I.1

INTRODUÇÃO ÀS MODERNAS TEORIAS ALGÉBRICAS

(Apenas o esboço dum curso de iniciação)

Página em branco

CAPÍTULO 1

GENERALIDADES SOBRE CONJUNTOS E TRANSFORMAÇÕES

1. Noção geral de conjunto e as relações lógicas primitivas

Em Matemática a palavra "conjunto" é hoje usada na mais larga acepção possível, como sinónimo de "classe", "colecção" ou "família": um conjunto de números, um conjunto de pontos, um conjunto de figuras, um conjunto de funções, um conjunto de sinais, um conjunto de palavras, um conjunto de livros, etc, etc., são exemplos de conjuntos admissíveis em Matemática. Exige-se apenas que os elementos de cada conjunto sejam entidades bem definidas, com individualidade bem marcada: um conjunto de estados psicológicos, por exemplo, estaria fora das considerações matemáticas.

Todavia, na linguagem comum, a palavra "conjunto" é usada com menor elasticidade. Não se dirá, por exemplo, "o conjunto das aves", mas antes "a classe das aves"; não se dirá "o conjunto dos triângulos", mas sim "a classe ou a família dos triângulos", etc. Mas já parece indiferente dizer "o conjunto dos números primos" ou a "classe dos números primos". Mesmo na linguagem matemática se transige, por vezes, com o uso, para obter maior clareza e expressividade: assim, por exemplo, dir-se-á de preferência "família de conjuntos, em vez de "conjunto de conjuntos". Não esqueçamos todavia que, na Matemática moderna, os termos "conjunto", "classe", "família", etc., são considerados sinónimos.

Para indicar que um dado ente a é elemento dum dado conjunto C, escreveremos $a \in C$ (ler "a pertence a C"); para indicar que dois entes a e b são elementos de C, escreveremos $a, b \in C$ (ler "a e b pertencem a C"), etc. Em certos casos, o símbolo "$\in$" deverá ler-se "pertencente" ou "pertencentes", em vez de "pertence" ou "pertencem".

Por outro lado, a expressão simbólica $a \notin C$ significará que a *não pertence a* C.

Dados dois conjuntos A, B, diremos que A *está contido* em B, ou que A é um *subconjunto* de B, quando todo o elemento de A for também um elemento de B, e escreveremos então para o indicar: $A \subset B$. Nesta mesma hipótese diremos que B *contém* A ou que é um *sobreconjunto* de A, e escreveremos para o indicar $B \supset A$. Assim, por exemplo, se representarmos por M_6 o conjunto dos múltiplos de 6, e por M_3 o conjunto dos múltiplos de 3 (no conjunto dos inteiros) ter-se-á: $M_6 \subset M_3$ ou $M_3 \supset M_6$.

Pode acontecer, em particular, que se tenha ao mesmo tempo: $A \subset B$ e $B \supset A$; então é claro que as letras A e B representarão o *mesmo conjunto*. Também se diz, neste caso, que os conjuntos A e B *coincidem* ou *são idênticos*, e para o indicar, escreveremos: $A = B$ (na realidade trata-se de um só conjunto, representado de dois modos diversos). Assim, por exemplo, se designarmos por L_3 a classe dos triângulos equiláteros e por A_3 a classe dos triângulos equiângulos, poderemos escrever: $L_3 = A_3$.

De resto, o sinal "=" está hoje a ser empregue, sistematicamente, como um símbolo de *identidade*, devendo ler-se "*coincide com*", "*idêntico a*", "*o mesmo que*", etc.. Para indicar, por exemplo, que dois dados pontos geométricos a e b coincidem (ou, falando mais correctamente, para indicar que os símbolos a, b representam um *mesmo* ponto), escreveremos $a = b$; mas, para indicar que dois dados segmentos $\overline{ab}$ e $\overline{cd}$ são geometricamente iguais (isto é, *sobreponíveis*, ou, como também se diz, *congruentes*) não será lícito escrever $\overline{ab} = \overline{cd}$ a não ser que tais segmentos coincidam. (1)

---

(1) – Comummente, em Geometria Elementar, os pontos são designados por letras minúsculas do alfabeto latino e a relação de identidade ou coincidência é expressa pelo sinal "$\equiv$" reservando-se o sinal "=" para exprimir igualdade geométrica, (isto é, congruência). É, portanto, necessário ter presente esta diversidade de convenções, para evitar equívocos, ao ler um texto de matemática moderna.

Como vimos, entre os subconjuntos dum conjunto A, figura sempre o próprio conjunto A; isto é, tem-se $A \subset A$, qualquer que seja o conjunto A (*propriedade reflexiva da inclusão*).

Aos subconjuntos de A distintos de A dá-se o nome de *subconjuntos próprios* ou partes de A.[1]

Por outro lado, é evidente que, todas as vezes que se tiver $A \subset B$ e $B \subset C$ será também $A \subset C$ quaisquer que sejam os conjuntos A, B, C (*propriedade transitiva da inclusão*). É nesta propriedade que consiste o princípio dos silogismos da lógica formal.

2. Operações lógicas sobre conjuntos

Chama-se *intersecção* ou *produto lógico* de dois conjuntos A, B, e representa-se por $A \cap B$, o conjunto dos elementos comuns a A e a B, isto é, o *máximo* conjunto contido ao mesmo tempo em A e em B.

Chama-se *reunião* ou *soma lógica* de dois conjuntos A, B, e representa-se por $A \cup B$, o conjunto de todos os elementos de A e de B, isto é, o *mínimo* conjunto que contém ao mesmo tempo A e B.

Exemplos:

1) Representando em geral por M_n o conjunto dos múltiplos de n, ter-se-á

$$M_6 = M_3 \cap M_2 .$$

2) Representando por R, L, Q, respectivamente a classe dos retângulos, a classe dos losangos e a classe dos quadrados, será:

$$Q = R \cap L .$$

3) Representando por $[a\ ,\ b]$ o conjunto dos números reais x tais que $a \leq x \leq b$ (*intervalo fechado de extremos a, b*) podemos escrever:

---

(1) – Alguns autores escrevem $A \subseteq B$ (em vez de $A \subset B$) para indicar que A está *contido* em B, e $A \subset B$ para indicar que A é um subconjunto *próprio* de B.

$$[3\,,\,7] \cap [5\,,\,9] = [5\,,\,7],$$

$$[3\,,\,7] \cup [5\,,\,9] = [3\,,\,9].$$

De modo inteiramente análogo se define a intersecção ou reunião de mais de dois conjuntos *A, B, C,* ..., em número finito ou infinito; Dados n conjuntos $A_1, A_2, \ldots, A_n$ representaremos por

$$A_1 \cap A_2 \cap \ldots \cap A_n$$

ou, abreviadamente, por

$$\bigcap_{i=1}^{n} A_i$$

a intersecção desses conjuntos, e por

$$A_1 \cup A_2 \cup \ldots \cup A_n$$

ou por

$$\bigcup_{i=1}^{n} A_i$$

a reunião dos mesmos conjuntos.

3. Conjuntos formados dum só elemento e conjuntos de conjuntos

Observemos desde já que um conjunto finito pode sempre ser definido pela simples enumeração dos seus elementos, o que já não acontece, naturalmente, com os conjuntos infinitos.

Para indicar que um conjunto M é formado pelos elementos *a, b, c,...* escreveremos: $M = \{a, b, c, \ldots\}$; assim, por exemplo, designando por D_6 o conjunto dos divisores (positivos) de 6, ter-se-á $D_6 = \{1, 2, 3, 6\}$; quanto ao conjunto dos múltiplos de 6, M_6 seria $M_6 = \{0, 6, 12, \ldots, 6n, \ldots\}$, mas é claro que, sendo este um conjunto infinito, não é possível defini-lo, mencionando um por um, todos os seus elementos.

Consideremos o conjunto $U = \{a, b, c\}$. Entre os subconjuntos de U figuram, além de U, os seguintes conjuntos:

$$\{a, b\}, \{a, c\}, \{b, c\}$$

que designaremos respectivamente por A, B, C. Ora é preciso notar que, na linguagem matemática, ao contrário do que sucede na linguagem comum, é lícito falar de conjuntos formados de um só elemento. Assim, por exemplo, o conjunto U admitirá ainda os subconjuntos $\{a\}$, $\{b\}$, $\{c\}$, que é preciso não confundir com os próprios elementos a, b, c: não será portanto lícito escrever $a = \{a\}$.

Uma outra convenção a registar é a que se refere a conjuntos de conjuntos. Continuemos a referir-nos ao exemplo anterior: é claro que os subconjuntos de U podem agora ser combinados entre si de vários modos, dando origem a novos conjuntos, por exemplo, os seguintes: $\{A, B\}$, $\{A, B, C\}$, $\{A, B, \{a\}\}$, que designaremos respectivamente por $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$. Diz-se que tais conjuntos $\mathscr{A}$, $\mathscr{B}$,... são *de tipo* 2, a respeito de a, b, ..., para os distinguir dos conjuntos de elementos de U, chamados também conjuntos do tipo 1 (a respeito de a, b, c,...).

Importa não confundir uma dada família de conjuntos com a reunião dos conjuntos dessa família. Assim, por exemplo, a reunião dos intervalos [2 , 5], [3 , 7] e [4 , 9], coincide com a reunião dos intervalos [2 , 7] e [5 , 9], embora se trate de dois conjuntos diversos de intervalos. Analogamente, o conjunto das rectas do espaço que passam por um ponto p (estrela de rectas de centro p) e o conjunto de planos que passam por p (estrela de planos de centro p) são duas famílias distintas de pontos do espaço, e, contudo, a reunião dos conjuntos de cada uma dessas famílias coincide com o espaço inteiro.

Observemos finalmente que, assim como se podem considerar conjuntos de conjuntos de elementos a, b, c, ... (conjuntos de *tipo* 2, a respeito de a, b, c, ...) também se podem considerar conjuntos de conjuntos do tipo 2 (*conjuntos de tipo* 3), conjuntos de conjuntos de tipo 3 (chamados *conjuntos de tipo* 4) e assim sucessivamente, prosseguindo mesmo no transfinito. É esta a ideia fundamental da teoria dos tipos, criada por BERTRAND RUSSEL, com o objectivo de resolver os paradoxos da teoria dos conjuntos.

4. A noção de conjunto vazio

Consideremos, por exemplo, os intervalos [3 , 4] e [7 , 9]. Como não existe nenhum elemento comum a tais intervalos, poderíamos dizer que a sua intersecção não existe. Todavia, é corrente em Matemática introduzir entidades convencionais, para tornar possíveis certas operações em todos os casos que se apresentam, tendo em vista unicamente a comodidade de linguagem – e, quem diz comodidade de linguagem, diz comodidade de pensamento. Aparecem assim, por exemplo, os números negativos, os números imaginários, os expoentes negativos ou fraccionários, os pontos do infinito, etc... Foi assim, também que, ainda antes destes conceitos, apareceu o de número 0.

Pois bem, é ainda por tal processo, que se apresentam, na teoria dos conjuntos, os conjuntos formados de um só elemento (de que já falámos) e a noção de *conjunto vazio* ou *conjunto desprovido de elementos*. Diremos assim que a intersecção dos intervalos [3 , 4], e [7 , 9] é o conjunto vazio, para exprimir abreviadamente o facto de não existirem pontos comuns a [3 , 4] e a [7 , 9]. Analogamente; diremos que é vazia a classe dos triângulos birectângulos (na geometria euclideana), a classe dos números primos divisíveis por 6, a classe dos números positivos x tais que $x^2 + 7x + 2 = 0$, etc.

Quando a intersecção de dois conjuntos A, B é o conjunto vazio, diremos ainda que A, B são *disjuntos*.

É agora fácil reconhecer que, uma vez incluídos entre os *subconjuntos* de um conjunto finito A, os conjuntos formados de um só elemento, o conjunto vazio e o próprio conjunto A, o número total de subconjuntos de A será 2^n sendo n o número de elementos de A. Trata-se dum simples problema de análise combinatória:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = (1 + 1)^n = 2^n .$$

5. O conceito geral de transformação

Dados dois conjuntos A, B, quaisquer, diz-se definida uma *transformação unívoca* φ de A sobre B, quando se tenha fixado um critério, pelo qual fique a corresponder, a cada elemento x de A, um,

e um só, elemento y de B, chamado *imagem* ou *transformado* de x por meio de φ e representável por $\varphi(x)$:

$$y = \varphi(x).$$

Dir-se-á ainda, neste caso, que a variável y é uma função da variável x definida no conjunto A; e chamar-se-á *contradomínio* de φ ao conjunto de todos os elementos $\varphi(x)$ de B, transformados dos elementos x de A por meio de φ.

Dir-se-á ainda que φ é um *operador* (ou uma operação) definido em A e de *contradomínio* contido em B.

Uma dada transformação unívoca θ de A sobre B diz-se uma transformação *biunívoca* ou *reversível* de A sobre B, quando, para cada elemento y de B, exista um, e um só, elemento x de A, do qual y seja a imagem por meio de θ, isto é, tal que $\theta(x) = y$; em tal hipótese chamaremos *tranformação inversa* de θ, e representaremos por θ^{-1} a transformação que consiste em passar de y (dado arbitrariamente sobre B) para o correspondente valor de x em A:

$$x = \theta^{-1}(y).$$

Exemplos:

O conceito de "correspondência" ou de "função" reside na base de todo o pensamento. Por isso encontramos dele exemplo a cada passo, mesmo na linguagem comum.

Consideremos, por exemplo, a expressão "capital de..."; é claro que esta expressão, por si só, nada designa de concreto, mas, uma vez seguida do nome de um determinado país, ela passa a designar uma *determinada* cidade. Então, se representarmos por P o conjunto dos países e por C o conjunto das cidades, e se, além disso, escrevermos abreviadamente "y = cap x" com o significado de "y é a capital de x", podemos dizer que a variável y é uma *função unívoca* da variável x, função que tem por domínio de existência o conjunto P e por contradomínio um subconjunto de C. Por outras palavras: o símbolo "cap" representa uma transformação unívoca do conjunto P sobre o conjunto C, do mesmo modo que, por exemplo, o símbolo *sen* (abreviatura do "seno de") representa uma transformação unívoca do conjunto **R** dos números reais sobre si mesmo.

Todavia, o símbolo "cap" não representa, nesta ordem de ideias, uma transformação biunívoca de P sobre C, visto que há cidades que não são capitais de nenhum país; mas, se representarmos por C^* o conjunto das cidades que são *capitais* (sendo então C^* o contradomínio da função "cap de x") já podemos dizer que se trata duma transformação biunívoca[1] de P sobre C^* (pois não pode haver mais de um país com a mesma capital) e a sua transformação inversa será então aquela indicada pela expressão: "x é o país cuja capital é y".

Por sua vez, o operador *sen* é uma transformação unívoca, mas não reversível, do conjunto dos números reais sobre o intervalo fechado [–1, 1] (contradomínio desse operador); ele define, contudo, uma transformação biunívoca do intervalo $[-\pi/2, \pi/2]$, sobre o intervalo [–1, 1], e a sua transformação inversa será então o operador *arc sen*.

