas estas igualdades constituem um sistema de equações algébricas em $x_1, x_2, \ldots, x_m$, com coeficientes racionais. As raízes de $f(z)$ existentes em $\mathbf{Ra}(\rho)$, isto é, da forma (14), são-nos dadas, então, por todas as soluções $(x_1, x_2, \ldots, x_m)$ deste sistema constituídas unicamente por números racionais. Trata-se, portanto, em última análise, de achar as soluções racionais do referido sistema, o que se consegue efectuando sucessivas eliminações e determinando as raízes racionais das equações algébricas assim obtidas.

Exercícios:

1) Determinar as raízes da equação

$$z^2 - \sqrt{3}\, z + 2 = 0$$

existentes no corpo $\mathbf{Ra}(\sqrt{3})$.

2) Verificar que o número $\sqrt{1+i}$ não pertence ao corpo $\mathbf{Ra}(i)$.

41. Isomorfismos e automorfismos entre corpos

Dados dois corpos Ω, $\overline{\Omega}$, chama-se *isomorfismo* de Ω sobre $\overline{\Omega}$ toda a transformação biunívoca τ de Ω sobre $\overline{\Omega}$ que respeite a adição e a multiplicação; isto é, tal que

$$\tau(a+b) = \tau(a) + \tau(b), \quad \tau(a \cdot b) = \tau(a) \cdot \tau(b),$$

quaisquer que sejam $a, b \in \Omega$.

Se, em particular, se tem $\Omega = \overline{\Omega}$, o isomorfismo τ é chamado um *automorfismo* do corpo Ω.

Por exemplo, é fácil ver que, fazendo corresponder a cada elemento $a+b\sqrt{2}$ do corpo $\mathbf{Ra}(\sqrt{2})$ o seu conjugado $a-b\sqrt{2}$ (com a, b racionais), a transformação assim definida é um automorfismo do corpo $\mathbf{Ra}(\sqrt{2})$.

Resulta da definição precedente que todo o isomorfismo τ entre dois corpos Ω, $\overline{\Omega}$ respeita também a subtracção e a divisão. Com efeito, pondo

$$x = a - b\,, \qquad y = a/b\,,$$

vem

$$b + x = a\,, \qquad by = a\,,$$

donde

$$\tau(b) + \tau(x) = \tau(a), \quad \tau(b) \cdot \tau(y) = \tau(a),$$

ou seja

$$\tau(a-b) = \tau(x) = \tau(a) - \tau(b)$$

$$\tau(a/b) = \tau(y) = \tau(a) \,/\, \tau(b) \qquad \text{q. e. d.}$$

É fácil agora provar que:

Todo o isomorfismo τ, *entre dois corpos, deixa fixos os números racionais.*

Comecemos por observar que, tendo-se

$$0 = a - a\,, \quad 1 = a/a \quad (\text{com } a \neq 0)\,,$$

resultará

$$\tau(0) = \tau(a) - \tau(a) = 0\,, \quad \tau(1) = \tau(a) \,/\, \tau(a) = 1\,.$$

Por outro lado, sendo m um número inteiro positivo, virá

$$m = 1 + 1 + \cdots + 1 \ (m \text{ vezes})$$

e portanto

$$\tau(m) = \tau(1) + \tau(1) + \cdots + \tau(1) = m\,.$$

Ter-se-á, por conseguinte, para todo o número racional positivo m/n:

$$\tau(m/n) = \tau(m) \,/\, \tau(n) = m/n$$

e, finalmente, para todo o número racional negativo, $-r$:

$$\tau(-r) = \tau(0 - r) = \tau(0) - \tau(r) = -\tau(r) = -r\,.$$

42. Teorema fundamental dos isomorfismos entre corpos algébricos

Consideremos um corpo Ω, extensão algébrica simples de um outro corpo Δ, e proponhamo-nos resolver o seguinte problema:

Determinar todos os isomorfismos de Ω (*sobre um segundo corpo* Ω, *coincidente ou não com* Ω) *que deixam fixos os elementos de* Δ.

Seja então α um elemento base de Ω a respeito de Δ e seja

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

a equação *irredutível em* Δ que admite α como raiz. Já sabemos que todo o elemento ζ de Ω será então da forma

$$\zeta = c_1 \alpha^{n-1} + c_2 \alpha^{n-2} + \cdots + c_n, \tag{16}$$

com $c_1, c_2, \ldots, c_n \in \Delta$.

Seja agora τ um isomorfismo de Ω que deixe fixos os elementos de Δ. Ponhamos $\overline{\alpha} = \tau(\alpha)$, $\overline{\zeta} = \tau(\zeta)$. Aplicando τ a ambos os membros da igualdade

$$\alpha^n + a_1 \alpha^{n-1} + \cdots + a_{n-1} \alpha + a_n = 0,$$

virá, atendendo a que τ é um isomorfismo que deixa fixos os elementos de Δ (e portanto os coeficientes $a_1, a_2, \ldots, a_n$):

$$\overline{\alpha}^n + a_1 \overline{\alpha}^{n-1} + \cdots + a_{n-1} \overline{\alpha} + a_n \equiv f(\overline{\alpha}) = 0.$$

Isto é, o número $\overline{\alpha}$, transformado de α por meio de τ, é ainda uma raiz de $f(z)$.

Aplicando agora τ a ambos os membros de (16), virá, analogamente

$$\overline{\zeta} = c_1 \overline{\alpha}^{n-1} + c_2 \overline{\alpha}^{n-2} + \cdots + c_{n-1} \overline{\alpha} + c_n.$$

Podemos assim concluir que:

Se τ é um isomorfismo de Ω que deixa fixos os elementos de Δ, então o elemento base α, raiz do polinómio $f(z)$, é transformado por τ numa outra raiz, $\overline{\alpha}$, de $f(z)$ e cada elemento ζ de Ω é transformado por τ no número ζ cujas componentes em Δ a respeito de $\overline{\alpha}$ são precisamente as mesmas que as de ζ a respeito de α. Deste modo o corpo $\Omega = \Delta(\alpha)$ é transformado por τ no corpo $\overline{\Omega} = \Delta(\overline{\alpha})$.

Vamos agora ver que a recíproca desta proposição é também verdadeira. Seja, com efeito, $\overline{\alpha}$ uma raiz qualquer de $f(z)$ e consideremos a transformação τ que faz corresponder a cada elemento

$$\zeta = c_1\alpha^{n-1} + c_2\alpha^{n-2} + \cdots + c_n \tag{17}$$

do corpo $\Delta(\alpha)$ (com $c_1, c_2, \ldots, c_n \in \Delta$), o elemento

$$\overline{\zeta} = c_1\overline{\alpha}^{n-1} + c_2\overline{\alpha}^{n-2} + \cdots + c_n \tag{18}$$

do corpo $\Delta(\alpha)$. Observemos então que:

1) *A transformação τ é biunívoca.* Com efeito, pela fórmula (17), fica estabelecida uma correspondência biunívoca entre os elementos ζ de Ω e os sistemas $(c_1, c_2, \ldots, c_n)$ de n elementos de Δ; analogamente, pela fórmula (18) fica estabelecida uma correspondência biunívoca entre tais sistemas de n elementos de Δ e os elementos $\overline{\zeta}$ de $\overline{\Omega}$; logo, a correspondência $\zeta \to \overline{\zeta}$ é também biunívoca.