Consideremos agora a expressão "múltiplo de"; seguida do nome dum número, esta expressão passa a designar, não um número determinado, mas sim toda uma classe de números dependente do primeiro. Diremos então que se trata de um *operador plurívoco* com infinitos *ramos unívocos*, que são, por exemplo, os operadores: "dobro de", "triplo de", etc.

Passemos à geometria. A projecção dos pontos do espaço euclideano, que representaremos por $\mathbf{R}_3$, sobre um plano α paralelamente uma direcção d (não paralela a α) é um exemplo de transformação unívoca, mas não reversível, de $\mathbf{R}_3$ sobre α.

Exemplos notáveis de transformações biunívocas do espaço $\mathbf{R}_3$ sobre si mesmo são as *homotetias*, as *translacções*, as *rotações*, e as *simetrias*:

1) Fixados ao arbítrio, um ponto c e um número real r (positivo ou negativo) chama-se *homotetia de centro c e de razão r* a operação geométrica θ que, deixando fixo o ponto c, transforma cada ponto p do espaço, distinto de c no ponto p^* tal que $\overline{cp^*}/\overline{cp} = |r|$ ficando p e p^* do mesmo lado ou do lado oposto em relação a c conforme a razão r for positiva ou negativa. O facto de se ter $\theta(c) = c$ exprime-se

---

(1) – Diz-se que uma transformação unívoca θ (de A sobre B) é *univalente* quando se tem $\theta(x_1) \neq \theta(x_2)$, para $x_1 \neq x_2$. Supondo verificada esta hipótese e representando por B^* o contradomínio de θ esta será uma transformação biunívoca de A sobre B, se, e só se, for $B^* = B$.

dizendo que o ponto c é *invariante* para θ. É claro que será esse o único ponto invariante se $r \neq 1$; mas, se $r = 1$ todos os pontos serão invariantes, e então dir-se-á que θ é a transformação *idêntica* ou *identidade*.

É fácil ver ainda que a transformação inversa da homotetia de centro c e razão r é, precisamente, a homotetia de centro c e razão $1/r$.

2) Fixados dois pontos quaisquer a, a^* de $\mathbf{R}_3$ chama-se translacção definida pelo vector $\overrightarrow{aa^*}$ a operação θ que consiste em passar de cada ponto p do espaço, para o ponto p^* tal que

$$\overrightarrow{pp^*} = \overrightarrow{aa^*}.$$

É claro que θ se reduz à identidade se, e só se, for $c^* = c$. Por outro lado, é fácil ver que a transformação inversa da translacção definida por $\overrightarrow{cc^*}$ é a translacção definida por $\overrightarrow{cc^*}$.

3) Sendo E uma recta qualquer orientada e φ um ângulo dado, positivo ou negativo, chama-se *rotação* de eixo E e de amplitude φ, a transformação θ que deixa invariantes os pontos de E e faz corresponder a cada ponto $p \in E$ o ponto p^*, tal que, designando por π o plano conduzido por p perpendicularmente a E e por c o ponto de intersecção de π com E, resultam verificadas as três condições:

$$p^* \in \pi;$$

$$\text{dist}\,(p, c) = \text{dist}\,(p^*, c);$$

$$\text{ang}\,(p^*\,\hat{c}\,p) = \varphi$$

(considerando como sentido positivo dos ângulos o sentido antihorário, a respeito de um observador colocado segundo a recta orientada E).

A transformação inversa da rotação de eixo E e de amplitude φ será manifestamente a rotação do eixo E e amplitude $-\varphi$.

4) As simetrias podem ser de três espécies: em relação a um ponto, em relação a uma recta e em relação a um plano. As definições destes tipos de operadores são bem conhecidas.

É curioso observar que a transformação inversa duma dada simetria é essa mesma simetria. Por outro lado, é de notar que a transformação idêntica pertence à classe das homotetias, à classe das translacções e à classe das rotações (constitui mesmo a intersecção dessas classes), mas não pertence à classe das simetrias.

6. Transformações entre conjuntos finitos

Já atrás observámos que todo o conjunto finito pode ser definido (pelo menos teoricamente) pela simples indicação dos elementos que o constituem. Analogamente, dados dois conjuntos finitos A, B, toda a transformação unívoca θ de A sobre B se poderá definir, indicando quais os elementos de B que correspondem, segundo θ nos diversos elementos de A, mencionados um por um, sem omissão: tal é por exemplo, o caso do operador "capital de" atrás considerado, definido entre o conjunto dos países e o conjunto das cidades.

Consideremos, para assentar ideias, o conjunto

$$A = \{a, b, c, d\}.$$

Se, por exemplo, fizermos corresponder ao elemento a o elemento b, ao elemento b o elemento c, ao elemento c o próprio c e ao elemento d o elemento a, ficará definida uma transformação unívoca do conjunto A sobre si mesmo. Designando por θ esta transformação, ter-se-á, em símbolos:

$$\theta(a) = b,\ \theta(b) = c,\ \theta(c) = c,\ \theta(d) = a\ .$$

A definição deste operador poderá ainda ser esquematizada na seguinte tabela:

$y = \theta(x)$

x	y
a	b
b	c
c	c
d	a

na qual, como se vê, estão escritos à esquerda os elementos de A (isto é, os dados ou valores da variável independente, x) e à direita, na mesma linha, os elementos de B que correspondem ordenadamente aos primeiros (isto é, os resultados ou valores da variável dependente, y). É claro que o uso das tabelas está indicado sobretudo para os casos em que seja muito grande (embora finito) o número dos valores da variável independente; tal é por exemplo, o que acontece a respeito das tabelas numéricas[1]. Quando, porém, é pouco numeroso o conjunto dos dados, costuma usar-se esta outra convenção: dispõem-se os dados numa linha horizontal e, por cima de cada um deles, o respectivo resultado; encerra-se depois o conjunto das duas linhas num parêntese: o símbolo composto assim obtido designa, por convenção, o operador definido.

Assim, por exemplo, para o operador θ, que estávamos considerando, ter-se-á

$$\theta = \begin{pmatrix} b & c & c & a \\ a & b & c & d \end{pmatrix}.$$

Observemos ainda que esta transformação deixa fixo (ou invariante) o elemento c. Além disso, θ não é uma transformação reversível, pois que se tem

$$\theta(b) = \theta(c), \text{ sendo } b \neq c\ .$$

Uma transformação biunívoca do mesmo conjunto A sobre si mesmo é, por exemplo, a seguinte:

$$\varphi = \begin{pmatrix} c & a & d & b \\ a & b & c & d \end{pmatrix},$$

cuja transformação inversa é, como facilmente se reconhece,

$$\varphi^{-1} = \begin{pmatrix} b & d & a & c \\ a & b & c & d \end{pmatrix},$$

tendo-se, portanto,

$$\varphi \neq \varphi^{-1}.$$

---

(1) – Estas tabelas (como, por exemplo, uma tábua de senos) referem–se geralmente a uma função real de variável real, x. Todavia, na prática, basta conhecer o valor da função para um número finito de valores de x.

As transformações biunívocas dum conjunto finito sobre si mesmo costumam aparecer na literatura matemática com o nome de *substituições*.

Segundo a convenção precedente, o símbolo

$$\begin{pmatrix} a_{i_1} & a_{i_2} & \cdots & a_{i_n} \\ a_1 & a_2 & \cdots & a_n \end{pmatrix},$$

em que $a_{i_1}, a_{i_2}, \ldots, a_{i_n}$ representam os elementos $a_1, a_2, \ldots, a_n$ dispostos numa ordem qualquer, sem omissão nem repetição, designará uma determinada substituição σ sobre os n elementos $a_1, a_2, \ldots, a_n$. Esta substituição não depende porém da ordem das colunas daquele símbolo: basta que, por cima de cada elemento, esteja indicado o respectivo transformado por meio de σ. Torna-se então manifesto que o número total das possíveis substituições sobre n elementos é precisamente igual ao número das permutações[1] desses n elementos ou seja $n!$.

Neste número está incluída a substituição idêntica ou identidade:

$$I = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}.$$

Discorrendo de modo análogo, chega-se à conclusão de que o número total de transformações unívocas (reversíveis ou não) dum conjunto de n elementos sobre si mesmo é igual ao número de arranjos com repetição de n objectos n a n, ou seja, como ensina a análise combinatória, n^n.

7. Produto de duas transformações

Consideremos três conjuntos A, B, C quaisquer e sejam: θ_1 uma transformação unívoca de B sobre C, θ_2 uma transformação unívoca de A sobre B. A cada elemento x de A, fará o operador θ_2 corresponder um determinado elemento y de B; por sua vez, ao elemento y de B, fará o operador θ_1 corresponder um determinado elemento z de C.

---

(1) – Alguns autores usam mesmo o termo "permutação" como sinónimo de "substituição".

Será então $y = \theta_2(x)$, $z = \theta_1(y) = \theta_1(\theta_2(x))$. É claro que, se fizermos corresponder directamente ao elemento x de A, o elemento z de C, ficará definida uma transformação unívoca de A sobre C. Designemos por θ essa transformação; diz-se então que θ é o produto de θ_1 por θ_2 e escreve-se $\theta = \theta_1 \cdot \theta_2$.

Ter-se-á, pois, por definição,

$$(\theta_1\ \theta_2)(x) = \theta_1(\theta_2(x)), \text{ para cada } x \in A.$$

Exemplos:

1) Designemos por *P, C, N,* respectivamente o conjunto dos países, o conjunto das cidades e o conjunto dos números naturais. Já no n.° 5 vimos que a expressão "capital de" representa uma transformação unívoca de *P* sobre *C*. Por sua vez, a expressão "número de habitantes de" representa uma transformação unívoca de *C* sobre *N* (e também de *P* sobre *N*). Seja então x um elemento qualquer de *P*; se aplicarmos sobre x o operador "capital de" e em seguida o operador "número de habitantes de", obter-se-á um determinado elemento de *N*, função de x: o *número de habitantes da capital de x.* Ficará assim definida, portanto, uma transformação unívoca de *P* sobre *N*, que será o produto do operador "número de habitantes de" pelo operador "capital de".

2) Consideremos o conjunto $A = \{a, b, c, d\}$ e as duas seguintes transformações de *A* sobre si mesmo

$$\theta_1 = \begin{pmatrix} b & d & a & b \\ a & b & c & d \end{pmatrix}, \quad \theta_2 = \begin{pmatrix} d & a & b & c \\ a & b & c & d \end{pmatrix}.$$

Será então

$$\theta_1\theta_2 = \begin{pmatrix} b & b & d & a \\ a & b & c & d \end{pmatrix},$$

pois que se tem: $\theta_2(a) = d$, $\theta_1(d) = b$, donde, $\theta_1(\theta_2(a)) = b$, $\theta_2(b) = a$, $\theta_1(a) = b$, donde $\theta_1(\theta_2(b)) = b$, etc.

Por outro lado será:

$$\theta_2\theta_1 = \begin{pmatrix} a\ c\ d\ a \\ a\ b\ c\ d \end{pmatrix},$$

e portanto $\theta_1\theta_2 \neq \theta_2\theta_1$.

Este simples exemplo mostra que a *lei comutativa não é aplicável ao produto de transformações*. Todavia, dados dois operadores σ, θ, pode acontecer que se tenha $\sigma\theta = \theta\sigma$; diz-se então que σ e θ são *permutáveis*. Tais são, por exemplo, os operadores

$$\sigma = \begin{pmatrix} c\ d\ b\ a \\ a\ b\ c\ d \end{pmatrix}, \quad \theta = \begin{pmatrix} b\ a\ d\ c \\ a\ b\ c\ d \end{pmatrix}.$$

3) Consideremos as funções $\varphi(x) \equiv x^3$ e $\psi(x) \equiv x-1$. Elas *definem* manifestamente transformações unívocas do conjunto dos números reais (e também do conjunto dos números complexos) sobre si mesmo. Trata-se, de resto, de duas operações elementares: a *elevação ao cubo* e a *subtracção duma unidade*.

Ter-se-á então:

$$\varphi(\psi(x)) \equiv (x-1)^3$$

$$\psi(\varphi(x)) \equiv x^3-1$$

e portanto, $\varphi\psi \neq \psi\varphi$. As duas operações consideradas não são pois permutáveis.

Sejam agora as duas seguintes transformações:

$$\varphi(x) \equiv x^2 \ , \ \psi(x) \equiv \sqrt[3]{x}$$

(*elevação ao quadrado* e *extracção da raiz cúbica*).

Ter-se-á neste caso:

$$(\varphi\psi)(x) \equiv \sqrt[3]{x^2}, \ (\psi\varphi)(x) \equiv (\sqrt[3]{x})^2$$

e, portanto,

$$\varphi\psi = \psi\varphi.$$

4) Sejam θ_1, θ_2 duas homotetias de centro c e de razões, respectivamente, r_1 e r_2. É fácil ver que o produto $\theta_1\theta_2$ é precisamente a homotetia de centro c e de razão $r_1 r_2$; ter-se-á, portanto $\theta_1\theta_2 = \theta_2\theta_1$. Em particular, se for $r_1 = r_2^{-1}$ (isto é, se for $\theta_1 = \theta_2^{-1}$), será $\theta_1\theta_2$ a transformação idêntica.

Sejam agora θ_1, θ_2 duas homotetias, respectivamente de centros c_1, c_2 (com $c_1 \neq c_2$) e de razões r_1, r_2. Se $r_1 \neq r_2^{-1}$, é fácil ver que o produto $\theta_1\theta_2$ é uma homotetia de razão $r_1 r_2$, cujo centro c é uma determinada função de c_1 e c_2; mas ter-se-á então, geralmente, $\theta_1\theta_2 \neq \theta_2\theta_1$. Se $r_1 = r_2^{-1}$, o produto $\theta_1\theta_2$ será uma translacção e ter-se-á ainda $\theta_1\theta_2 \neq \theta_2\theta_1$.

8. Propriedades gerais dos produtos de transformações

Já vimos no número precedente que a multiplicação definida entre operadores não é uma operação comutativa, dizendo-se que: dois operadores φ, ψ são *permutáveis*, quando se tem, excepcionalmente, $\varphi\psi = \psi\varphi$. Todavia, vamos ver que a referida multiplicação goza da propriedade associativa, isto é, que se tem

$$(\theta_1\theta_2)\,\theta_3 = \theta_1\,(\theta_2\theta_3),$$

quaisquer que sejam os operadores θ_1, θ_2, θ_3 desde que os produtos considerados tenham sentido. Para fixar ideias, suponhamos que θ_1, θ_2, θ_3 são transformações unívocas dum *conjunto A sobre si mesmo* (no caso geral a demonstração é análoga). Se fizermos $\sigma_1 = \theta_1\theta_2$, será, por definição de produto,

$$\sigma_1(x) = \theta_1(\theta_2(x)) \quad \text{(para cada } x \in A),$$

donde, substituindo x por $\theta_3(x)$,

$$\sigma_1(\theta_3(x)) = \theta_1(\theta_2(\theta_3(x))), \quad \text{(para cada } x \in A),$$

ou, ainda, substituindo σ_1 por $\theta_1\,\theta_2$:

(1) $\qquad ((\theta_1\,\theta_2)\,\theta_3)(x) = \theta_1(\theta_2(\theta_3(x))), \quad$ para cada $x \in A$.