2) *Quaisquer que sejam $\zeta, \zeta' \in \Omega$, tem-se*

$$\tau(\zeta + \zeta') = \tau(\zeta) + \tau(\zeta').$$

Com efeito, designando por $c_1', c_2', \ldots, c_n'$ as componentes de ζ' a respeito de α (e portanto as de $\tau(\zeta')$ a respeito de $\overline{\alpha}$) é claro que as componentes de $\zeta + \zeta'$ a respeito de α serão

$$c_1 + c_1', \quad c_2 + c_2', \ldots, \quad c_n + c_n'.$$

Serão pois essas as componentes de $\tau(\zeta + \zeta')$ a respeito de $\overline{\alpha}$. Mas, por outro lado, as componentes de

$$\tau(\zeta) + \tau(\zeta')$$

a respeito de α serão ainda $c_1 + c_1'$, $c_2 + c_2'$, ..., $c_n + c_n'$, e que prova a afirmação feita.

3) *Quaisquer que sejam* $\zeta, \zeta' \in \Omega$, tem-se

$$\tau(\zeta\zeta') = \tau(\zeta)\,\tau(\zeta').$$

Para reconhecer este facto, basta observar que, tal como acontece para a soma, as componentes do produto $\zeta\zeta'$ (a respeito de α) se obtêm a partir das componentes de ζ e de ζ' do mesmo modo que as componentes de $\overline{\zeta} \cdot \overline{\zeta}'$ (a respeito de $\overline{\alpha}$) se obtêm a partir das componentes de $\overline{\zeta}$ e de $\overline{\zeta}'$ utilizando o processo indicado na última parte do número 31.

Finalmente, é obvio que τ deixa fixos os elementos de Δ.

E assim fica provado que τ é um isomorfismo de $\Delta(\alpha)$ sobre $\Delta(\overline{\alpha})$ que deixa invariantes os elementos de Δ.

Podemos portanto afirmar que:

Os isomorfismos de Ω *que deixam fixos os elementos de* Δ *são todas as transformações que se obtêm, substituindo o elemento base* α *por uma outra raiz* $\overline{\alpha}$, *qualquer, da equação* $f(z) = 0$ *(irredutível em* Δ*) e fazendo corresponder a cada elemento* ζ *de* $\Delta(\alpha)$ *o elemento* ζ *de* $\Delta(\overline{\alpha})$ *cujas componentes em* Δ *a respeito de* $\overline{\alpha}$ *são precisamente as mesmas que as de* ζ *a respeito de* α.

Sejam

$$\alpha_1 (= \alpha), \alpha_2, \ldots, \alpha_n$$

as raízes de $f(z)$. Pode acontecer, em particular, que se tenha

$$\Delta(\alpha_1) = \Delta(\alpha_2) = \cdots = \Delta(\alpha_n).$$

Nesta hipótese, é claro que todos os isomorfismos de Ω que deixam fixos os elementos de Δ são automorfismos. Diz-se então que o corpo Ω é *normal* a respeito de Δ. Também se diz, neste caso, que a equação $f(z) = 0$ é *normal* a respeito de Δ.

A equação $f(z)=0$ será portanto normal a respeito de Δ, quando (e só quando) todas as suas raízes forem exprimíveis numa qualquer delas, mediante funções racionais de coeficientes em Δ.

Exemplos:

a) *Determinar os isomorfismos do corpo* $\mathbf{Ra}(\sqrt{2},\sqrt{3})$ *que deixam fixos os elementos de* $\mathbf{Ra}(\sqrt{2})$. Ponhamos

$$\delta = \mathbf{Ra}(\sqrt{2}),\ \Omega = \Delta(\sqrt{3}).$$

O elemento base $(\sqrt{3})$ é raiz da equação $x^2-3=0$, irredutível em Δ. Por outro lado, a equação $x^2-3=0$ é normal em Δ (toda a equação do segundo grau é normal). Deste modo, os isomorfismos procurados serão a identidade e o automorfismo

$$c_1 + c_2\sqrt{3} \to c_1 - c_2\sqrt{3}$$

em que $c_1, c_2 \in \Delta$.

b) *Determinar todos os isomorfismos do corpo*

$$\Omega = \mathbf{Ra}(\sqrt{2},\sqrt{3}).$$

Já no número 40 se viu que $\mathbf{Ra}(\sqrt{2},\sqrt{3}) = \mathbf{Ra}(\sqrt{2}+\sqrt{3})$. A equação irredutível em **Ra** que admite o elemento base $\sqrt{2}+\sqrt{3}$ como raiz é

$$z^4 - 10\,z^2 + 1 = 0,$$

equação normal a respeito de **Ra**. Portanto, os isomorfismos de Ω são todos eles automorfismos, os quais se obtêm substituindo o elemento base $\sqrt{2}+\sqrt{3}$ por um qualquer dos números $\sqrt{2}+\sqrt{3}$, $\sqrt{2}-\sqrt{3}$, $-\sqrt{2}+\sqrt{3}$, $-\sqrt{2}-\sqrt{3}$, raízes da referida equação.

c) *Determinar os isomorfismos do corpo* $\mathbf{Ra}(\sqrt[3]{2})$. A equação irredutível em **Ra** que admite $\sqrt[3]{2}$ como raiz é $x^3-2=0$. Os isomorfismos de $\mathbf{Ra}(\sqrt[3]{2})$ obtêm-se portanto substituindo o elemento base $\sqrt[3]{2}$ por um qualquer dos números $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$, em que ω designa uma raiz cúbica primitiva da unidade. Mas pode-se demonstrar que os corpos

$$\mathbf{Ra}(\sqrt[3]{2}),\ \mathbf{Ra}(\omega\sqrt[3]{2}),\ \mathbf{Ra}(\omega^2\sqrt[3]{2})$$

são distintos, (isto é, que a equação $x^3-2=0$ não é normal). Por conseguinte, destes três isomorfismos só a identidade é automorfismo.

43. O grupo de GALOIS como grupo de automorfismos

Seja Ω uma extensão algébrica simples e normal de um dado corpo Δ, e designe Γ a família de todos os automorfismos de Ω que deixam fixos os elementos de Δ.

Do que ficou estabelecido no número precedente, resulta imediatamente que *o produto e o cociente de dois quaisquer elementos de* Γ *é ainda um elemento de* Γ. O conjunto Γ é pois um grupo ao qual se dá o nome de *grupo de* GALOIS *do corpo* Ω *a respeito do corpo* Δ, ou, abreviadamente, *grupo* de GALOIS *de* Ω/Δ.

Seja agora $f(z)=0$ uma equação algébrica de coeficientes em Δ, sem raízes múltiplas (irredutível ou não a respeito de Δ). Chama-se *corpo de* GALOIS desta equação a respeito de Δ o corpo

$$\Omega = \Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

obtido pela adjunção de todas as raízes $\alpha_1, \alpha_2, \ldots, \alpha_n$ de $f(z)$ ao corpo Δ.

Desde logo convém observar que o corpo de GALOIS de $f(z)=0$ *a respeito de* Δ *é uma extensão algébrica simples de* Δ. Com efeito, já no número 34 vimos como é possível construir uma função racional dos $\alpha\alpha$

$$\pi = k_1\alpha_1 + k_2\alpha_2 + \cdots + k_n\alpha_n, \tag{19}$$

de coeficientes inteiros, pertencente em sentido restrito ao grupo $\mathscr{T}$, na qual se podem portanto, segundo o teorema de LAGRANGE, exprimir todos os elementos de Ω, mediante funções racionais de coeficicentes em Δ. Ter-se-á pois

$$\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n) = \Delta(\pi),$$

o que prova a afirmação feita.

Posto isto, sejam

$$\pi_1 (= \pi), \pi_2, \ldots, \pi_\upsilon$$

as funções conjugadas de π (já sabemos que é $\upsilon = n!$). A equação

$$F(z) \equiv (z - \pi_1)(z - \pi_2) \cdots (z - \pi_\upsilon) = 0$$

que admite $\pi_1, \pi_2, \ldots, \pi_\upsilon$ como raízes, tem os coeficientes em Δ. Por outro lado, o polinómio $F(z)$ é decomponível num produto de factores irredutíveis em Δ (podendo, em particular ser já $F(z)$ irredutível). Seja então $R(z)$ o factor irredutível em Δ que admite π_1 como raiz e sejam $\pi_1, \pi_2, \ldots, \pi_r$ as raízes de $R(z)$. A equação

$$R(z) \equiv (z - \pi_1)(z - \pi_2) \cdots (z - \pi_r) = 0$$

diz-se uma *resolvente* de GALOIS da equação $f(z) = 0$ a respeito de Δ.

Notemos agora que o corpo $\Omega = \Delta(\pi)$ é normal em Δ. Com efeito, qualquer das raízes $\pi_1, \pi_2, \ldots, \pi_r$ de $R(z)$ é uma função racional dos $\alpha\alpha$ (de coeficientes inteiros) pertencente em sentido restrito ao grupo $\mathscr{T}$, e, portanto, qualquer delas pode gerar o corpo Ω a partir de Δ.

Então, segundo a análise do número precedente, os isomorfismos de Ω que deixam fixos os elementos de Δ serão todos eles automorfismos, que se obtêm substituindo o elemento base π por uma outra raiz, $\overline{\pi}$, qualquer, de $R(z)$ e fazendo corresponder a cada elemento ζ de Ω aquele elemento $\overline{\zeta}$ ainda de Ω cujas componentes em Δ a respeito de $\overline{\pi}$ são precisamente as mesmas que as de ζ a respeito de π.

Designemos então por Γ o conjunto de todos estes automorfismos, isto é, o grupo de GALOIS de Ω/Δ. Vamos provar que:

O grupo Γ *é isomorfo ao grupo de* GALOIS *da equação* $f(z) = 0$ *a respeito de* Δ.

Seja com efeito τ uma transformação pertencente a Γ e punhamos

$$\overline{\alpha}_1 = \tau(\alpha_1), \quad \overline{\alpha}_2 = \tau(\alpha_2), \ \ldots, \quad \overline{\alpha}_n = \tau(\alpha_n).$$

Raciocinando como anteriormente, é fácil reconhecer que se tem $f(\overline{\alpha}_i) = 0$, isto é, que $\overline{\alpha}_i$ ainda é uma raiz de $f(z)$, qualquer que seja $i=1, 2,\ldots, n$. Por outro lado, é evidente que os números $\overline{\alpha}_1, \overline{\alpha}_2, \ldots, \overline{\alpha}_n$ são ainda todos distintos entre si. Deste modo, a transformação τ traduz-se na substituição

$$\theta = \begin{pmatrix} \overline{\alpha}_1 & \overline{\alpha}_2 & \cdots & \overline{\alpha}_n \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix}$$

sendo ainda manifesto que a correspondência $\tau \rightarrow \theta$ assim definida é um homomorfismo. Mais ainda: esta correspondência é biunívoca. Com efeito, aplicando τ a ambos os membros de (19), vem

$$\overline{\pi} = \tau(\pi) = k_1 \overline{\alpha}_1 + k_2 \overline{\alpha}_2 + \cdots + k_n \overline{\alpha}_n .$$

Ora, há uma *única* transformação τ pertencente a Γ que transforma π em $\overline{\pi}$ e portanto uma única que transforma α_1 em $\overline{\alpha}_1$, α_2 em $\overline{\alpha}_2, \ldots, \alpha_n$ em $\overline{\alpha}_n$.

Representaremos por G o conjunto das substituições θ assim induzidas sobre os $\alpha\alpha$. Resta-nos provar que G é o grupo de GALOIS da equação $f(z)=0$, a respeito de Δ. Para isso, devemos demonstrar as duas seguintes proposições, chamadas *propriedades características de G*:

A.

Seja $\beta = \varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *uma função racional dos* $\alpha\alpha$, *com os coeficientes em* Δ, *que se mantenha numericamente invariante para todas as substituições de G. Então, podemos afirmar que* β *é um elemento de* Δ.

Demonstração:

Visto ser β um elemento de $\Omega = \Delta(\pi)$, é claro que poderemos escrever

$$\beta = p(\pi),$$

designando por p um polinómio de coeficientes em Δ. Efectuando sobre os $\alpha\alpha$ todas as substituições de G, o elemento π transforma-se

nos seus conjugados $\pi_1, \pi_2, \ldots, \pi_r$, enquanto β, por hipótese, se mantém invariante.

Então virá

$$\beta = p(\pi_1) = p(\pi_2) = \cdots = p(\pi_r)$$
$$= \frac{1}{n}[p(\pi_1) + p(\pi_2) + \cdots + p(\pi_r)].$$

Ora, a expressão entre colchetes é uma função simétrica das raízes de $R(z)$ e, como tal, racionalmente exprimível nos coeficientes de $R(z)$; o seu valor numérico está pois em Δ, e o mesmo acontecerá quanto a β.

B.

Seja $\beta = \varphi(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *uma função racional dos* $\alpha\alpha$, *com os coeficientes em* Δ, *cujo valor numérico*, β, *esteja em* Δ. *Então, podemos afirmar que tal função se mantém numericamente invariante para todas as substituições de G.*

A demonstração desta propriedade é imediata, atendendo a que toda a substituição pertencente a G define um automorfismo de Ω que deixa fixos os elementos de Δ.

Ora, da propriedade A deduz-se que G é um grupo admissível de $f(z)=0$, a respeito de Δ, pois que, se uma função fica formalmente invariante para uma dada substituição σ sobre os $\alpha\alpha$, também ficará numericamente invariante para σ (só a recíproca não é verdadeira). Seja agora H um subgrupo de G, admissível de $f(z)=0$ a respeito de Δ, e seja

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

uma função racional dos $\alpha\alpha$, com coeficientes em Δ, pertencente, em sentido restrito a H: o valor numérico, β, desta função deve então, estar em Δ; mas, segundo a propriedade B, ela ficará numericamente invariante (e portanto formalmente, visto pertencer a G em sentido restrito) para todas as substituições de G; logo $H = G$. Podemos pois concluir que G é o mínimo grupo admissível de $f(z)=0$ a respeito de Δ, ou seja, o grupo de GALOIS de $f(z)=0$ a respeito de Δ, q.e.d.

44. Estudo da redutibilidade através do grupo de GALOIS

Mantendo as hipóteses e as notações do número precedente, consideremos um elemento β qualquer de $\Omega = \Delta(\pi)$. Existirá então um polinómio $p(z)$ de coeficientes em Δ tal que $\beta = p(\pi)$. Pondo

$$\beta_1 = p(\pi_1),\ \beta_2 = p(\pi_2),\ \ldots,\ \beta_r = p(\pi_r),$$

a equação

$$P(z) \equiv (z - \beta_1)\,(z - \beta_2) \cdots (z - \beta_r) = 0,$$

que é uma transformação de TSCHIRNHAUS de $R(z) = 0$, terá os coeficientes em Δ. O polinómio $P(z)$ pode ser ou não irredutível em D. Em qualquer hipótese, existirá um seu factor $Q(z)$ irredutível em Δ que admite β_1 como raiz.