Por outro lado, se pusermos $\sigma_2 = \theta_2 \theta_3$, virá:

$$\sigma_2(x) = \theta_2(\theta_3(x)), \quad (\theta_1 \sigma_2)(x) = \theta_1(\sigma_2(x)),$$

para cada $x \in A$, ou seja

$$(\theta_1(\theta_2 \theta_3)(x) = \theta_1(\theta_2 (\theta_3(x))),$$

para cada $x \in A$, donde, por comparação com (1),

$$(\theta_1 \theta_2)\, \theta_3 = \theta_1(\theta_2 \theta_3) \quad \text{q.e.d.}$$

Podemos então escrever simplesmente $\theta_1\, \theta_2\, \theta_3$ em vez de $(\theta_1 \theta_2)\, \theta_3$ ou de $\theta_1(\theta_2 \theta_3)$ e dizer que $\theta_1 \theta_2 \theta_3$ é o produto dos três operadores $\theta_1, \theta_2, \theta_3$ na ordem em que estão escritos. Analogamente se definem produtos de quatro operadores, cinco operadores, etc.

Já atrás foi dito que se chama transformação idêntica ou identidade, e se representa por I, a transformação que faz corresponder a cada elemento x o mesmo elemento x; isto é, em símbolos: $I(x) \equiv x$.

Ora é fácil ver que se tem

$$I\,\theta = \theta\, I = \theta$$

qualquer que seja a transformação θ.

Seja agora σ uma transformação *biunívoca* do conjunto A sobre si mesmo. Imediatamente se reconhece que

$$\sigma \sigma^{-1} = \sigma^{-1} \sigma = I.$$

Este resultado permite-nos resolver o seguinte problema: dadas duas transformações unívocas σ, θ do conjunto A sobre si mesmo, das quais a segunda seja reversível, determinar uma terceira transformação ξ tal que

$$\xi \theta = \sigma \tag{2}$$

ou uma transformação η tal que

$$\theta \eta = \sigma.$$

No primeiro caso, multiplicando ambos os membros de (2) por θ^{-1}, *à direita,* virá

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

e dir-se-á que $\sigma\,\theta^{-1}$ é o *cociente da divisão à direita* de σ por θ. Discorrendo analogamente no segundo caso, virá

$$\eta = \theta^{-1}\sigma$$

e dir-se-à que $\theta^{-1}\sigma$ é o *cociente da divisão à esquerda* de σ por θ. Pode reconhecer-se, por substituição directa, que tais valores de ξ e η verificam, de facto, as referidas equações.

Apresentam-se, pois, duas modalidades de divisão (divisão *à direita* e divisão *à esquerda*), em consequência da não comutatividade da multiplicação.

Convém tomar ainda nota do seguinte teorema:

O produto de duas transformações reversíveis σ, θ *é ainda, uma transformação reversível, tendo-se, precisamente,*

$$(\sigma\,\theta)^{-1} = \theta^{-1}\,\sigma^{-1}.$$

Demonstração: Sejam σ uma transformação biunívoca dum conjunto A sobre um conjunto B e θ uma transformação biunívoca de B sobre um outro conjunto C (em participar pode ser $A = B = C$). Poderemos então afirmar que, a cada elemento z de C corresponderá, *um e um só* elemento x de A tal que $z = (\sigma\,\theta)(x)$. Tem-se, com efeito, sucessivamente: $z = \sigma\,(\theta\,(x))$, $\sigma^{-1}(z) = \theta\,(x)$, $\theta^{-1}\,(\sigma^{-1}\,(z)) = x$, $(\theta^{-1}\,\sigma^{-1})\,(z) = x$. Pode agora verificar-se directamente que $(\theta^{-1}\,\sigma^{-1})$ $(\sigma\,\theta) = I$ e portanto

$$(\sigma\,\theta)^{-1} = \theta^{-1}\,\sigma^{-1}, \quad \text{q.e.d.}$$

Este resultado é generalizável a qualquer número de factores:

$$(\sigma_1\,\sigma_2\,\cdots\,\sigma_n)^{-1} = \sigma_n^{-1}\,\sigma_{n-1}^{-1}\,\cdots\,\sigma_1^{-1}.$$

Uma sua consequência imediata é que, para todo o operador reversível θ, virá

$$(\theta^{-1})^n = (\theta^n)^{-1}.$$

9. Potências dum operador

Do anterior conceito de multiplicação, deriva um natural conceito de *potência* θ^n *dum operador* θ (com $n > 1$). Será, por definição:

$$\theta^n = \theta \cdot \theta \cdot \cdots \cdot \theta \quad (n \text{ vezes}).$$

Seja, por exemplo, a função $\varphi(x) \equiv \sqrt{1-x}$; ter-se-á então

$$\varphi^2(x) \equiv \sqrt{1-\sqrt{1-x}}\,; \quad \varphi^3(x) \equiv \sqrt{1-\sqrt{1-\sqrt{1-x}}}$$

etc.

É ainda natural, dizer que a potência de expoente 1 dum operador θ é o próprio operador θ; isto é, em símbolos: $\theta^1 = \theta$, qualquer que seja θ. Por outro lado, convenciona-se dizer que a potência de expoente 0 dum operador θ é a identidade; ou seja, em símbolos: $\theta^0 = I$, qualquer que seja θ.

Estas definições podem condensar-se no seguinte esquema de recorrência:

$$\sigma^0 = I, \quad \sigma^{n+1} = \sigma \cdot \sigma^n.$$

Podemos agora estender, ao novo conceito de potência, a propriedade do produto de potências da mesma base.

Ter-se-á, com efeito:

$$\sigma^m \cdot \sigma^n = \underset{m \text{ vezes}}{(\sigma\sigma \cdots \sigma)} \; \underset{n \text{ vezes}}{(\sigma\sigma \cdots \sigma)},$$

donde, pela associatividade da multiplicação:

$$\sigma^m \sigma^n = \sigma^{m+n}.$$

Daqui se deduzem imediatamente os seguintes corolários:

I – Duas potências quaisquer dum mesmo operador são sempre operadores permutáveis entre si.

II – Quaisquer que sejam os números naturais *m, n*, tem-se $(\sigma^m)^n = \sigma^{mn}$ – em que σ representa uma qualquer transformação unívoca dum conjunto *A* sobre si mesmo.

Todavia a conhecida regra do *produto de potências do mesmo expoente*:

$$\sigma^m \cdot \theta^m = (\sigma\theta)^m,$$

só é agora válida no caso em que σ e θ são operadores permutáveis.

Notemos ainda que, para os operadores reversíveis, podemos definir de maneira natural *potência de expoente negativo*. Bastará pôr

$$\sigma^{-n} = (\sigma^{-1})^n,$$

sendo σ um qualquer operador reversível e *n* um número natural. É fácil ver que as anteriores propriedades são ainda generalizáveis ao novo conceito de potência.

10. Período duma transformação

Se representarmos por σ a rotação de 120° em torno dum determinado eixo *E*, é claro que σ^2 será a rotação de 240° em torno de *E* e σ^3 será a identidade, isto é, $\sigma^3 = I$. Dum modo geral, toda a rotação que tenha por amplitude uma fracção *p/q* da circunferência (com *p, q* inteiros), reproduz a identidade quando elevada ao expoente *q*. Pelo contrário, se a amplitude duma rotação σ tiver medida irracional em graus, será sempre $\sigma^n \neq I$, para todo o expoente inteiro *n*, positivo ou negativo.

Ora bem, diz-se que uma transformação reversível θ tem *período finito*, quando existe pelo menos um número inteiro $m > 0$ tal que $\theta^m = I$; em tal hipótese, chama-se *período* de θ ao menor número inteiro $m > 0$ que satisfaz àquela condição. No caso contrário, diz-se que θ tem *período infinito*.

Voltando ao exemplo anterior, vê-se imediatamente que o período duma rotação que tenha por amplitude a fracção p/q de circunferência, com p e q *primos entre si*, é precisamente igual ao denominador q. É também fácil verificar que: a) toda a translação distinta de I tem período infinito; b) a transformação $\varphi(x) \equiv \sqrt[3]{1-x}$ tem período infinito; c) a transformação

$$\theta(x) \equiv \frac{-\sqrt{3}\,x - 1}{x - \sqrt{3}}$$

tem período 6, etc., etc.

Podemos agora demonstrar o seguinte teorema:

Dada uma transformação reversível θ *de período finito, condição necessária e suficiente para que se tenha* $\theta^m = I$, *com m inteiro e positivo, é que m seja um múltiplo do período de* θ.

Que a condição é suficiente, não oferece dúvidas. Suponhamos então que se tem $\theta^m = I$, com m inteiro e positivo e seja n o período do operador θ. Representando por q e por r, respectivamente, o cociente e o resto da divisão de m por n, virá:

$$\theta^m = \theta^{qn+r} = I, \text{ com } r < n$$

ou seja, atendendo às propriedades das potências (n.º 9):

$$(\theta^n)^q \cdot \theta^r = I,$$

ou ainda, visto ser, por hipótese, $\theta^n = I$:

$$\theta^r = I.$$

Mas, como se tem $r < n$, e visto que n é, por hipótese, o *menor* inteiro positivo tal que $\theta^n = I$, segue-se que $r = 0$ e que, portanto, m é multiplo de n, q.e.d.

Notemos ainda que se for θ uma transformação reversível de período finito n, será

$$\theta^{n-1} = \theta^n \,.\, \theta^{-1} = \theta^{-1}.$$

Tem-se pois que: *A transformação inversa duma transformação reversível de período finito é igual a uma potência de expoente positivo dessa transformação.*

Em particular: *Condição necessária e suficiente para que uma transformação reversível tenha período 2 é que coincida com a sua inversa.* Estão neste caso as simetrias, a transformação $y = 1 - x$, etc., etc.

Seja agora A um conjunto qualquer formado de n elementos, e seja q uma transformação biunívoca de A sobre si mesmo. Visto que o número total de substituições sobre n elementos é finito e igual, precisamente a $n!$ (n.º 6), segue-se que as substituições $\theta, \theta^2, \ldots, \theta^n, \ldots$ não podem ser todas distintas entre si. Haverá, pois, pelo menos, dois expoentes n_1, n_2, com $n_1 > n_2$ para os quais se tenha

$$\theta^{n_1} = \theta^{n_2}.$$

Mas daqui resulta, multiplicando ambos os membros por θ^{-n_2}

$$\theta^{n_1} \cdot \theta^{-n_2} = \theta^{n_1 - n_2}$$

ou seja

$$\theta^{n_1 - n_2} = I$$

e, como $n_1 - n_2$ é um inteiro positivo maior que 0, segue-se que θ é uma transformação de período finito.

Tem-se, pois, o seguinte resultado:

Toda a transformação biunívoca dum conjunto finito em si mesmo tem período finito.

Em particular: *A transformação inversa duma substituição σ é sempre igual a uma potência de expoente positivo de σ.*

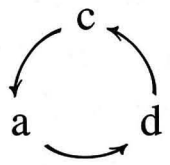
11. Substituições cíclicas

Diz-se que uma substituição σ é *cíclica*, ou que é um *ciclo*, quando os elementos que ela *muda* podem ser dispostos numa ordem

circular tal que cada um desses elementos seja o transformado do precedente por meio de σ. Seja por exemplo, a substituição:

$$\sigma = \begin{pmatrix} d\ b\ a\ c \\ a\ b\ c\ d \end{pmatrix}.$$

Tem-se $\sigma(a) = d$, $\sigma(d) = c$, $\sigma(c) = a$; o elemento b é invariante. A substituição é portanto cíclica e a ordem circular a que se refere a definição é a indicada pelo seguinte esquema



Costuma então representar-se mais concisamente pelo símbolo

$$(a\ d\ c)$$

uma tal substituição.

É claro que nem todas as substituições são cíclicas. Consideremos, por exemplo, a substituição

$$\theta = \begin{pmatrix} e\ f\ c\ a\ d\ b \\ a\ b\ c\ d\ e\ f \end{pmatrix}.$$

Partindo do elemento a, virá sucessivamente: $\theta(a) = e$, $\theta(e) = d$, $\theta(d) = a$. Fica, assim, gerado o ciclo $\sigma_1 = (a\ e\ d)$. Mas é claro que não se tem $\theta = \sigma_1$, pois que, por exemplo, o elemento b ainda é alterado por σ. Partindo agora de b, virá $\theta(b) = f$, $\theta(f) = b$, fechando-se deste modo, um segundo ciclo $\sigma_2 = (b\ f)$. E como c é invariante, podemos escrever finalmente

$$\theta = (a\ e\ d)\ (b\ f).$$

Seja agora θ uma substituição qualquer. Discorrendo de modo análogo, chega-se à conclusão de que será em geral:

$$\theta = \sigma_1 \sigma_2 \cdots \sigma_r,$$

em que σ_1, σ_2, ..., σ_r, designam ciclos sem elementos comuns (podendo ser $r = 1$).

Podemos assentar no seguinte resultado:

Toda a substituição θ *distinta de I é decomponível, e dum só modo, num produto de substituições cíclicas sobre conjuntos disjuntos dois a dois.*

Esta teorema apresenta analogias com o da decomposição dos números naturais em produtos de factores primos.

Observemos ainda que o *período duma substituição cíclica é precisamente igual ao número de elementos que ela muda.*

Chamam-se *transposições* os ciclos de período 2.

12. Conceito de grupo de transformações

Consideremos um conjunto *A* qualquer, finito ou infinito, e seja *H* uma família não *vazia* de transformações *biunívocas* do conjunto *A* sobre si mesmo. Diz-se que a família *H* constitui um *grupo*, quando verifica as duas seguintes condições: 1) dadas duas quaisquer transformações σ, θ, (distintas ou idênticas) pertencentes a *H* também o produto $\sigma\,\theta$ pertence a *H*; 2) a transformação inversa de toda a transformação pertencente a *H* é ainda um elemento de *H*.

Assim, por exemplo, a família das translações do espaço constitui um grupo, visto que o produto de duas translações é ainda uma translação e a transformação inversa duma translação é também uma translação. Analogamente, é um grupo o conjunto das rotações em torno dum mesmo eixo *E*. Mas já não é um grupo o conjunto de todas as rotações possíveis, porque o produto de duas rotações em torno de eixos não complanares não é uma rotação.

Nestes exemplos, os grupos citados são *infinitos*, (ou de *ordem infinita*) isto é, formados de infinitas transformações. Mas, seja, por exemplo, ρ a rotação de 60° em torno dum determinado eixo *E*; é claro que as transformações ρ, ρ^2, ρ^3, ρ^4, ρ^5, $\rho^6 = I$ formam um grupo finito, de ordem 6 (isto é, constituído por seis elementos), que é um *subgrupo* do grupo (infinito) de todas as rotações em torno de *E*.

Chama-se pois *ordem* dum grupo o número dos seus elementos.