Seja agora τ um automorfismo de Ω que deixe fixos os elementos de Δ, e ponhamos $\overline{\beta}_1 = \tau(\beta_1)$. Visto que se tem

$$Q(\beta_1) = 0,$$

será ainda

$$Q(\overline{\beta}_1) = 0.$$

Ora os transformados de β_1 por meio de todas as transformações de Γ (grupo de GALOIS de Ω/Δ) são precisamente $\beta_1, \beta_2, \ldots, \beta_r$. Tem-se pois que todas as raízes de $P(z)$ são ainda raízes de $Q(z)$, o que obriga a concluir que é

$$P(z) = k[Q(z)]^{\mu},$$

sendo k um factor constante e μ um número natural, que pode em particular reduzir-se a 1.

Em conclusão: *Os elementos em que pode ser transformado* β *pelas transformações pertencentes a* Γ *são raízes duma equação irredutível em* Δ *cujo grau é um divisor do grau de* $R(z) = 0$.

Pode ainda reconhecer-se que, se $\mu = 1$, e só então, β será um elemento primitivo de Ω a respeito de Δ.

Note-se que β pode, em particular, ser uma das raízes de $f(z)$. Podemos assim concluir que:

Os elementos em que pode ser transformada uma raiz α_i de $f(z)$ pelas substituições de G são as raízes do factor de $f(z)$, irredutível em Δ, que admite α_i como raiz.

Mas os elementos em que pode ser transformada α_i pelas substituições de *G* constituem, por definição, o sistema de transitividade a que pertence α_i. *Deste modo, a cada sistema da transitividade de G corresponde um factor de $f(z)$ irredutível em Δ, e reciprocamente.*

Em particular:

Condição necessária e suficiente para que $f(z) = 0$ seja irredutível em Δ é que seja transitivo o seu grupo de GALOIS *a respeito de Δ.*

Como exemplo, consideremos a equação

$$(x^2 - 2)\,(x^2 - 3) = 0,$$

cujo corpo de GALOIS (a respeito de **Ra**) é, como já sabemos,

$$\Omega = \mathbf{Ra}(\sqrt{2}, \sqrt{3}) = \mathbf{Ra}(\sqrt{2} + \sqrt{3})$$

e de que é uma resolvente de GALOIS a equação irredutível

$$z^4 - 10\,z^2 + 1 = 0,$$

que admite $\sqrt{2} + \sqrt{3}$ como raiz. O grupo de GALOIS de $\Omega/\mathbf{Ra}$ traduz-se então num grupo de substituições sobre os números $\sqrt{2}$, $-\sqrt{2}$, $\sqrt{3}$, $-\sqrt{3}$, cujos sistemas de transitividade são

$$\{\sqrt{2}, -\sqrt{2}\},\ \ \{\sqrt{3}, -\sqrt{3}\}.$$

A estes sistemas correspondem, precisamente, os factores irredutíveis x^2-2, x^2-3, da equação proposta.

45. Equações binómias

Consideremos a equação binómia

$$z^p - a = 0 \tag{20}$$

em que p designa um número primo e a um elemento de um dado corpo Δ, *o qual contenha as raízes primitivas de índice p da unidade.* Designemos por ω uma tal raiz primitiva e por ζ uma raiz qualquer de (20). As raízes desta equação serão pois

$$\zeta_1 = \zeta\,,\quad \zeta_2 = \omega\zeta\,,\quad \zeta_3 = \omega^2\zeta\,,\ldots,\quad \zeta_p = \omega^{p-1}\zeta\,.$$

Podemos então escrever

$$\zeta_2 = \omega\zeta_1\,,\quad \zeta_3 = \omega\zeta_2\,,\ldots,\quad \zeta_p = \omega\zeta_{p-1},\quad \zeta_1 = \omega\zeta_p\,. \tag{21}$$

Vê-se pois que, multiplicar por ω cada um dos $\zeta\zeta$, equivale a efectuar sobre estes elementos a substituição

$$\sigma = (1\ 2\ \ldots\ p)\,.$$

Portanto, efectuar sobre os $\zeta\zeta$ a substituição σ^m equivale a multiplicar cada um deles pala potência ω^m de ω ($m = 1, 2,\ldots$).

Designemos então por G o grupo de GALOIS da equação (20) a respeito de Δ e seja θ uma substituição qualquer de G. Ponhamos, por outro lado,

$$\theta(\zeta_1) = \overline{\zeta}_1\,,\quad \theta(\zeta_2) = \overline{\zeta}_2,\ldots,\quad \theta(\zeta_p) = \overline{\zeta}_p\,.$$

Ora θ define um automorfismo de $\Delta(\zeta)$ que deixa fixos os elementos de Δ. Além disso, Δ contém ω, por hipótese. Logo, atendendo a (21),

$$\overline{\zeta}_2 = \omega\overline{\zeta}_1\,,\quad \overline{\zeta}_3 = \omega\overline{\zeta}_2,\ldots,\quad \overline{\zeta}_p = \omega\overline{\zeta}_{p-1}\,.$$

Então, se for

$$\overline{\zeta}_1 = \zeta_i = \omega^i \zeta_1,$$

é claro que será também

$$\overline{\zeta}_2 = \omega \overline{\zeta}_1 = \omega \cdot \omega^i \zeta_1 = \omega^i \cdot \omega \zeta_1 = \omega^i \zeta_2,$$

e, analogamente,

$$\overline{\zeta}_3 = \omega^i \zeta_3, \ldots, \quad \overline{\zeta}_p = \omega^i \zeta_p.$$

Mas já vimos que multiplicar por ω^i cada um dos $\zeta\zeta$ equivale a efectuar sobre eles a substituição σ^i. Logo

$$\theta = \sigma^i.$$

Pode pois concluir-se que o grupo G é um subgrupo do grupo cíclico C_p gerado por σ e, como a ordem de C_p é um número primo, de duas uma: ou $G = C_p$ ou $G = \mathscr{I}$. No primeiro caso, o grupo G será manifestamente transitivo, o que implica, segundo o resultado do número precedente, a irredutibilidade de (20) a respeito de Δ. Se $G = \mathscr{I}$, então é claro que todas as raízes de (20) estarão em Δ.

Em resumo:

Se não existir em Δ um número ζ tal que $\zeta^p = a$, então o grupo de GALOIS *da equação*

$$z^p - a = 0$$

a respeito de Δ é um grupo cíclico transitivo de ordem p, e a equação é portanto irredutível em Δ. Caso contrário, o grupo da equação a respeito de Δ reduz-se à identidade.

46. Teorema de GALOIS sobre adjunções

Designe G o grupo de GALOIS duma dada equação $f(z) = 0$ a respeito dum corpo Δ. Efectuando a adjunção de um ou mais elementos

$\gamma_1, \gamma_2, \ldots, \gamma_m$ ao corpo Δ, é claro que o grupo de GALOIS de $f(z)=0$ a respeito do corpo ampliado $\Delta(\gamma_1, \gamma_2, \ldots, \gamma_n)$ não pode deixar de ser um subgrupo G' do primitivo grupo G, podendo em particular ter-se ainda $G' = G$. Exprime-se abreviadamente este facto, dizendo que a adjunção de tais elementos *reduz* ou *conserva* o grupo de GALOIS da equação considerada.

Ora, o estudo da resolubilidade por meio de radicais, assenta em parte sobre o seguinte teorema de GALOIS (mais tarde generalizado por JORDAN).

Dada uma equação $\rho(z)=0$, *cujo grupo de GALOIS a respeito do corpo* Δ *seja um grupo cíclico transitivo de ordem prima p, a adjunção de uma raiz desta equação ao corpo* Δ *ou conserva o grupo de equações* $f(z)=0$ *(a respeito de* Δ*) ou o reduz a um seu subgrupo invariante de índice p.*

Demonstração:

Sejam $\zeta_1, \zeta_2, \ldots, \zeta_p$ as raízes de $\rho(z)=0$. Recordemos em primeiro lugar que (n.° 37), sendo o grupo C de $\rho(z)=0$ um grupo cíclico transitivo, ele só pode ser gerado por uma substituição cíclica, que podemos supor seja precisamente o ciclo $\sigma = (1\ 2\ \ldots\ p)$.

Ora a equação $\rho(z)=0$ é normal a respeito de Δ (n.° 42), por outras palavras: *toda a equação cíclica é normal.* Com efeito, designando por C o grupo gerado por σ, a raiz ζ_1, como função racional de $\zeta_1, \zeta_2, \ldots, \zeta_p$, pertence em sentido restrito ao grupo $\mathcal{T}$ em C. Então, segundo o teorema de LAGRANGE generalizado, dada uma raiz ζ_i qualquer de $\rho(z)$, será possível determinar p elementos

$$C_1^i, C_2^i, \ldots, C_p^i$$

de Δ, tais que

$$\zeta_i = C_1^i \zeta_1^p + C_2^i \zeta_1^{p-1} + \cdots + C_p^i,$$

o que significa precisamente que a equação $\rho(z)=0$ é normal a respeito de Δ.

Seja então G o grupo da equação $f(z) = 0$ a respeito de Δ e seja H o grupo da mesma equação a respeito do corpo ampliado $\Delta(\zeta_1)$. Construída uma função racional, com coeficientes racionais,

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

das raízes de $f(z)$, pertencente em sentido restrito ao grupo H, deverá ter-se $\beta \in \Delta(\zeta_1)$, ou seja

$$\beta = \phi(\zeta_1),$$

sendo ϕ uma função racional com coeficientes em Δ.

Designando por $\beta_1, \beta_2, \ldots, \beta_m$ as funções conjugadas de β em G (elementos em que é transformado β por todas as transformações do grupo de GALOIS de Ω/Δ), a equação

$$Q(z) \equiv (z - \beta_1)(z - \beta_2) \cdots (z - \beta_m) = 0,$$

deverá, segundo o estabelecido no n.° 44, ser irredutível em Δ (pois que os números $\beta_1, \beta_2, \ldots, \beta_m$ são todos distintos). Deste modo, $Q(z)$ é o polinómio irredutível em Δ que admite como raiz o elemento $\beta_1 = \phi(\zeta_1)$, situado no corpo $\Delta(\zeta_1)$. Por outro lado, já vimos que este corpo é normal a respeito de Δ (contém todas as raízes da equação $\rho(z) = 0$). Então, atendendo ainda ao que foi estabelecido no n.°44, segue-se que o grau m de $Q(z)$ deve ser um divisor do grau p de $\rho(z)$, e, como p é por hipótese um número primo, de duas uma: ou $m = 1$ ou $m = p$. Mas m é o índice de H em G (número das conjugadas de β em G). Logo, ou se tem $H = G$ ou H é um subgrupo de índice p de G.

Resta provar que o grupo H é invariante em G. Para isso, basta observar que os elementos $\beta_1, \beta_2, \ldots, \beta_m$ estão todos situados no corpo $\Delta(\zeta_1)$, o que leva a concluir, (atendendo à propriedade B estabelecida no n.° 43) que $\beta_1, \beta_2, \ldots, \beta_m$ são funções dos $\alpha\alpha$ pertencentes ao grupo H em G, visto ser H o grupo de GALOIS de $f(z) = 0$ a respeito do corpo $\Delta(\zeta_1)$. Ora, segundo o que se disse antes, isto significa precisamente que o grupo H é invariante em G.

47. Equações ciclotómicas[1]

Seja ainda p um número primo. Como é sabido, as raízes primitivas de índice p da unidade são todas as raízes da equação

$$\gamma(z) \equiv \frac{x^p - 1}{x - 1} \equiv x^{p-1} + x^{p-2} + \cdots + x + 1 = 0,$$

chamada *equação ciclotómica* ou *equação da divisão do círculo*, porque traduz analiticamente o problema da divisão do círculo em p partes iguais. Designando por ω uma raiz qualquer da equação $\gamma(z) = 0$, já sabemos que as raízes desta equação coincidem, na sua totalidade, com as potências

$$\omega, \omega^2, \ldots, \omega^{p-1}$$

da raiz ω. Por outro lado, também é sabido que, para se ter

$$\omega^m = \omega^n,$$

é necessário e suficiente que resulte: $m \equiv n$ (mod. p).

Ora, demonstra-se, na teoria dos números, que, qualquer que seja o número primo p, existe um número inteiro g cujas potências

$$g, g^2, \ldots, g^{p-2}, g^{p-1}$$

são, àparte a ordem, congruentes aos números $1, 2, 3, \ldots, p-1$, a respeito do módulo p; tendo-se, em particular,

$$g^{p-1} \equiv 1 \text{ (mod. } p).$$

Quer isto então dizer que os números

$$\omega^g, \omega^{g^2}, \ldots, \omega^{g^{p-2}}, \omega^{g^{p-1}} \tag{22}$$

---

(1) – Para um estudo detalhado deste assunto, veja-se PROF. VICENTE GONÇALVES, Curso de Álgebra Superior, 2.º Vol.

coincidirão, àparte a ordem, com

$$\omega, \omega^2, \omega^3, \ldots, \omega^{p-1},$$

raízes da equação ciclotómica $\gamma(z) = 0$; tendo-se, em particular,

$$\omega^{g^{p-1}} = \omega .$$

Portanto, se designarmos estes números por $\omega_1, \omega_2, \ldots, \omega_{p-1}$, segundo a ordem por que se apresentam em (22), virá, como é fácil ver,

$$(23) \qquad \omega_2 = \omega_1^g, \omega_3 = \omega_2^g, \ldots, \omega_{p-1} = \omega_{p-2}^g, \omega_1 = \omega_{p-1}^g .$$

Vê-se pois que, *elevar cada uma das raízes* $\omega_1, \omega_2, \ldots, \omega_{p-1}$ à potência do expoente g, equivale a efectuar sobre elas a substituição cíclica[1]

$$\sigma = (1\ 2\ \ldots\ \ldots\ p-1);$$

e que, portanto, efectuar sobre as raízes $\omega_1, \omega_2, \ldots, \omega_{p-1}$ *a substituição* $\sigma^i (i = 1, 2, \ldots)$ *equivale a elevar cada uma delas à potência do expoente* g^i.