Exemplo trivial dum grupo é o grupo $\mathscr{T}$ constituído pela identidade: $\mathscr{T} = \{I\}$.

Um grupo diz-se *comutativo* ou *abeliano*, quando nele é válida a lei comutativa da multiplicação.

Como consequência imediata da definição de "grupo", tem-se que:

a) *Todo o grupo contém a identidade.*

b) *Se* θ *é um elemento dum grupo G, qualquer potência de* θ *é ainda um elemento de G.*

Note-se ainda de passagem *como o conjunto de todas as potências (positivas e negativas) duma mesma transformação* θ *constitui um grupo comutativo, que será finito ou infinito, conforme for finito ou infinito o período de* θ, *sendo no primeiro caso a ordem do grupo precisamente igual ao período de* θ. Chama-se *grupo cíclico* (gerado por θ) um tal grupo.[1]

13. Grupos de substituições

Consideremos agora, em particular, grupos de substituições. Um grupo de tal natureza é necessariamente finito, visto ser finito (igual a $n!$) o número de substituições sobre n elementos. Chama-se *grupo simétrico* (ou *grupo total*) sobre n letras e representa-se por S_n o grupo constituído por todas as possíveis substituições sobre n letras. Mas outros exemplos se apresentam de grupos de substituições:

a) Consideremos o triângulo equilátero da Fig. 1, cujos vértices são designados por 1, 2, 3. Cada um dos deslocamentos deste triângulo que o transformam em si mesmo será manifestamente definido por uma conveniente substituição sobre os três vértices 1, 2, 3. Ora é fácil ver que o grupo de tais substituições coincide com o grupo total,

$$S_3 = \{I, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

(1) – Note-se que esta noção nada tem que ver com a de substituição cíclica.

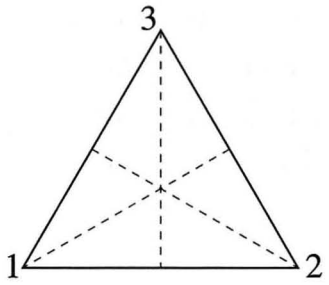


Fig. 1

Todavia, se considerarmos apenas, entre tais deslocamentos, aqueles que não mudam a *face* do triângulo, ficaremos reduzidos a um grupo de ordem 3: o grupo constituído pelas potências do ciclo (1 2 3).

b) Seja agora o quadrado [1 2 3 4] (Fig. 2). É fácil ver que o grupo desta figura – grupo que designaremos por Q_4 – é constituído pelas substituições *I*, (1 3), (2 4), (1 2), (3 4), (1 4) (2 3), (1 3) (2 4), (1 2 3 4), (4 3 2 1).

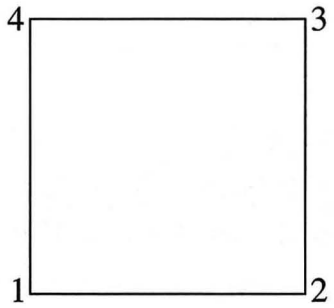


Fig. 2

Tem-se pois $Q_4 \neq S_4$, visto que a ordem de S_4 é 4! = 24.

c) Se em vez dum quadrado considerarmos um rectângulo (Fig. 3) seremos conduzidos ao grupo formado pelas substituições *I*, (1 2) (3 4), (1 4) (2 3), (1 3) (2 4). Este grupo que, ao contrário do anterior, é comutativo – é geralmente conhecido por "grupo quártico de KLEIN" e representa-se por V_4.

Exemplos instrutivos de grupos são, em geral, todos aqueles que se apresentam em cristalografia.

Importa ainda salientar o seguinte facto:

Para que um conjunto H de substituições constitua um grupo basta que verifique a condição de conter o produto $\sigma\theta$ de todo o par σ, θ de substituições que lhe pertençam.

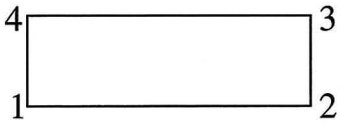


Fig. 3

Com efeito, uma vez verificada esta condição, tem-se que, dado um elemento σ de H, também σ^{-1} pertencerá a H – pois que, como vimos (n.° 10), a inversa duma substituição σ coincide sempre com uma potência de expoente positivo de σ.

14. Grupo duma função

Como se sabe, duas funções de uma ou mais variáveis dizem-se *idênticas* quando tomam o mesmo valor para cada sistema de possíveis valores das variáveis independentes. Por exemplo, são *idênticas* as funções $\varphi(x, y) \equiv (x + y)^2$, $\psi(x, y) \equiv x^2 + 2xy + y^2$, o que se exprime escrevendo $\varphi(x, y) \equiv \psi(x, y)$ ou simplesmente $\varphi \equiv \psi$.

Seja então $\varphi(x, y)$ uma qualquer função das duas variáveis x, y; diz-se que esta função é *simétrica* ou *comutativa*, quando se tem $\varphi(x, y) \equiv \varphi(y, x)$. Os primeiros exemplos de funções simétricas são-nos dados, naturalmente, pela adição e pela multiplicação: $x+y \equiv y+x$, $xy \equiv yx$; e os primeiros exemplos de funções *assimétricas* aparecem-nos com a subtracção e a divisão: $x-y \not\equiv y-x$, $x:y \not\equiv y:x$.

Mas o conceito de função simétrica generaliza-se imediatamente a funções de qualquer número de variáveis (para fixar ideias, podemos limitar-nos a funções complexas de variáveis complexas). Diz-se que uma função $\varphi(z_1, z_2, \ldots, z_n)$ é *simétrica* quando fica idêntica a si mesma, qualquer que seja a substituição efectuada sobre as suas variáveis. Exemplo: a função

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

é simétrica; a função

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

é assimétrica.

Todavia, uma função $\varphi(z_1, z_2, \ldots, z_n)$ pode, sem ser simétrica, ficar invariante para algumas substituições sobre as suas variáveis. Assim, por exemplo, a função

$$\varphi(z_1, z_2, z_3) \equiv (z_1 - z_2)\,(z_1 - z_3)\,(z_2 - z_3)$$

é assimétrica e contudo mantém-se inalterada para as substituições I, (1 2 3), (1 3 2)[1].

Dum modo geral, dada uma função $\varphi(z_1, z_2, \ldots, z_n)$, convencionaremos representar abreviadamente por $\theta\{\varphi\}$ a função que se obtém da primeira, efectuando sobre as variáveis $z_1, z_2, \ldots, z_n$ a substituição θ.

Sejam então σ, θ duas substituições sobre $z_1, z_2, \ldots, z_n$, que deixem inalterada a função φ, isto é, duas substituições tais que

$$\sigma\{\varphi\} = \theta\{\varphi\} = \varphi.$$

Daqui resulta imediatamente, pela definição de produto $\sigma\theta$:

$$(\sigma\theta)\{\varphi\} = \sigma\{\theta\{\varphi\}\} = \sigma\{\varphi\} = \varphi;$$

isto é, o produto $\sigma\theta$ também deixa invariante a função φ. Podemos pois, atendendo à observação final do número precedente, assentar no seguinte resultado:

As substituições sobre $z_1, z_2, \ldots, z_n$ que deixam invariante uma dada função destas variáveis (qualquer que ela seja) formam um grupo G.

---

(1) – Para representar as substituições sobre as variáveis $z_1, z_2, \ldots, z_n$, bastará escrever os índices.

Diz-se então que a função φ *pertence ao grupo* G ou que G é o *grupo da função* φ. Duas funções dizem-se *semelhantes*, quando pertencem ao mesmo grupo. Por exemplo, as funções

$$z_1 + z_2 - z_3 \quad \text{e} \quad z_1 + z_2 + z_3^2$$

são semelhantes: pertencem ambas ao grupo $G = \{I, (1\ 2)\}$. Note-se, de passagem que, na expressão analítica duma função de n variáveis, podem não figurar explicitamente algumas dessas variáveis; tal é o caso, por exemplo, das funções

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

$$\varphi(z_1, z_2, z_3) \equiv z_1 \cdot z_2,$$

as quais[1] pertencem ainda manifestamente ao grupo

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

Pode mesmo acontecer que não apareça explicitamente nenhuma variável: tal é o caso das funções que se reduzem a constantes, funções que devemos naturalmente incluir na categoria das simétricas.

Em particular, o grupo duma função pode reduzir-se à identidade, como acontece, por exemplo, com a função

$$\varphi(z_1, z_2, z_3) \equiv z_1 - z_2 + 2z_3.$$

Demonstra-se mesmo que, dado arbitrariamente um grupo G de substituições sobre n variáveis $z_1, z_2, \ldots, z_n$, é sempre possível construir uma função (racional inteira) de $z_1, z_2, \ldots, z_n$, a qual pertença a G.

São dignos de nota os dois seguintes exemplos: ao grupo Q_4 do quadrado [1 2 3 4] atrás considerado pertence, entre outras, a função $z_1 z_3 + z_2 z_4$; ao grupo V_4 do rectângulo pertence a função $(z_1 - z_2)(z_3 - z_4)$.

---

(1) – Podemos ainda escrever $z_1 + z_2 + 0 \cdot z_3$ em vez de $z_1 + z_2$ e $z_1\ z_2 + 0 \cdot z_3$ em vez de $z_1\ z_2$, passando assim a variável z_3 a figurar explicitamente.

Chama-se *grupo alternante* (sobre n letras) e representa-se por A_n o grupo a que pertence a função definida pelo determinante de VANDERMONDE:

$$V = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ z_1 & z_2 & \cdots & z_n \\ z_1^2 & z_2^2 & \cdots & z_n^2 \\ \cdots & \cdots & \cdots & \cdots \\ z_1^{n-1} & z_2^{n-1} & \cdots & z_n^{n-1} \end{vmatrix} = (z_n - z_1)(z_n - z_2) \cdots (z_n - z_{n-1}) \\ (z_{n-1} - z_1) \cdots (z_{n-1} - z_{n-2}) \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ (z_2 - z_1) \quad .$$

Abreviadamente:

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

Dizem-se *pares* as substituições pertencentes a A_n e ímpares as restantes. Toda a transposição é (pois que se traduz numa troca entre duas colunas do determinante V) uma substituição ímpar. Por outro lado, visto que o efeito duma substituição sobre as variáveis de que depende V consiste quando muito em mudar o sinal desta função, segue-se que o produto de duas substituições ímpares é uma substituição par e que o produto duma substituição par por uma substituição ímpar é uma substituição ímpar. Deste modo, fixada uma transposição $(i\,k)$, podemos fazer corresponder a cada substituição par, σ, uma, e uma só, substituição ímpar, $\overline{\sigma}$, por meio da fórmula $\overline{\sigma} = (i\,k)$; reciprocamente, esta mesma fórmula faz corresponder a cada substituição ímpar $\overline{\sigma}$, a substituição par

$$\sigma = (i\,k)^{-1}\,\overline{\sigma} = (i\,k)\,\overline{\sigma} \, .$$

Daqui resulta que há tantas substituições pares quantas as substituições ímpares e que, portanto, o número de elementos de A_n será $n!/2$.

De resto, demonstra-se facilmente que toda a substituição é decomponível – de várias maneiras – num produto de transposições (possivelmente com elementos comuns); ora, em virtude do que acabamos de ver, o número de transposições dum tal produto, deve ser necessariamente par ou ímpar, conforme for par ou ímpar a substituição de que se trata.

15. Intersecção de dois ou mais grupos. Geradores dum grupo

Consideremos um conjunto A qualquer (finito ou infinito) e sejam G_1, G_2 dois grupos de transformações (reversíveis) do conjunto A sobre si mesmo. Os grupos G_1, G_2 têm, pelo menos, um elemento comum: a identidade; e estão contidos num mesmo grupo: o grupo *total* ou *simétrico* que designaremos por $S(A)$. Sejam então σ, θ, dois elementos da intersecção $G_1 \cap G_2$: como σ, θ pertencem ao grupo G_1, também $\sigma\theta$ pertencerá a G_1; analogamente, como σ, θ pertencem a G_2, também $\sigma\theta$ pertencerá a G_2; logo, o produto $\sigma\theta$ será um elemento comum a G_1 e a G_2, isto é, pertencerá a $G_1 \cap G_2$. De modo análogo se demonstra que a inversa de cada transformação pertencente a $G_1 \cap G_2$ é ainda um elemento de $G_1 \cap G_2$. Podemos, pois concluir que o conjunto $G_1 \cap G_2$ constituiu também um grupo.

Este resultado generaliza-se imediatamente a um número qualquer, finito ou infinito, de grupos de transformações (sobre os mesmos elementos): *a intersecção de vários grupos será sempre um grupo.*

Podemos nós afirmar o mesmo a respeito da reunião de dois ou mais grupos? É fácil ver que não. Seja, por exemplo, H_c o grupo das homotetias de centro c e T o grupo das translações: o conjunto $H \cup T$ não é um grupo, visto que o produto duma homotetia σ^c de centro c por uma translacção $\theta \neq I$ é uma homotetia de centro $c' \neq c$.

Seja M um conjunto qualquer de transformações reversíveis do conjunto A sobre si mesmo e designe (M) o conjunto de todas as transformações que se obtém tomando os elementos de M e os seus inversos, e multiplicando-os entre si dois a dois, três a três, etc., de todos os modos possíveis, com ou sem repetição. Os elementos de (M) serão assim todas as transformações $\mathcal{C}$ da forma

$$\mathcal{C} = \sigma_1^{s1} \cdot \sigma_2^{s2} \cdots \sigma_m^{sm} \tag{3}$$

em que $\sigma_1, \sigma_2, \ldots, \sigma_m$, designam elementos arbitrários de M (em número arbitrário), eventualmente repetidos, e $s_1, s_2, \ldots, s_m$ números inteiros quaisquer, positivos ou negativos. Podemos então afirmar que o conjunto (M) é um grupo (que contém o conjunto M). Com efeito, o produto de duas transformações da forma (3) ou a transformação inversa duma tal transformação é ainda uma transformação da mesma forma:

$$(\sigma_1^{s_1}\,\sigma_2^{s_2}\cdots\sigma_m^{s_m})\,(\theta_1^{t_1}\,\theta_2^{t_2}\cdots\theta_r^{t_r}) = \sigma_1^{s_1}\,\sigma_2^{s_2}\cdots\sigma_m^{s_m}\,\theta_1^{t_1}\,\theta_2^{t_2}\cdots\theta_r^{t_r},$$

$$(\sigma_1^{s_1}\,\sigma_2^{s_2}\cdots\sigma_m^{s_m})^{-1} = \sigma_m^{-s_m}\cdots\sigma_2^{-s_2}\,\sigma_1^{-s_1}.$$

Mais ainda: podemos afirmar que (M) é o grupo mínimo que contém o conjunto M; isto é, podemos afirmar que todo o grupo que contenha M contém necessáriamente o grupo (M). Para exprimir este facto, diz-se que (M) é o grupo *gerado* pelos elementos de M ou que os elementos de M são *geradores* do grupo (M).

a) Por exemplo, o grupo gerado por todas as possíveis rotações do espaço (em torno de eixos quaisquer) é o chamado grupo dos *deslocamentos* (movimentos das figuras invariáveis). Interessa observar, entretanto, que todo o deslocamento se pode reduzir ao produto de uma rotação por uma translação.

b) Analogamente, o grupo gerado pelo conjunto $H_c \cup T$, atrás citado (sendo H_c o grupo das homotetias de centro c e T o grupo das translações) é o conjunto que tem por elementos todas as homotetias e todas as translações, isto é, o conjunto $H_p \cup T$, representando por H_p o conjunto de todas as homotetias.

c) O grupo gerado por uma única transformação θ será, manifestamente, o grupo cíclico

$$H = \{\ldots, \theta^{-2}, \theta^{-1}, I, \theta, \theta^2, \ldots\}.$$

Convém, todavia, não perder de vista que um grupo admite, geralmente, mais de um sistema de geradores.