Seja agora θ uma substituição qualquer do grupo de GALOIS da equação $\gamma(z) = 0$ a respeito de **Ra**. Aplicando θ a ambos os membros das igualdades (23), tem-se, atendendo ao que foi atrás estabelecido,

$$\overline{\omega}_2 = \overline{\omega}_1^g, \overline{\omega}_3 = \overline{\omega}_2^g, \ldots, \overline{\omega}_{p-1} = \overline{\omega}_{p-1}^g, \overline{\omega}_1 = \overline{\omega}_{p-1}^g .$$

Mas $\overline{\omega}_1$ é ainda uma das raízes de $\gamma(z)$; ponhamos $\overline{\omega}_1 = \omega^{g^k}$. Então virá

$$\overline{\omega}_2 = \omega_1^{g^{k+1}} = (\omega_1^g)^{g^k} = \omega_2^{g^k},$$

e, analogamente,

---

(1) – Este facto pode designar-se, de maneira sugestiva, por *circulação das raízes da equação ciclotómica.*

$$\omega_3 = \omega_3^{g^k}, \ldots, \overline{\omega}_{p-1} = \omega_{p-1}^{g^k}.$$

Logo, será

$$\theta = \sigma^k.$$

O grupo de GALOIS de $\gamma(z) = 0$ a respeito de **Ra** será portanto um subgrupo do grupo C gerado por σ. Demonstra-se mesmo que coincide com este grupo; mas, para o que se segue, basta-nos saber que C é um grupo admissível da equação $\gamma(z) = 0$ a respeito de **Ra**.

Observemos, por outro lado, que *todo o grupo cíclico (finito) é resolúvel.*

Seja com efeito G um grupo cíclico de ordem m, e seja p_1 um factor primo de m. Designando por τ uma das transformações geradoras de G, facilmente se reconhece que o período de τ^{p_1} é precisamente igual a m/p_1. Deste modo, o grupo G_1 gerado por τ^{p_1} será um subgrupo de índice primo, p_1, de G. Além disso, G_1 é invariante em G, visto G ser comutativo. Procedendo para G_1 como se procedeu para G, é-se conduzido a um novo grupo G_2, subgrupo invariante de índice primo de G_1. E assim sucessivamente. Como as ordens de G, G_1, G_2,... vão sendo cada vez menores, chegar-se-á necessariamente, por este processo, ao grupo idêntico. E assim fica provado que G é resolúvel.

Ora, como vimos há pouco, a equação ciclotómica $\gamma(z) = 0$ tem por grupo de GALOIS a respeito de **Ra** um grupo cíclico de ordem $\leq p-1$. Então, atendendo ao que foi estabelecido no n.° 38, podemos finalmente concluir que:

Toda a raiz primitiva de índice primo p de unidade é exprimível por meio de radicais de índices primos inferiores a p, a partir do corpo racional.

Seja, por exemplo, a equação

$$\frac{z^7 - 1}{z - 1} \equiv z^6 + z^5 + \cdots + z + 1 = 0.$$

Recorrendo à teoria das equações recíprocas, vê-se imediatamente que esta equação é resolúvel a partir do corpo racional, mediante três radicais quadráticos e um radical cúbico, devidamente sobrepostos.

Seja ainda a equação

$$\frac{z^{17}-1}{z-1} \equiv z^{16}+z^{15}+\cdots+z+1\,.$$

Visto que um dos grupos admissíveis desta equação a respeito de **Ra** é um grupo cíclico de ordem $16(=2^4)$, segue-se que as suas raízes se podem obter, a partir de **Ra**, mediante 4 radicais quadráticos sobrepostos (o que implica a possibilidade de dividir a circunferência em 17 partes iguais por meio da régua e do compasso).

48. Critério geral de resolubilidade por meio de radicais

Já vimos que, se o grupo de GALOIS de uma dada equação $f(z)=0$ a respeito dum corpo Δ é resolúvel, então a equação é resolúvel por meio de radicais a respeito de Δ. Vamos agora demonstrar a proposição recíproca, isto é, vamos acabar de estabelecer o seguinte

TEOREMA – *Condição necessária e suficiente para que a equação* $f(z)=0$ *seja resolúvel por meio de radicais a respeito de* Δ, *é que o seu grupo de* GALOIS *a respeito de* Δ *seja resolúvel.*

Suponhamos pois que as raízes $\alpha_1, \alpha_2, \ldots, \alpha_n$ de $f(z)$ podem ser obtidas por meio de operações racionais e extrações de raiz efectuadas sobre elementos de Δ ou sobre resultados de tais operações. Podemos desde já supor que o índice de cada extracção de raiz é primo, pois que se tem

$$\sqrt[pq]{a} = \sqrt[p]{\sqrt[q]{a}}\,.$$

Nestas condições, é claro que as raízes $\alpha_1, \alpha_2, \ldots, \alpha_n$ poderão ser atingidas mediante uma cadeia de radicais

$$\sqrt[p_1]{a_1}\,,\ \sqrt[p_2]{a_2}\,,\ldots,\ \sqrt[p_r]{a_r}\,, \tag{24}$$

de índices primos e em que a_1 é um elemento do corpo Δ, a_2 um elemento do corpo obtido de Δ pela adjunção do primeiro radical, a_3 um elemento do corpo obtido de Δ pela adjunção dos dois primeiros

radicais, etc. Os $\alpha\alpha$ serão funções racionais, com os coeficientes em Δ, destes radicais.

Como vimos no número anterior, as raízes primitivas de índice p da unidade (sendo p um número primo) podem exprimir-se, a partir do corpo racional, mediante radicais de índices inferiores a p, isto é, *mediante uma cadeia de radicais do tipo* (24), *sendo agora* Δ *o corpo racional.* Imaginemos então escritos por ordem os radicais da cadeia correspondente a $p = 3$, em seguida os radicais da cadeia correspondente a $p = 5$, e assim por diante, segundo a sucessão dos números primos, até atingir o maior dos números $p_1, p_2, \ldots, p_r$. Depois destes radicais, imaginemos colocados na devida ordem os radicais da fila (24). Obtém-se deste modo uma cadeia de radicais

$$\sqrt[q_1]{b_1}, \sqrt[q_2]{b_2}, \ldots, \sqrt[q_s]{b_s}, \tag{25}$$

que verifica as seguintes condições: 1) os índices $q_1, q_2, \ldots, q_s$ são primos; 2) b_1 está contido no corpo Δ, enquanto $b_2, b_3, \ldots$ estão contidos, respectivamente, nos corpos que se obtêm de Δ pela adjunção do primeiro radical, dos dois primeiros radicais,...; 3) as raízes $\alpha_1, \alpha_2, \ldots, \alpha_n$ são funções racionais com coeficientes em Δ destes racionais, uma vez que o são a respeito dos radicais (24), incluídos em (25); 4) os radicais (25) estão dispostos numa ordem tal que após a adjunção dos radicais anteriores a um qualquer deles,

$$\sqrt[q_k]{b_k},$$

se obtém um corpo que contém as raízes primitivas de índice q_k da unidade.

Deste modo, em virtude do estabelecido no n.° 45, a equação

$$z^{q_k} - b_k = 0$$

será cíclica a respeito do corpo obtido de Δ pela adjunção dos $k-1$ primeiros radicais ($k = 1, 2, \ldots, s$).

Seja então G o grupo de GALOIS da equação $f(z) = 0$ a respeito de Δ. Segundo o teorema do n.° 46, a adjunção do primeiro radical (25) a Δ ou conserva G ou o reduz a um seu subgrupo invariante de

índice primo q_1. Por sua vez, a ulterior adjunção do segundo radical (25) ou não altera o grupo anterior ou o reduz a um seu subgrupo invariante de índice primo q_2. E assim sucessivamente. Visto que os $\alpha\alpha$ são funções racionais, com coeficientes em Δ, dos radicais (25), o último grupo a que se chega por esta via é, necessariamente, o grupo idêntico. É portanto possível passar de G para I por meio de uma cadeia de grupos, cada um dos quais é subgrupo invariante de índice primo do precedente. Logo G é um grupo resolúvel, q.e.d.

49. Equações com coeficientes variáveis

Até aqui temo-nos referido, sistematicamente, a equações com coeficientes numéricos. Ora a verdade é que o maior interesse reside nas equações algébricas cujos coeficientes são funções de uma ou mais variáveis independentes. Neste caso, as raízes não são números, mas sim funções, que é preciso definir de maneira conveniente, para que a teoria de GALOIS possa ser aplicada a tais equações. Consideremos em primeiro lugar uma equação em z

$$f(z,t) \equiv p_0(t)\,z^n + p_1(t)\,z^{n-1} + \cdots + p_n(t) = 0$$

cujos coeficientes, $p_n(t)$, $p_1(t), \ldots, p_n(t)$, sejam funções racionais de ums só variável t (complexa).

Suponhamos que o discriminante $D(t)$, desta equação não é identicamente nulo (caso contrário, a equação admitiria raízes múltiplas, qualquer que fosse t, e seria portanto possível substituí-la por equações cujo discriminante já não fosse identicamente nulo). Seja então c um valor da variável t que não anule o discriminante $D(t)$. Neste caso, as raízes $\alpha_1, \alpha_2, \ldots, \alpha_n$ da equação numérica

$$f(z,c) = 0,$$

são todas numericamente distintas, e portanto a função

$$f'_z(z,t) \equiv np_0(t)\,z^{n-1} + (n-1)\,p_1(t)\,z^{n-2} + \cdots + p_{n-1}(\mathrm{t})$$

não se anulará, quando se fizer $t = c$ e se substituir z por um qualquer dos números $\alpha_1, \alpha_2, \ldots, \alpha_n$ – de contrário o polinómio $f(z, c)$ e a sua derivada teriam pelo menos uma raiz comum, que seria raiz múltipla de $f(z, c)$.

Ora, o teorema das funções implícitas continua a ser válido para as funções deriváveis de uma ou mais variáveis complexas.(1) Podemos portanto afirmar que, no caso precedente, a equação $f(z, t) = 0$ define implicitamente, numa conveniente vizinhança de c, n funções contínuas de t

$$z_1 = \varphi_1(t),\ z_2 = \varphi_2(t), \ldots,\ z_n = \varphi_n(t),$$

as quais, para $t = c$, tomam respectivamente os valores $\alpha_1, \alpha_2, \ldots, \alpha_n$. Pois é precisamente a tais funções de t que chamaremos *raízes da equação* $f(z, t) = 0$, relativamente à incógnita z.

Analogamente se definem *raízes duma equação em* z

$$f(z, t_1, t_2, \ldots, t_m) = 0,$$

cujos coeficientes sejam funções racionais de m variáveis independentes $t_1, t_2, \ldots, t_m$. Neste caso, as raízes serão funções contínuas de $t_1, t_2, \ldots, t_m$ (as chamadas *funções algébricas*) definidas numa vizinhança dum ponto $(c_1, c_2, \ldots, c_n)$ no qual resulte diferente de zero o discriminante da equação.

Resta agora averiguar como se pode extender a tais equações a teoria de GALOIS. Para isso são necessárias as considerações do número seguinte.

50. Corpos de funções

O conceito de corpo, tal como o definimos no n.° 33, extende-se imediatamente a conjuntos de funções. Diremos que uma dada família Ω de funções (de uma ou mais variáveis) constitui um *corpo*,

---

(1) – Dizem-se analíticas tais funções. O seu estudo sistemático será feito na cadeira de Análise Superior.

quando for fechada a respeito das operações racionais e contiver mais de um elemento[1]. (No capítulo seguinte será dada uma definição geral de corpo, que engloba e precisa a actual definição).

Assim, por exemplo, o conjunto de todas as funções racionais de uma variável z é um corpo, e o mesmo podemos dizer, mais geralmente, a respeito do conjunto de todas as funções racionais de n variáveis $z_1, z_2, \ldots, z_n$.

A ideia de adjunção encontra também aqui a sua extensão imediata. Consideremos, por exemplo, um corpo Δ (corpo numérico ou corpo de funções) e uma variável independente, z; o corpo $\Delta(z)$, obtido pela adjunção de z a Δ, será manifestamente o conjunto de todas as funções racionais de z, de coeficientes em Δ (note-se que z é uma variável e não um número). Analogamente se pode considerar o corpo gerado pelas raízes duma equação algébrica cujos coeficientes sejam funções racionais de um ou mais parâmetros.

Para que a teoria de GALOIS se possa extender às equações algébricas com coeficientes situados num corpo de funções, é necessário ainda precisar o sentido que adquirem neste caso certas expressões atrás usadas. Consideremos uma equação algébrica $f(z) = 0$, cujos coeficientes sejam funções racionais de m variáveis $t_1, t_2, \ldots, t_m$; as raízes $z_1, z_2, \ldots, z_n$ desta equação são, como dissemos há pouco, determinadas funções de $t_1, t_2, \ldots, t_m$; então, dadas duas funções $\varphi(z_1, z_2, \ldots, z_n)$, $\psi(z_1, z_2, \ldots, z_n)$ das referidas raízes, diremos que tais funções são *formalmente iguais*, quando resultam idênticas, considerando $z_1, z_2, \ldots, z_n$ como variáveis independentes; e diremos que são *concretamente iguais*, quando, substituindo $z_1, z_2, \ldots, z_n$ pelos respectivos valores em função de $t_1, t_2, \ldots, t_m$, se obtém, a partir delas, funções idênticas de $t_1, t_2, \ldots, t_m$. (Aqui o termo "concretamente" substitui o termo "numericamente", atrás usado). É claro que duas funções das raízes formalmente iguais serão também concretamente iguais, mas a recíproca não é verdadeira. Seja, por exemplo, a equação recíproca

$$z^4 + az^3 + bz^2 + az + 1 = 0,$$

---

(1) – Supõe-se nesta definição que, exceptuada a função identicamente nula (elemento 0), todos os elementos de Ω admitem inverso.

cujas raízes (funções de *a, b*) podem ser designadas por z_1, z_2, z_3, z_4, de modo que se tenha $z_1 z_2 = 1$, $z_3 z_4 = 1$; neste caso, $z_1 z_2$ e $z_3 z_4$ são funções das raízes formalmente distintas, mas concretamente iguais.

Posto isto, diremos que uma dada função das raízes *pertence em sentido restrito* a um dado grupo G de substituições sobre essas raízes, quando: 1) a função é *formalmente* invariante para todas as substituições de G e só para essas; 2) as suas conjugadas em G são todas *concretamente* distintas.

Com estas premissas, toda a teoria de GALOIS, tal como a expusemos anteriormente, se pode extender, sem modificações substanciais, aos novos tipos de equações. Todavia, a legitimidade de tal extensão só pode ser estabelecida de modo inteiramente rigoroso, com os métodos modernos da Álgebra abstracta.