16. Imagem dum conjunto; imagem duma transformação

Seja θ uma transformação *unívoca* dum conjunto A sobre um conjunto B. Dado um subconjunto M, qualquer, de A, chamaremos *imagem* ou *transformado* de M, por meio de θ, e representaremos por $\theta(M)$, o conjunto dos transformados dos elementos de M por

meio de θ. Assim, por exemplo, a transformada duma figura geométrica F por meio duma homotetia θ será a figura $\theta(F)$ cujos pontos são os transformados de todos os pontos de F por meio de θ.

Sejam agora φ uma transformação *unívoca* do conjunto A sobre si mesmo e θ uma transformação *biunívoca* de A sobre B. A cada elemento x de A faz o operador φ corresponder um elemento y, também de A. Mas, por outro lado, ao elemento x de A corresponderá em B uma imagem, $\bar{x}$, por meio de θ, e, analogamente, ao elemento y de A corresponderá em B uma imagem, $\bar{y}$, por meio de θ. Deste modo, ao operador φ, que transforma x em y, corresponderá o operador $\bar{\varphi}$ que transforma $\bar{x}$ em $\bar{y}$: $\bar{y} = \bar{\varphi}(\bar{x})$. A este operador $\bar{\varphi}$ é natural chamar o *transformado* ou a *imagem* de φ por meio de θ. Escreveremos então:

$$\bar{\varphi} = \theta[\varphi].$$

Esta definição pode ser resumida no seguinte esquema:

$$\bar{\varphi} = \theta[\varphi]:$$

$$y = \varphi(x), \begin{cases} \bar{x} = \theta(x) \\ \bar{y} = \theta(y) \end{cases} \rightarrow \bar{y} = \bar{\varphi}(\bar{x}).$$

Notemos entretanto que, visto ser θ reversível, (por hipótese), virá

$$x = \theta^{-1}(\bar{x})$$

e, portanto:

$$\bar{y} = \theta(y) = \theta(\varphi(x)) = \theta(\varphi(\theta^{-1}(\bar{x})),$$

isto é,

$$\bar{y} = (\theta\, \varphi\, \theta^{-1})(\bar{x})$$

donde, por comparação com $\bar{y} = \bar{\varphi}(\bar{x})$:

$$\bar{\varphi} = \theta\, \varphi\, \theta^{-1}.$$

Esta última fórmula podia-nos servir para definir directamente "transformada de φ por meio de θ", mas tal definição seria menos *natural* do que a primeira.

Exemplos:

a) Representemos por P o conjunto dos números positivos e por **R** o conjunto de números reais. O operador $\sqrt[3]{\ }$ é uma transformação biunívoca de P sobre P; o operador *log,* uma transformação biunívoca de P sobre **R**. Ter-se-á então

$$y = \sqrt[3]{x}\,, \quad \begin{cases} \bar{x} = \log x \\ \bar{y} = \log y \end{cases} \rightarrow \bar{y} = \frac{1}{3}\bar{x}\,.$$

A extracção da raiz cúbica é, pois transformada pelo *operador log* na *divisão por 3*.

b) Sejam α, β dois planos quaisquer e c um ponto de α. Se representarmos por θ a operação de projecção dos pontos de α sobre β, segundo uma direcção determinada d (não paralela nem a α nem a β), é fácil ver que toda a homotetia de centro c (em α) é transformada por θ na homotetia de igual razão e de centro c' (em β) sendo $c' = \theta(c)$.

c) Consideremos o conjunto

$$A = \{a, b, c, d\}.$$

O operador

$$\sigma = \begin{pmatrix} c\ a\ b\ c \\ a\ b\ c\ d \end{pmatrix}$$

será uma transformação unívoca de A sobre A; o operador

$$\theta = \begin{pmatrix} c\ a\ d\ b \\ a\ b\ c\ d \end{pmatrix}$$

será também uma transformação biunívoca de A sobre A. Para determinar a transformada $\overline{\sigma}$ de σ por meio de θ, em vez de utilizar a fórmula

$$\sigma = \theta\,\sigma\,\theta^{-1}$$

é mais cómodo proceder directamente conforme o esquema

$$y = \sigma(x)\,, \quad \begin{cases} \overline{x} = \theta(x) \\ \overline{y} = \theta(y) \end{cases} \rightarrow \quad \overline{y} = \overline{\sigma}(\overline{x})\,.$$

Ter-se-á então:

$$\overline{\sigma} = \begin{pmatrix} \overline{a} & \overline{a} & \overline{b} & \overline{c} \\ \overline{a} & \overline{b} & \overline{c} & \overline{d} \end{pmatrix}, \text{ com}$$

$$\overline{a} = \theta(a),\ \overline{b} = \theta(b),\ \overline{c} = \theta(c),\ \overline{d} = \theta(d),$$

isto é,

$$\overline{\sigma} = \begin{pmatrix} d & c & a & d \\ c & a & d & b \end{pmatrix} = \begin{pmatrix} c & d & d & a \\ a & b & c & d \end{pmatrix}.$$

Tudo se resume, portanto, em efectuar a substituição θ *sobre as letras do quadro representativo do operador* σ.

Observe-se agora o seguinte facto:

Condição necessária e suficiente para que se tenha $\theta\,\varphi\,\theta^{-1} = \varphi$ *é que os operadores* θ, φ *sejam permutáveis.*

Por outros termos: a igualdade $\theta\,\varphi\,\theta^{-1} = \varphi$ é equivalente à igualdade $\theta\,\varphi = \varphi\,\theta$.

Para reconhecer este facto, basta multiplicar à direita, por θ, ambos os membros da igualdade

$$\theta\,\varphi\,\theta^{-1} = \varphi,$$

e multiplicar, também à direita, por θ^{-1}, ambos os membros de $\theta\,\varphi = \varphi\,\theta$.

É fácil ainda verificar as duas seguintes propriedades:
1) *O transformado do produto é igual ao produto dos transformados:* $\theta[\varphi \cdot \psi] = \theta[\varphi] \cdot \theta[\psi]$.
2) *O transformado do inverso coincide com o inverso do transformado (quando este existe)*: $\theta[\varphi^{-1}] = (\theta[\varphi])^{-1}$.

Bastará demonstrar a propriedade 1):

$$\begin{aligned}\theta[\varphi] \cdot \theta[\psi] &= (\theta\,\varphi\,\theta^{-1})\,(\theta\,\psi\,\theta^{-1}) = \\ &= (\theta\,\varphi)\,(\theta^{-1}\,\theta)\,(\psi\,\theta^{-1}) = \\ &= (\theta\,\varphi)\,(\psi\,\theta^{-1}) = \theta(\varphi\,\psi)\,\theta^{-1} = \\ &= \theta[\varphi\,\psi].\end{aligned}$$

17. Transformado dum grupo

Sejam ainda A, B dois conjuntos quaisquer (distintos ou coincidentes) e seja θ uma transformação biunívoca de A sobre B. Dado um conjunto H de transformações biunívocas de A sobre A, chamaremos transformado de H por meio de θ ao conjunto $\overline{H}$ de todas as transformações da forma

$$\theta\,\xi\,\theta^{-1},$$

em que ξ designa um elemento qualquer de H; isto é, simbolicamente,

$$\overline{H} = \theta\,H\,\theta^{-1} \text{ ou } \overline{H} = \theta[H].$$

(Em geral, dada uma transformação θ e um conjunto H de transformações do mesmo tipo, representaremos por θH o conjunto de todas as transformações que se obtém multiplicando θ por cada elemento de H; analogamente, dados dois conjuntos T, H de transformações do mesmo tipo, representaremos por TH o conjunto de todas as transformações que se obtém, multiplicando cada elemento de T por cada elemento de H).

Ora é fácil de ver que, se o conjunto H é um grupo, também o seu transformado H por meio de θ é um grupo: basta atender às duas últimas propriedades indicadas no final do número precedente.

Como exemplo, consideremos de novo o grupo V_4, a função

$$\varphi(z_1, z_2, z_3, z_4) \equiv (z_1 - z_2)\,(z_3 - z_4)$$

e punhamos $\theta = (1\ 3)$.

Ter-se-á

$$\varphi(z_3, z_2, z_1, z_4) \equiv (z_3 - z_2)\,(z_1 - z_4)$$

e, portanto, $$\theta\{\varphi\} \neq \varphi\,.$$

Ora o grupo a que pertence a função $\theta\{\varphi\}$ é precisamente o grupo

$$\theta\, V_4\, \theta^{-1}.$$

A diferença entre φ e $\theta\{\varphi\}$ está apenas na diversidade de notação, isto é, na maneira de representar as variáveis, e outro tanto se pode dizer a respeito de V_4 e de $\overline{V}_4$; para a função φ, as variáveis são z_1, z_2, z_3, z_4; para a função $\theta\{\varphi\}$, os símbolos das variáveis são substituídos, respectivamente, por z_3, z_2, z_1, z_4.

CAPÍTULO II

TRANSITIVIDADE E HOMOMORFIA

18. Relações de equivalência; repartições dum conjunto

Diz-se que, num dado conjunto A, é definida uma *relação binária* ρ, quando se tenha fixado um critério, pelo qual, dados dois quaisquer elementos x, y de A (distintos ou coincidentes), se apresenta sempre uma, e uma só, das seguintes hipóteses: 1) os elementos x, y, na ordem por que estão escritos, *verificam* a relação ρ; 2) os elementos x, y, na ordem por que estão escritos, *não verificam* a relação ρ. No primeiro caso também se diz que o *par ordenado* (x, y) verifica a relação ρ, e, para o indicar, escreve-se

$$x \rho y .$$

Assim, por exemplo, a relação $<$ é definida no conjunto dos números reais; a relação *múltiplo de* é definida no conjunto dos números inteiros ou mesmo no conjunto dos polinómios, etc. Em Geometria euclideana, a relação de paralelismo é definida no conjunto das rectas, no conjunto dos planos ou mesmo na reunião dos dois conjuntos, mas já o não é no conjunto dos pontos, pois que *não faz sentido* dizer que dois pontos sejam ou não paralelos.

Sendo ρ uma relação definida num conjunto A, diz-se que:

I) a relação ρ *é reflexiva*, quando se tem: $x \rho x$, qualquer que seja $x \in A$;

II) a relação ρ é *simétrica*, quando, todas as vezes que se tem $x \rho y$, se tem igualmente $y \rho x$;

III) a relação é *transitiva*, quando, todas as vezes que se tem simultaneamente $x \rho y$ e $y \rho z$, se tem igualmente $x \rho z$.

Para exprimir que uma dada relação ρ é ao mesmo tempo reflexiva, simétrica e transitiva, costuma dizer-se que ρ é uma *relação de equivalência.*

Como exemplo de relação de equivalência, apresenta-se em primeiro lugar a relação lógica de identidade, expressa pelo símbolo "=". No campo da Geometria euclideana, além da relação de identidade (ou coincidência), são relações de equivalência a de igualdade geométrica (ou congruência), a de semelhança, a de afinidade, a de paralelismo (considerando a coincidência como um caso particular do paralelismo), etc., etc. Mas já a relação de perpendicularidade não é uma relação de equivalência, porque não é reflexiva nem transitiva.

Posto isto, seja ρ uma relação de equivalência definida num conjunto A. Dado um elemento a qualquer de A podemos imaginar reunidos num conjunto todos os elementos de A equivalentes a a (segundo ρ), conjunto que designaremos por K_a. Como K_a contém necessariamente a (pela reflexividade de ρ), segue-se que a reunião de todos os conjuntos K_a assim obtidos, quando a percorre A, é precisamente o conjunto A. Por outro lado, tem-se que:

1) *Se a é equivalente a b (segundo* ρ*), então* $K_a = K_b$. Com efeito, em virtude da transitividade e da simetria de ρ, se a é equivalente a b, todo o elemento x equivalente a a (isto é, pertencente a K_a) é também equivalente a b (isto é, pertencente a K_b) e, reciprocamente, todo o elemento de K_b será um elemento de K_a.

2) *Se a não é equivalente a b (segundo* ρ*), então os conjuntos* K_a e K_b *são disjuntos*. Com efeito, se os conjuntos K_a e K_b tivessem um elemento comum c, ter-se-ia ao mesmo tempo $a \rho c$, $c \rho b$, e portanto $a \rho b$, contra a hipótese.

Deste modo, o conjunto A fica decomposto numa família $\mathcal{F}$ de conjuntos K_a, K_b, ..., disjuntos dois a dois e cuja reunião é A. A uma tal família dá-se, genericamente, o nome de *repartição* de A, e aos conjuntos que a constituem, o nome de *elementos*, *células* ou *classes* da repartição. Do que precede resulta então que:

Condição necessária e suficiente para que se tenha $a \rho b$ *é que a, b pertençam à mesma célula de repartição determinada em A por* ρ.

Reciprocamente, é manifesto que, dada uma repartição $\mathcal{F}$ do conjunto A, ficará definida em A uma relação ρ de equivalência, desde que se ponha, por definição:

$x \rho y$, *se, e só se*, x, y pertencem à mesma classe de repartição $\mathcal{F}$.

Exemplos:

a) Como se sabe, dados três números inteiros, x, y, p, diz-se que x *é congruente a* y *relativamente ao módulo* p, e escreve-se

$$x \equiv y \pmod{p},$$

quando $x - y$ é um múltiplo de p. Uma vez fixado o número p, fica assim definida uma relação binária entre as variáveis x, y, relação manifestamente reflexiva, simétrica e transitiva: uma relação de equivalência. Seja, por exemplo, $p = 3$; então, o conjunto dos inteiros (positivos e negativos, incluído o zero) ficará *repartido* em três classes: a dos números que divididos por 3 dão resto 0, a dos números que divididos por 3 dão resto 1 e a dos números que divididos por 3 dão resto 2.

b) Consideremos agora a relação de paralelismo, definida no conjunto das rectas. É fácil ver que esta relação determina, em tal conjunto, uma repartição, cujos elementos são as diferentes *direcções* – se chamarmos *direcção duma recta* à classe de todas as rectas que lhe são paralelas. (Segundo a acepção corrente, *a direcção duma recta* não é propriamente a classe das rectas que lhe são paralelas, mas sim aquilo que há de *comum* a todas essas rectas – ou, como se diz, a *entidade abstracta* de que qualquer dessas rectas é uma *representação*. Mas trata-se aqui duma distinção puramente psicológica, que se revelou inessencial em Matemática).

c) A relação de semelhança entre figuras geométricas determina no conjunto de tais figuras uma repartição, cujos elementos são as diferentes *formas* – se chamarmos *forma duma figura*, à classe das figuras que lhe são semelhantes. (Observação análoga à precedente).

d) Diz-se que dois conjuntos são *equipotentes* ou *igualmente numerosos*, quando é possível estabelecer entre os elementos dum e do outro uma correspondência biunívoca. Trata-se ainda aqui duma relação de equivalência, que conduz, por *abstracção*, à ideia de *número* (*cardinal*).

e) Consideremos finalmente o conjunto

$$M = \{a, b, c, d\}.$$

Uma repartição deste conjunto será, por exemplo, a família

$$\mathcal{F} = \{\{a, c\}, \{b, d\}\}.$$

A relação de equivalência definida por tal repartição será a relação ρ descrita no seguinte quadro:

$x \rho y$

x \ y	a	b	c	d
a	*		*	
b		*		*
c	*		*	
d		*		*

em que, a presença ou ausência do asterístico no cruzamento da linha x com a coluna y está a indicar que o par ordenado (x, y) verifica ou não a relação ρ.

Em particular as células da repartição definida num conjunto A podem reduzir-se aos elementos de A: neste caso, a relação será, manifestamente, a relação de identidade. Por outro lado, toda a relação de equivalência se traduz numa relação de identidade: a identidade entre as classes da repartição correspondente. Assim, por exemplo, dizer que duas rectas são *paralelas* equivale a dizer que têm a *mesma* direcção (equivalência entre as rectas, *identidade* entre as respectivas direcções); analogamente dizer que 2 figuras são *semelhantes* equivale a dizer que têm a *mesma* forma, etc., etc..

19. Equivalência a respeito dum grupo. Sistemas de transitividade

Seja A um conjunto qualquer e designe G um grupo de transformações reversíveis do conjunto A sobre si mesmo. Diz-se que dois elementos x, y de A são *equivalentes* a respeito de G, e escreve-se, para o indicar,

$$x \sim y(G),$$

quando existe pelo menos uma transformação θ pertencente a G, que transforme x em y: $\theta(x) = y$. Uma vez fixado o grupo G, podemos escrever simplesmente $x \sim y$, em vez de $x \sim y(G)$. A relação expressa então pelo símbolo "~" é efectivamente uma relação de equivalência, como mostram as considerações seguintes:

1) $x \sim x$, qualquer que seja $x \in A$. Com efeito, existe em G o elemento I, que faz corresponder a x o próprio x.

2) Se $x \sim y$, *também* $y \sim x$. Com efeito, se $x \sim y$, quer dizer que existe em G um elemento θ tal que $\theta(x) = y$. Mas então será

$$x = \theta^{-1}(y)$$

e, como $\theta^{-1} \in G$ (visto ser G um grupo), segue-se que também $y \sim x$.

3) Se $x \sim y$ e $y \sim z$, *então* $x \sim z$. Com efeito, se existem em G dois elementos σ, θ tais que $\sigma(x) = y$, $\theta(y) = z$, então ter-se-á $\theta(\sigma(x)) = z$, ou seja

$$(\theta\,\sigma)(x) = z\,,$$

e, como $\theta\,\sigma \in G$, segue-se que $x \sim z$.

A relação expressa pelo sinal "~" é pois uma relação de equivalência que, como tal, determina em A uma repartição. Ora bem, chamam-se *sistemas de transitividade de* G (sobre A), precisamente, as classes de tal repartição.

O sistema de transitividade a que pertence um dado elemento x de A será pois, o conjunto de todos os elementos de A em que x pode ser transformado por meio de transformações pertencentes a G.

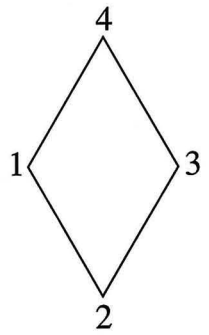


Fig. 4

Consideremos, por exemplo, o grupo L_4 do losango [1 2 3 4], (Fig. 4). Ter-se-á

$$L_4 = \{I, (1\ 3), (2\ 4), (1\ 3)\ (2\ 4)\}.$$

Os sistemas de transitividade deste grupo serão, manifestamente, os conjuntos $\{1,3\}$ e $\{2,4\}$. (Ao mesmo grupo pertence, por exemplo, a função $z_1 z_3 - z_2 z_4$).

Pode acontecer, em particular, que o grupo G admita, como único sistema de transitividade, o próprio conjunto A: em tal hipótese, todos os elementos de A serão equivalentes a respeito de G. Diz-se então que o grupo G é *transitivo* (sobre A) ou que o conjunto A é *homogéneo* a respeito de G; caso contrário, diz-se que G é *intransitivo*. Assim, por exemplo, o espaço euclideano $\mathbf{R}_3$ é *homogéneo* a respeito do grupo das translacções, e portanto, a respeito do grupo dos deslocamentos, do grupo das semelhanças, etc.; por sua vez, o espaço projectivo $\overline{\mathbf{R}}_3$ (que resulta de $\mathbf{R}_3$ pela adjunção dos chamados *pontos impróprios* ou *pontos do infinito*) não é homogéneo a respeito do grupo das semelhanças ou do grupo das afinidades, mas já é homogéneo a respeito do grupo das *colineações*. (Chamam-se *colineações* as transformações pontuais biunívocas do espaço $\overline{\mathbf{R}}_3$ sobre si mesmo que respeitam a noção de recta, isto é, que transformam rectas em rectas. Chamam-se *afinidades* as colineações que transformam pontos impróprios em pontos impróprios e, portanto, rectas paralelas entre si em rectas paralelas entre si. A respeito do espaço euclideano $\mathbf{R}_3$, as afinidades podem ser definidas simplesmente como as transformações biunívocas de $\mathbf{R}_3$ sobre si mesmo que transformam rectas em rectas).

A anterior definição de equivalência a respeito de G, é susceptível de generalização, passando dos elementos para os conjuntos.

Dados dois subconjuntos M, N de A, diz-se *que M é equivalente a N, a respeito de G*, quando existe em G pelo menos uma transformação θ que transforme M em N: $\theta(M) = N$.

Assim, por exemplo, duas rectas serão equivalentes a respeito do grupo das translações, se, e só se, forem paralelas. É curioso observar como o grupo das translações, sendo transitivo sobre o conjunto $\mathbf{R}_3$ dos pontos, não o é sobre o conjunto das rectas. Todavia, este último conjunto já é homogéneo a respeito do grupo dos deslocamentos, visto que é sempre possível passar duma recta para outra recta por meio duma rotação.

20. Alusão ao programa de Erlangen

Duas figuras geométricas dizem-se *iguais* (ou *congruentes* ou *sobreponíveis*), quando são equivalentes entre si a respeito do grupo G_d dos deslocamentos; dizem-se *semelhantes*, quando equivalentes entre si a respeito do grupo G_s das transformações de semelhança (gerado pelas homotetias e pelos deslocamentos); dizem-se *afins*, quando equivalentes entre si a respeito do grupo G_a das afinidades, dizem-se *homeomorfas*, quando equivalentes a respeito do grupo G_h dos *homeomorfismos* (ou transformações bicontínuas), etc., etc. Ter-se-á:

$$\mathscr{T} \subset G_d \subset G_s \subset G_a \subset G_h \subset S(\mathbf{R}_3)$$

designando por $\mathscr{T}$ o grupo que se reduz à identidade e por $S(\mathbf{R}_3)$ o grupo total. É claro que dois conjuntos de pontos serão equivalentes a respeito de $\mathscr{T}$, se, e só se, forem *coincidentes*, e serão equivalentes a respeito de $S(\mathbf{R}_3)$, se, e só se, forem *equipotentes* (isto é, com o mesmo número de elementos).

A cada geometria corresponde um grupo: o grupo das transformações que respeitam os conceitos estudados por essa geometria. A cada grupo corresponde uma geometria: a geometria dos conceitos que se mantêm invariantes para todas as transformações desse grupo.

Ao grupo G_s corresponde a *geometria euclideana*, que estuda os conceitos definíveis, em última análise, a partir das noções de "recta", "situado entre" e "equidistância". Ao grupo G_a corresponde a *geometria afim*, que estuda apenas as noções afins, isto é, as noções exprimíveis nos conceitos de "recta" e de "situado entre". Ao grupo G_h corresponde a *topologia*, que estuda as noções definíveis a partir do conceito de "limite", tais como a de "interior", "exterior", "fronteira", "conjunto fechado", "conjunto conexo", etc., etc. Ao grupo $S(\mathbf{R}_3)$ corresponde a *lógica formal* (para os conjuntos de pontos), que estuda noções tais como as de "contido", "intersecção", "reunião", etc., etc.

Observemos ainda que, reportando-nos ao espaço projectivo $\overline{\mathbf{R}}_3$, o grupo afim se pode considerar contido no grupo projectivo G_p (constituído pelas colineações) que é o grupo característico da geometria projectiva. Por sua vez, G_p está contido no grupo G_h dos homeomorfismos de $\overline{\mathbf{R}}_3$, que dá a *topologia do espaço projectivo*, diferente da topologia do espaço euclideano.

Tal é, em linhas muito gerais, a ideia da sistematização das geometrias mediante o conceito de "grupo", exposta por FELIX KLEIN no célebre programa de Erlangen.

21. Funções conjugadas duma função dada. Conceito de subgrupo invariante

Consideremos uma função $\varphi(z_1, z_2, \ldots, z_n)$ e um grupo G, qualquer, de substituições sobre $z_1, z_2, \ldots, z_n$. Quais as substituições de G que deixam φ invariante? Designando por G^* o grupo da função φ, a intersecção $G \cap G^*$ será, manifestamente, o subgrupo H de G constituído por *todas as substituições de G que deixam* φ *invariante*. Diremos então que φ pertence ao grupo H *em* G.

Efectuando sobre as variáveis $z_1, z_2, \ldots, z_n$ todas as substituições de G obter-se-ão várias funções a partir de φ (desde que seja $H \neq G$). Sejam $\varphi, \varphi_2, \varphi_3, \ldots, \varphi_m$ todas as funções distintas assim obtidas: diremos então que $\varphi, \varphi_2, \ldots, \varphi_m$ *são as funções conjugadas de* φ *em* G, (ou simplesmente, *as funções conjugadas de* φ, se G é o grupo simétrico).

Seja, por exemplo, a função

$$\varphi(z_1, z_2, z_3, z_4) \equiv z_1 z_3 + z_2 z_4$$

já considerada, cujo grupo designámos por Q_4 – grupo de ordem 8 que pode ser gerado pelas substituições (1 3) e (1 2 3 4). Consideremos, por outro lado, o grupo alternante A_4. O grupo da função φ em A_4 será a intersecção $A_4 \cap Q_4$, ou, seja o grupo constituído pelas substituições *pares* de Q_4, que são: *I*, (1 2) (3 4), (1 4) (2 3), (1 3) (2 4); mas estas são, precisamente, as substituições do grupo V_4 do rectângulo; tem-se pois:

$$A_4 \cap Q_4 = V_4 .$$

Quanto às funções conjugadas de φ em A_4, elas serão, como é fácil ver:

$$\varphi_1(z_1, z_2, z_3, z_4) \equiv \varphi(z_1, z_2, z_3, z_4) \equiv z_1 z_3 + z_2 z_4$$
$$\varphi_2(z_1, z_2, z_3, z_4) \equiv \varphi(z_2, z_3, z_1, z_4) \equiv z_2 z_1 + z_3 z_4,$$
$$\varphi_3(z_1, z_2, z_3, z_4) \equiv \varphi(z_1, z_3, z_4, z_2) \equiv z_1 z_4 + z_3 z_2 .$$

Posto isto, tornemos a considerar uma função φ qualquer das variáveis $z_1, z_2, \ldots, z_n$, cujo grupo em G seja H e cujas funções conjugadas em G sejam $\varphi_1 (= \varphi), \varphi_2, \ldots, \varphi_n$; e propunhamo-nos resolver o seguinte problema:

Dada uma função φ_i, *conjugada de* φ *em G, determinar todas as substituições de G que fazem passar de* φ *para* φ_i.

Seja então θ_i uma das substituições de G que convertem φ em φ_i, isto é, tal que

$$\theta_i \{\varphi\} = \varphi_i .$$

Se for $\mathcal{C}$ uma outra substituição que produza o mesmo efeito, ter-se-á

$$\mathcal{C}\{\varphi\} = \theta_i \{\varphi\} = \varphi_i ,$$

donde

$$(\theta_i^{-1}\mathcal{C})\{\varphi\} = (\theta_i^{-1}\theta_i)\{\varphi\} = \varphi .$$

A substituição $\theta_i^{-1}\mathcal{C}$ deixa pois invariante a função φ, o que quer dizer que tal substituição pertence ao grupo H:

$$\theta_i^{-1}\mathcal{C} \in H,$$

ou seja, pondo $\theta_i^{-1}\mathcal{C} = \sigma$:

$$\mathcal{C} = \theta_i\sigma, \text{ com } \sigma \in H.$$

Reciprocamente, toda a substituição de G da forma $\theta_i\sigma$, com $\sigma \in H$, converte φ em φ_i:

$$(\theta_i\sigma)\{\varphi\} = \theta_i\{\sigma\{\varphi\}\} = \theta_i\{\varphi\} = \varphi_i .$$

Podemos pois concluir que, *se for* θ_i *uma substituição de* G *que converte* φ em φ_i, *as substituições de* G *que produzem este efeito serão todas aquelas da forma* $\theta_i\sigma$, em que σ *representa uma qualquer substituição de* H. Segundo a convenção do n.º 17, o conjunto de tais substituições poderá representar-se por $\theta_i H$. Suponhamos que se tem

$$H = \{I, \sigma_2, \sigma_3, \ldots, \sigma_p\};$$

será então

$$\theta_i H = \{\theta_i, \theta_i\sigma_2, \theta_i\sigma_3, \ldots, \theta_i\sigma_p\}.$$

Fazendo agora variar i de 1 a m (sendo m o número dos conjugados de φ em G) e tomando, para maior simplicidade, $\theta_1 = I$, o grupo G ficará repartido em m conjuntos, de p elementos cada um:

$$\begin{aligned}
&I, \sigma_2, \sigma_3, \ldots, \sigma_p && (\varphi \to \varphi)\\
&\theta_2, \theta_2\sigma_2, \theta_2\sigma_3, \ldots, \theta_2\sigma_p && (\varphi \to \varphi_2)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\theta_m, \theta_m\sigma_2, \theta_m\sigma_3, \ldots, \theta_m\sigma_p && (\varphi \to \varphi_m).
\end{aligned}$$

Estes conjuntos chamar-se-ão *classes laterais de* H *em* G. Mas deste assunto trataremos mais a fundo no número seguinte.

Procuraremos agora resolver uma questão mais geral do que a precedente:

Dadas duas quaisquer funções φ_i, φ_k *conjugadas de* φ em G, *determinar todas as substituições de* G *que fazem passar de* φ_i para φ_k.