Em particular, a pesquisa do grupo de GALOIS conduz agora a problemas deste tipo:

Dada uma equação algébrica $f(z) = 0$ *cujos coeficientes sejam funções racionais com coeficientes racionais, de variáveis* $t_1, t_2, \ldots, t_m$, *determinar as suas raízes porventura existentes no corpo* $\mathbf{Ra}(t_1, t_2, \ldots, t_m)$ (*isto é, que sejam funções racionais, com coeficientes racionais, de* $t_1, t_2, \ldots, t_m$).

O problema resolve-se de modo análogo ao da pesquisa das raízes racionais duma equação de coeficientes racionais.

51. Equação geral de grau *n*

Chama-se *equação algébrica geral de grau n* a equação

$$f(z) \equiv z^n + a_1 z^{n-1} + a_2 z^{n-2} + \cdots + a_n = 0,$$

em que $a_1, a_2, \ldots, a_n$ são *variáveis independentes*. De acordo com o ponto de vista adoptado no número 49, as raízes $\zeta_1, \zeta_2, \ldots, \zeta_n$ desta equação são determinadas funções de $a_1, a_2, \ldots, a_n$.

Usemos agora os símbolos $z_1, z_2, \ldots, z_n$ como variáveis independentes. A equação que admite estas variáveis como raízes será

$$F(z) \equiv z^n - s_1 z^{n-1} + s_2 z^{n-2} - \cdots + (-1)^n s_n = 0,$$

em que

$$s_1 = \sum z_1,\ s_2 = \sum z_1 z_2, \ldots,\ s_n = z_1 z_2 \ldots z_n .$$

Note-se bem: na equação $f(z) = 0$ os coeficientes são variáveis independentes e as raízes variáveis dependentes, enquanto na equação $F(z) = 0$ sucede precisamente o contrário.

Propunhamo-nos determinar o grupo de GALOIS da equação $f(z) = 0$ a respeito do corpo $K(a_1, a_2, \ldots, a_n)$, constituído por todas as funções racionais, com coeficientes complexos, de $a_1, a_2, \ldots, a_n$. Seja então $\varphi(\zeta_1, \zeta_2, \ldots, \zeta_n)$ uma função racional das raízes desta equação cujo valor esteja situado no referido corpo, isto é, uma função tal que

$$\varphi(\zeta_1, \zeta_2, \ldots, \zeta_n) = \phi(a_1, a_2, \ldots, a_n)$$

em que ϕ designa uma função racional, com coeficientes numéricos determinados. Visto que $a_1, a_2, \ldots, a_n$ são variáveis independentes, podemos pôr $a_1 = -s_1$, $a_2 = s_2, \ldots, a_n = (-1)^n s_n$. Então virá: $\zeta_1 = z_1$, $\zeta_2 = z_2, \ldots, \zeta_n = z_n$, e portanto

$$\varphi(z_1, z_2, \ldots, z_n) = \phi(-s_1, s_2, \ldots, (-1)^n s_n) .$$

Ora o segundo membro desta igualdade é, por intermédio dos *ss*, uma função simétrica dos *zz*. Logo, o mesmo deve acontecer para o primeiro membro: φ é pois uma função simétrica.

Somos assim levados a concluir que as únicas funções racionais dos $\zeta\zeta$ cujo valor está contido no corpo $K(a_1, a_2, \ldots, a_n)$ são as funções simétricas. Ora, atendendo à definição do grupo de GALOIS, isto significa, precisamente, que:

O grupo de GALOIS *da equação geral de grau n a respeito do corpo* $K(a_1, a_2, \ldots, a_n)$ *é o grupo simétrico.*

52. O grupo S_n, para $n > 4$, não é resolúvel

A demonstração que vamos dar neste facto – notabilíssimo em toda a história da Matemática – é relativamente recente e muito mais simples do que as demonstrações anteriormente conhecidas.

Começaremos por estabelecer o seguinte:

Lema: Se um grupo G de substituições sobre n elementos (com $n > 4$) contém todos os ciclos de três elementos, e se H é um subgrupo invariante de G tal que G/H seja um grupo comutativo, então H contém também todos os ciclos de três elementos.

Demonstração:

Segundo as considerações do n.° 26, existe um homomorfismo T de G sobre o grupo cociente G/H. Ponhamos

$$\sigma = (ijk); \quad \theta = (krs)$$

em que i, j, k, r, s são cinco números arbitrários distintos entre si (o que é possível, visto ser $n > 4$). De acordo com a hipótese, σ, θ são elementos de G. Então, atendendo a que, G/H é comutativo e pondo $T(\sigma) = \overline{\sigma}$, $T(\theta) = \overline{\theta}$, virá

$$T(\sigma^{-1}\theta^{-1}\sigma\theta) = \overline{\sigma}^{-1}\overline{\theta}^{-1}\overline{\sigma}\overline{\theta} = I,$$

e portanto $\sigma^{-1}\theta^{-1}\sigma\theta \in H$, pois que o grupo H (núcleo do homomorfismo T) é constituído por todas as substituições de G que são transformadas por T na identidade de G/H. Mas

$$\sigma^{-1}\theta^{-1}\sigma\theta = (kji)\,(srk)\,(ijk)\,(krs) = (kjs).$$

Tem-se pois $(kjs) \in H$, sendo k, j, s três números arbitrários, distintos entre si – e é nisto, precisamente, que consiste a tese do Lema.

E agora é fácil demonstrar o teorema em questão. Suponhamos que o grupo S_n (com $n > 4$) é resolúvel; quer isto dizer que existe uma cadeia de grupos

$$S_n \supset G_1 \supset G_2 \supset \cdots \supset G_r \supset \mathcal{I},$$

cada um dos quais, a partir do segundo, é subgrupo invariante de índice primo do precedente. Mas, sendo assim, os grupos

$$S_n/G_1,\ G_1/G_2,\ \ldots,\ G_r/\mathscr{T}$$

serão todos de ordem prima, e portanto cíclicos, e portanto comutativos. Por outro lado, S_n, grupo total das substituições sobre n elementos, contém todos os ciclos ternários. Logo, em virtude do Lema, também G_1 conterá todos os ciclos ternários, e o mesmo acontecerá a respeito de G_2, de $G_3, \ldots$, de $\mathscr{T}$. Mas $\mathscr{T}$ é o grupo que se reduz à substituição I e, como tal, não contém nenhum ciclo de três elementos. Fomos assim conduzidos a um absurdo, supondo S_n resolúvel.

Este teorema, associado ao do n.° precedente, habilita-nos a concluir que:

A equação algébrica geral de grau n, para $n > 4$, não é resolúvel por meio de radicais a respeito do corpo constituído pelas funções racionais dos coeficientes.

Mas a equação geral de grau n é uma equação de coeficientes variáveis. Uma outra questão que se põe é a de saber se existem ou não equações algébricas com coeficientes *numéricos*, que não sejam resolúveis por meio de radicais a respeito do corpo gerado pelos coeficientes. Ora demonstra-se que, para cada valor de n, é possível construir infinitas equações algébricas de grau n, com coeficientes numéricos, cujo grupo de GALOIS a respeito do corpo gerado pelos coeficientes é o grupo gerado pelos coeficientes é o grupo simétrico. Pode mesmo dizer-se que o facto de o grupo de GALOIS de uma equação não ser o simétrico é um caso *excepcional*, do mesmo modo que é *excepcional* o facto de uma equação de coeficientes racionais (tomados ao arbitrio) ter raízes racionais.

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 $c_1, c_2, \ldots, c_m$ 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

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

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

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

considerando $\omega^0, \omega, \ldots, \omega^{n-1}$ 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)**