Seja então γ uma substituição de G que converta φ_i em φ_k:

$$\gamma\{\varphi_i\} = \varphi_k .$$

Sendo agora θ_i, θ_k duas substituições de G que convertam φ_i respectivamente em φ_i e em φ_k, virá:

$$\gamma\{\theta_i\{\varphi\}\} = \theta_k\{\varphi\},$$

ou seja

$$(\theta_k^{-1}\,\gamma\theta_i)\,\{\varphi\} = \varphi .$$

A substituição $\theta_k^{-1}\,\gamma\theta_i$ deixa pois a função φ invariante, o que quer dizer que tal substituição pertence a H:

$$\theta_k^{-1}\,\gamma\theta_i \in H,$$

ou seja, pondo $\theta_k^{-1}\,\gamma\theta_i = \sigma$:

$$\gamma = \theta_k\,\sigma\,\theta_k^{-1},\ \text{com}\ \sigma \in H .$$

Reciprocamente, toda a substituição de G da forma $\theta_k\,\sigma\,\theta_k^{-1}$, com $\sigma \in H$, converte φ_i em φ_k:

$$(\theta_{jk}\,\sigma\,\theta_i^{-1})\{\varphi_i\} = (\theta_k\sigma)\{\varphi\} = (\theta_k)\{\varphi\} = \varphi_k .$$

Podemos assim concluir que, *se forem* θ_i, θ_k *duas substituições de* G *que convertem* φ *respectivamente em* φ_i *e em* φ_k, *as substituições de* G *que fazem passar de* φ_i *para* φ_k *serão todas aquelas da forma*

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

em que σ *representa uma qualquer substituição de H. O conjunto de tais substituições será pois*

$$\theta_k H \theta_i^{-1}.$$

Em particular: *O grupo a que pertence a função* φ_i *em G (isto é, o conjunto das substituições de G que convertem* φ_i *em* φ_i*) será*

$$\theta_i H \theta_i^{-1}$$

ou seja (n.º 17), *o grupo transformado de H por meio de* θ_i.

Como exemplo, consideremos de novo a função

$$u = z_1 z_3 + z_2 z_4,$$

cujo grupo em A_4 é, como vimos,

$$V_4 = \{I, (1\ 2)\ (3\ 4), (1\ 4)\ (2\ 3), (1\ 3)\ (2\ 4)\}.$$

Uma das substituições de A_4 que convertem a função u na sua conjugada

$$u_2 = z_1 z_2 + z_3 z_4$$

é o ciclo (1 2 3); o grupo a que pertence a função u_2 em A_4 será portanto (1 2 3) V_4 (1 3 2). Para determinar as substituições deste grupo não temos mais do que efectuar sobre os elementos dos ciclos representativos das substituições de V_4 a substituição (1 2 3):

$$(1\ 2\ 3)\ V_4\ (1\ 2\ 3)^{-1} = \{I, (2\ 3)\ (1\ 4), (2\ 4)\ (3\ 1), (2\ 1)\ (3\ 4)\}.$$

Observa-se, porém, este facto notável: o grupo transformado de V_4 por meio do ciclo (1 2 3) – isto é, o grupo a que pertence a função u_2 em A_4 – coincide com V_4. Analogamente se reconhece que o grupo transformado de V_4 por meio do ciclo (2 3 4) – grupo a que pertence a função

$$u_3 = z_1 z_4 + z_2 z_3$$

– coincide com V_4.

Ter-se-á portanto

$$\theta\, V_4\, \theta^{-1} = V_4,$$

qualquer que seja

$$\theta \in A_4.$$

Dum modo geral, diz-se que um subgrupo H dum grupo G é *invariante* ou *normal* em G, quando se tem

$$\theta\, H\, \theta^{-1} = H,$$

para todo o $\theta \in G$.

O grupo V_4 é pois invariante em A_4, mas já, por exemplo, o grupo Q_4 não é invariante em S_4, como é fácil reconhecer.

22. Classes laterais dum grupo

Designe G um grupo qualquer de transformações e seja H um seu subgrupo. Dadas duas transformações θ_1, θ_2 de G, diz-se que θ_1 é *congruente* a θ_2, a respeito de H, e escreve-se

$$\theta_1 \equiv \theta_2 (H),$$

quando o cociente $\theta_2^{-1}\, \theta_1$ é um elemento de H; por outras palavras: quando exista uma transformação $\sigma \in H$, tal que

$$\theta_1 = \theta_2 \sigma.$$

Uma vez fixado o grupo H, pode escrever-se simplesmente $\theta_1 \equiv \theta_2$, em vez de $\theta_1 \equiv \theta_2 (H)$. A relação binária "$\equiv$" assim definida é uma relação de equivalência, como se conclui do que segue:

1) $\theta \equiv \theta$, *qualquer que seja* $\theta \in G$. Com efeito, tem-se $\theta = \theta I$, pertencendo I a H.

2) *Se* $\theta_1 \equiv \theta_2$, *também* $\theta_2 \equiv \theta_1$. Com efeito, se $\theta_1 \equiv \theta_2$ (a respeito de *H*), quer dizer que existe em *H* um elemento σ tal que $\theta_1 = \theta_2 \sigma$. Mas então virá

$$\theta_2 = \theta_1 \sigma^{-1}$$

e, como $\sigma^{-1} \in H$, segue-se que $\theta_2 \equiv \theta_1$.

3) *Se* $\theta_1 \equiv \theta_2$ e $\theta_2 \equiv \theta_3$, *também* $\theta_1 \equiv \theta_3$. Com efeito, se existem duas transformações σ, σ^* de *H* tais que

$$\theta_1 = \theta_2 \sigma, \quad \theta_2 = \theta_3 \sigma^*,$$

ter-se-á

$$\theta_1 = (\theta_3\, \sigma^*)\, \sigma = \theta_3 (\sigma^* \sigma) \quad \text{e, portanto}$$

$$\theta_1 \equiv \theta_3, \text{ visto que } \sigma^* \sigma \in H.$$

A relação "≡" determina portanto uma repartição no grupo *G*; aos elementos dessa repartição dá-se o nome de *classes laterais de H em G*[1]. Seja θ um elemento qualquer de *G*: a classe lateral (de *H* em *G*) a que pertence θ será, manifestamente, o conjunto de todas as transformações da forma $\theta \sigma$, com $\sigma \in H$ – ou seja o conjunto θH.

Podemos agora estabelecer o seguinte:

Teorema – As classes laterais de H em G têm todas o mesmo número de elementos (número finito ou infinito).

Com efeito, a fórmula $\sigma^* = \theta \sigma$ define uma transformação biunívoca $\sigma \rightarrow \sigma^*$ de *H* sobre θH: a cada elemento σ de *H* fica a corresponder um, e um só, elemento $\sigma^* = \theta \sigma$ de θH, e a cada elemento σ^* de θH fica a corresponder o elemento

$$\sigma = \theta^{-1} \sigma^* \text{ de } H, \text{ e só esse.}$$

---

(1) – Mais precisamente: classes laterais esquerdas, porque se apresenta ainda o conceito de "classe lateral direita". Podemos todavia limitar-nos ao primeiro conceito, o que torna dispensável a especificação.

Em particular, se $\theta \in H$ (e só então), tem-se $\theta H = H$: uma das classes laterais de H em G é pois o próprio grupo H. Seja agora θ_2 uma transformação pertencente a G, mas não a H: será $\theta_2 H$ uma classe lateral de H em G, distinta de H; seja por sua vez θ_3 um elemento de G não pertencente a H nem a $\theta_2 H$: será $\theta_3 H$ uma classe lateral de H em G, distinta de H e de $\theta_2 H$; e assim sucessivamente. Poderá então escrever-se:

$$G = H \cup \theta_2 H \cup \theta_3 H \cup \cdots,$$

sendo os conjuntos H, $\theta_2 H$, $\theta_3 H$,... distintos entre si 2 a 2. Importa ainda notar que, *excepto H, nenhuma das classes laterais de H em G pode ser um grupo, pois que nenhuma dessas classes contem a identidade.*

Do teorema precedente resulta imediatamente o seguinte corolário importante:

Se o grupo G é finito, a ordem do subgrupo H de G é um divisor da ordem de G.

Na hipótese do grupo G ser finito, chama-se *índice* de H em G ao cociente r/p da ordem r de G pela ordem p de H. É fácil constatar agora, recordando o que foi dito no n.º anterior, que, se for φ uma função pertencente a H em G, o número das conjugadas de φ em G será precisamente igual ao índice de H em G.

Um outro facto a salientar é o seguinte:

Quando a ordem de G é um número primo, os únicos subgrupos possíveis de G são o próprio G e o grupo idêntico I, donde resulta que G será então um grupo cíclico.

Por conseguinte, encontra-se em tais condições todo o grupo gerado por uma transformação θ cujo período seja um número primo – facto este que irá intervir de maneira essencial na teoria da resolubilidade por meio de radicais.

Convém ainda ilustrar as anteriores considerações com um exemplo intuitivo. Consideremos o octaedro regular [1 2 3 4 5 6] (Fig. 5), cujo grupo designaremos por O_6. Um subgrupo de O_6 é, por exemplo, $\overline{Q_4}$, constituído pelas substituições de O_6 que transformam em si mesmo o quadrado [1 2 3 4] – grupo da ordem 8, conforme o

que se viu no n.º 13. A substituição $\theta = (1\ 5)\ (3\ 6)$ transforma [1 2 3 4] em [5 2 6 4] e a substituição $\mathcal{C} = (2\ 5)\ (4\ 6)$ transforma [1 2 3 4] em [1 5 3 6]. Ter-se-à então

$$O_6 = \overline{Q_4} \cup \theta \overline{Q_4} \cup \mathcal{C} \overline{Q_4}.$$

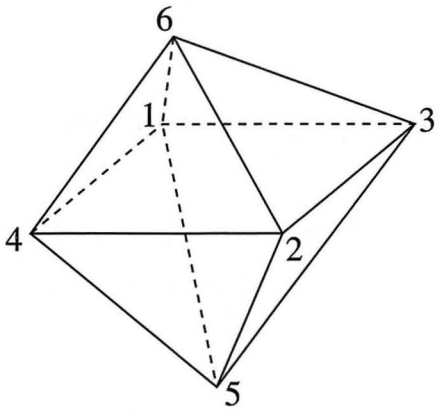


Fig. 5

O grupo O_6 é portanto da ordem 24.

As substituições de G que deixam o quadrado [5 2 6 4] invariante são manifestamente as do grupo

$$\theta \overline{Q_4} \theta^{-1}$$

e as que deixam invariante o quadrado [1 5 3 6] são as do grupo

$$\mathcal{C} \overline{Q_4} \mathcal{C}^{-1}.$$

Como exercício, propomos ainda a demonstração dos seguintes factos:

I – *O grupo alternante A_n é um subgrupo normal do grupo simétrico, S_n, qualquer que seja $n = 2, 3, \ldots$.*
As classes laterais de A_n em S_n são: A_n (conjunto das substituições pares) e $(1\ 2)\ A_n$ (conjunto das substituições ímpares).

II – *Todo o subgrupo dum grupo comutativo G é invariante em G.*

III – *O grupo constituído pela identidade é invariante em qualquer grupo.*

23. O conceito de homomorfismo entre grupos

Continuemos a considerar como exemplo o grupo O_6 do octaedro e, para brevidade de expressão, designemos respectivamente por Γ_1, Γ_2, Γ_3 os quadrados diagonais [1 2 3 4], [2 6 4 5], [1 5 3 6]. É de observar que cada substituição σ de O_6 (executada sobre os vértices 1, 2, 3, 4, 5, 6) determina uma substituição $\overline{\sigma}$ sobre os quadrados Γ_1, Γ_2, Γ_3. Assim, por exemplo, a substituição (1 2 3 4) sobre os vértices determina a substituição $(\Gamma_2\ \Gamma_3)$ sobre os quadrados diagonais; a substituição (1 4 5) (2 6 3) sobre os vértices traduz-se na substituição $(\Gamma_1\ \Gamma_2\ \Gamma_3)$ sobre os quadrados diagonais, etc. Mais ainda: é fácil ver que *uma* mesma substituição sobre os quadrados diagonais pode ser determinada por *quatro* substituições distintas sobre os vértices; por exemplo, a substituição I sobre os quadrados Γ_1, Γ_2, Γ_3 pode provir de qualquer das seguintes substituições sobre os vértices: I, (1 3), (2 4), (1 3) (2 4). As substituições assim obtidas sobre os quadrados Γ_1, Γ_2, Γ_3 constituem manifestamente um grupo (que facilmente se reconhece ser o grupo simétrico sobre os três elementos Γ_1, Γ_2, Γ_3), grupo que designaremos por $\overline{O_6}$. Além disso, fica assim estabelecida uma transformação *unívoca* $\sigma \to \overline{\sigma}$ de O_6 sobre $\overline{O_6}$, com a seguinte particularidade notável:

Sejam σ_1, σ_2 *duas substituições quaisquer de* O_6 *e sejam* $\overline{\sigma}_1$, $\overline{\sigma}_2$, *as substituições que lhes correspondem respectivamente em* O_6. *Pois bem, ao produto* $\sigma_1 \cdot \sigma_2$ *corresponderá precisamente em* O_6 *o produto* $\overline{\sigma}_1 \cdot \overline{\sigma}_2$:

$$\sigma_1 \to \overline{\sigma}_1$$
$$\sigma_2 \to \overline{\sigma}_2$$
$$\sigma_1 \cdot \sigma_2 \to \overline{\sigma}_1 \cdot \overline{\sigma}_2 .$$

Exprime-se este facto dizendo que tal transformação é um *homomorfismo* do grupo O_6 sobre o grupo $\overline{O_6}$.

Dum modo geral, sejam H, $\overline{H}$ duas famílias quaisquer de transformações (sobre os mesmos elementos ou sobre elementos diversos). Dada uma transformação unívoca T de H sobre $\overline{H}$, diz-se que T é um homomorfismo (de H sobre $\overline{H}$), quando verifica as duas seguintes condições:

1) Para cada elemento $\overline{\sigma}$ de $\overline{H}$, há, *pelo menos*, um elemento σ de H que é transformado em $\overline{\sigma}$ por T (isto é, tem-se $T(H) = \overline{H}$).

2) Quaisquer que sejam $\sigma_1, \sigma_2 \in H$, tem-se

$$T(\sigma_1 \cdot \sigma_2) = T(\sigma_1) \cdot T(\sigma_2).$$

Suponhamos agora que o conjunto H é um grupo. Vamos provar, em primeiro lugar, que *T transforma necessariamente a identidade na identidade e o inverso no inverso.* Com efeito, designando por σ um qualquer elemento de H, tem-se

$$I \cdot \sigma = \sigma$$

donde, aplicando T a ambos os membros desta igualdade e atendendo à propriedade 2):

$$\overline{I} \cdot \overline{\sigma} = \overline{\sigma}, \quad \text{ou seja} \quad \overline{I} = \overline{\sigma} \cdot \overline{\sigma}^{-1} = I$$

como tinhamos afirmado. Por outro lado, tem-se, para cada elemento σ de H:

$$\sigma\, \sigma^{-1} = I,$$

donde

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

ou seja

$$T(\sigma^{-1}) = [T(\sigma)]^{-1}$$

como se tinha dito.

Podemos agora demonstrar que, se H é um grupo, também $\overline{H}$ é um grupo. Sejam, com efeito, $\overline{\sigma}$, $\overline{\theta}$ dois elementos quaisquer de $\overline{H}$; a $\overline{\sigma}$ corresponderá em H *pelo menos um elemento* σ e a $\overline{\theta}$ pelo menos um elemento θ; ao produto $\overline{\sigma} \cdot \overline{\theta}$ corresponderá, pela propriedade 2), o produto $\sigma\,\theta$; mas, se H é um grupo $\sigma\,\theta$ pertence a H – logo $\overline{\sigma} \cdot \overline{\theta}$ pertencerá a $\overline{H}$, visto que $\overline{H}$ é constituído pelos transformados de todos os elementos de H. Analogamente se demonstra que o inverso de cada elemento de $\overline{H}$ é ainda um elemento de $\overline{H}$ e que portanto $\overline{H}$ é um grupo (na hipótese de H o ser).

Em resumo:

I – *A imagem homomórfica dum grupo é sempre um grupo.*

II – *Se T é um homomorfismo dum grupo H sobre um grupo* $\overline{H}$, *então*

$$T(I) = I, \quad T(\sigma^{-1}) = [T(\sigma)]^{-1}.$$

Posto isto, sejam G, G', G'' três grupos, e T, S, dois homomorfismos, respectivamente de G sobre G' e de G' sobre G''. Dados dois elementos σ, θ quaisquer de G, virá, aplicando sucessivamente as transformações T, S do produto $\sigma\,\theta$:

$$ST(\sigma \cdot \theta) = S(T(\sigma) \cdot T(\theta)) = ST(\sigma) \cdot ST(\theta),$$

isto é:

O produto de dois homomorfismos é também um homomorfismo.

Dados dois grupos G, G', diz-se que G' é *homomorfo* a G, e escreve-se, para o indicar,

$$G \sim G',$$

quando é possível definir um homomorfismo de G sobre G'. Em virtude do resultado precedente, tem-se que, se $G \sim G'$ e $G' \sim G''$, também $G \sim G''$; por outros termos: a relação de homomorfia, expressa pelo símbolo "~", é *transitiva.*

24. Isomorfismos e automorfismos

Quando um homomorfismo entre dois grupos é uma transformação reversível, toma a designação particular de *isomorfismo.* Desde logo se reconhece que:

A transformação inversa dum isomorfismo é também um isomorfismo.

Seja com efeito T um isomorfismo entre dois grupos G, $\overline{G}$ e sejam $\overline{\sigma}_1$, $\overline{\sigma}_2$ dois elementos arbitrários de G. Em G existirão dois elementos, σ_1, σ_2 que corresponderão respectivamente a $\overline{\sigma}_1$, $\overline{\sigma}_2$

segundo T^{-1}. Ora, como T é um isomorfismo, segue-se que, ao produto $\sigma_1 \cdot \sigma_2$, corresponderá segundo T o produto $\overline{\sigma}_1 \cdot \overline{\sigma}_2$. Mas, por sua vez, como T é reversível, ao produto $\overline{\sigma}_1 \cdot \overline{\sigma}_2$ corresponderá segundo T^{-1} o produto $\sigma_1 \cdot \sigma_2$, isto é:

$$T^{-1}(\overline{\sigma}_1\, \overline{\sigma}_2) = T^{-1}(\overline{\sigma}_1) T^{-1}(\overline{\sigma}_2), \text{ q.e.d.}$$

Dados dois grupos G_1, G_2, diz-se que G_1 é *isomorfo* a G_2, e escreve-se, para o indicar,

$$G_1 \cong G_2,$$

quando é possível definir um isomorfismo de G_1 sobre G_2. A relação de isomorfia, expressa pelo símbolo "$\cong$", é *transitiva*, (visto ser um caso particular da homomorfia); é *simétrica* (visto que a transformação inversa dum isomorfismo é ainda um isomorfismo); é finalmente *reflexiva* (pois basta fazer corresponder a cada elemento σ de G esse mesmo elemento σ, para ficar definido um isomorfismo de G sobre G). Em resumo: a relação de isomorfia é uma relação de equivalência.

Chamam-se *automorfismos* dum grupo G os isomorfismos do grupo G *sobre si mesmo*. Visto que o produto de dois automorfismos é ainda um automorfismo e a transformação inversa dum automorfismo é também um automorfismo, segue-se que o conjunto G de todos os automorfismos do grupo G é também um grupo – *o grupo dos automorfismos de G.*

Como exemplo, consideremos de novo o grupo V_4 do rectângulo e o grupo L_4 do losango:

$$V_4 = \{I, (1\,2)\,(3\,4), (1\,4)\,(2\,3), (1\,3)\,(2\,4)\},$$

$$L_4 = \{I, (1\,3), (2\,4), (1\,3)\,(2\,4)\}.$$

Se pusermos $s_1 = (1\,2)\,(3\,4)$, $s_2 = (1\,4)\,(2\,3)$,

$s_3 = (1\,3)\,(2\,4)$, $t_1 = (1\,3)$,

$t_2 = (2\,4)$, $t_3 = s_3$,

e estabelecermos a correspondência

$$I \to I, \quad s_1 \to t_1, \quad s_2 \to t_2, \quad s_3 \to t_3,$$

ficará definido, como é fácil ver, um isomorfismo de V_4 sobre L_4. Mas tanto V_4 como L_4 admitem vários automorfismos. Para V_4, por exemplo, ter-se-ão os seguintes automorfismos:

$$I, (s_1 s_2), (s_1 s_3), (s_2 s_3), (s_1 s_2 s_3), (s_3 s_2 s_1).$$

Cada uma destas substituições, multiplicada pelo isomorfismo anterior de V_4 sobre L_4, dará, manifestamente, um novo isomorfismo de V_4 sobre L_4.

25. Propriedades algébricas e propriedades específicas. Isomorfismos internos

As propriedades dum grupo G, bem como as dos seus elementos (tomados 1 a 1, 2 a 2, ...) podem ser divididas em duas categorias: 1) propriedades que se mantêm invariantes para todas as possíveis transformações isomórficas de G; 2) propriedades que não são necessáriamente respeitadas pelos isomorfismos de G. As primeiras são chamadas propriedades *algébricas*: as segundas, propriedades *específicas*.

Por exemplo, o facto de uma dada transformação ter período μ; o facto de duas transformações serem permutáveis entre si; o facto de um dado subgrupo ser invariante, etc., etc., são propriedades algébricas. Mas o facto de uma dada transformação ser ou não cíclica, o facto de um dado grupo ser ou não transitivo, etc., etc., são propriedades específicas. Que a transitividade não é propriedade algébrica podemos reconhecê-lo no exemplo do número anterior: os grupos V_4 e L_4 são isomorfos, sendo o primeiro transitivo e o segundo intransitivo.

Dum modo geral, as propriedades algébricas são todas aquelas que podem em, última análise, ser definidas a partir do conceito de "produto" (conceito algébrico fundamental da teoria dos grupos).

Retomemos o exemplo do grupo L_4. Tem-se:

$$t_1^2 = t_2^2 = t_3^2 = I, \quad t_1 t_2 = t_2 t_1 = t_3, \quad t_1 t_3 = t_3 t_1 = t_2, \quad t_2 t_3 = t_3 t_2 = t_1.$$

Vê-se, pois que, do ponto de vista algébrico, nada distingue entre si as substituições t_1, t_2, t_3, as quais, por isso mesmo, são transformadas umas nas outras pelos automorfismos de L_4. E, contudo, as substituições t_1, t_2 são cíclicas (transposições), enquanto t_3 o não é.

Se em vez de L_4 considerarmos V_4, as regras de multiplicação serão precisamente as mesmas que as anteriores (bastaria substituir t_1, t_2, t_3 por s_1, s_2, s_3, em qualquer ordem) – o que está de acordo com o facto dos grupos V_4 e L_4 serem isomorfos.

Por isso, quando dois grupos são isomorfos, diz-se ainda que têm a mesma *estrutura algébrica* ou que definem o mesmo *grupo abstracto*.

Sejam agora A, $\overline{A}$ dois conjuntos quaisquer e G um grupo de transformações biunívocas do conjunto A sobre si mesmo. Seja por outro lado θ uma transformação biunívoca de A sobre $\overline{A}$. Já no n.º 16 vimos o que se entende por transformado dum elemento σ de G por meio de θ. O transformado $\theta G \theta^{-1}$ de G por meio de θ é, como vimos, um outro grupo, $\overline{G}$. Nestes termos, o operador θ traduz-se numa transformação biunívoca de G sobre $\overline{G}$; a cada elemento σ de G corresponde o elemento $\theta[\sigma] = \theta \sigma \theta^{-1}$ de $\overline{G}$, e a cada elemento $\overline{\sigma}$ de $\overline{G}$ corresponde o elemento

$$\theta^{-1}[\overline{\sigma}] = \theta^{-1} \overline{\sigma} \theta$$

de G. Por outro lado, vimos que se tem

$$\theta[\sigma_1 \cdot \sigma_2] = \theta[\sigma_1] \cdot \theta[\sigma_2]$$

quaisquer que sejam σ_1, $\sigma_2 \in G$. Uma tal transformação θ é pois um isomorfismo de G sobre $\overline{G}$, mas um isomorfismo de natureza particular, proveniente duma transformação definida entre A e $\overline{A}$. Aos isomorfismos deste tipo dá-se o nome de *isomorfismos internos*.

Assim, por exemplo, os isomorfismos atrás estudados entre V_4 e L_4 não são internos.

É ainda de observar que, entre os automorfismos de V_4 (atrás indicados), só a identidade é um automorfismo interno.

Facilmente se reconhece agora que *certas propriedades não algébricas, como por exemplo a da transitividade, são respeitadas por todos os isomorfismos internos.*

26. Primeira noção de grupo cociente

Consideremos uma função $\varphi(z_1, z_2, \ldots, z_n)$ e designe G um grupo qualquer de substituições sobre as variáveis $z_1, z_2, \ldots, z_n$. Seja por outro lado H o grupo a que pertence φ em G e sejam $\varphi_1(=\varphi), \varphi_2, \varphi_3, \ldots, \varphi_m$ as funções conjugadas de φ em G (será pois m o índice de H em G).

Vejamos o que acontece quando se efectua uma substituição θ de G sobre as variáveis $z_1, z_2, \ldots, z_n$. A função φ_1 será então convertida numa das suas conjugadas em G. Mas que efeito produz sobre as restantes funções $\varphi_2, \ldots, \varphi_m$ essa mesma substituição θ? Consideremos, por exemplo, a função φ_2; o facto de φ_2 ser uma conjugada de φ_1 em G, significa que existe uma substituição θ_2 de G que converte φ_1 em φ_2; efectuar a substituição θ em φ_2 equivale portanto a efectuar a substituição $\theta\theta_2$ em φ_1:

$$\theta\{\varphi_2\} = \theta\{\theta_2\{\varphi_1\}\} = (\theta\theta_2)\{\varphi_1\}.$$

Mas, como $\theta \in G$ e $\theta_2 \in G$, também $\theta\theta_2 \in G$, visto que G é, por hipótese, um grupo; logo, a função $\theta\{\varphi_2\}$ será ainda uma conjugada de φ_1 em G. Análoga conclusão para as restantes funções $\varphi_3, \ldots, \varphi_m$.

Ponhamos então:

$$\theta\{\varphi_1\} = \varphi_{i_1}, \quad \theta\{\varphi_2\} = \varphi_{i_2}, \ldots, \theta\{\varphi_m\} = \varphi_{i_m}.$$

É claro que não poderá ser $\theta\{\varphi_i\} = \theta\{\varphi_k\}$ com $i \neq k$, visto que, efectuando θ^{-1} nos dois membros, viria $\varphi_i = \varphi_k$. Podemos pois garantir que os *índices* de $i_1, i_2, \ldots, i_m$ *são ainda os números* $1, 2, \ldots$ m *dispostos numa ordem possivelmente diversa, mas sem omissão nem repetição*. Em resumo: cada substituição θ sobre os zz determina uma substituição $\overline{\theta}$ sobre os $\varphi\varphi$:

$$\overline{\theta} = \begin{pmatrix} \varphi_{i_1} & \varphi_{i_2} & \cdots & \varphi_{i_m} \\ \varphi_1 & \varphi_2 & \cdots & \varphi_m \end{pmatrix};$$

isto é:

$$\overline{\theta}(\varphi_i) = \theta\{\varphi_i\}, \quad \text{para} \quad i = 1, 2, \ldots, m.$$

Note-se bem: θ é uma substituição *sobre os zz*, enquanto $\overline{\theta}$ é a substituição correspondente *sobre os* $\varphi\varphi$. A correspondência $\theta \to \overline{\theta}$ é unívoca, mas não necessariamente reversível: veremos que se pode ter $\overline{\theta}_1 = \overline{\theta}_2$, com $\theta_1 \neq \theta_2$. Além disso, ao produto $\sigma\theta$ de duas quaisquer substituições de G, corresponde precisamente o produto das substituições correspondentes sobre os $\varphi\varphi$:

$$\overline{\sigma\,\theta}\,(\varphi_i) = (\sigma\theta)\{\varphi_i\} = \sigma\{\theta\{\varphi_i\}\} = \overline{\sigma}\,(\overline{\theta}(\varphi_i)) = (\overline{\sigma}\,\overline{\theta})(\varphi_i).$$

Daqui se conclui que: a) a correspondência $\theta \to \overline{\theta}$ é um homomorfismo; b) o conjunto $\overline{G}$ de todas as substituições $\overline{\theta}$ obtidas sobre os $\varphi\varphi$ é um grupo (visto que G também o é).

Ocorre agora investigar quais as substituições de G que se traduzem na identidade em $\overline{G}$, isto é, ocorre determinar aquelas substituições de G (efectuadas sobre os *zz*), que convertem φ_1 em φ_1, φ_2 em $\varphi_2, \ldots,$ φ_m em φ_m. Ora, já sabemos que as substituições de G que deixam invariante cada função φ_i são precisamente as do grupo transformado

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

designando por θ_i uma das substituições de G que convertem φ_1 em φ_i e por H, como dissemos, o grupo a que pertence φ_1 em G ($i = 1, 2, \ldots, m$). As substituições de G que se traduzem na identidade sobre os $\varphi\varphi$ são pois as substituições comuns aos grupos

$$\theta_i H\,\theta_i^{-1}, \quad \text{para} \quad i = 1, 2, \ldots, m,$$

isto é, serão os elementos do grupo

$$N = H \cap \theta_2 H \theta_2^{-1} \cap \cdots \cap \theta_m H \theta_m^{-1}.$$

Em particular, pode ter-se

$$H = \theta_2 H \theta_2^{-1} = \cdots = \theta_m H \theta_m^{-1}$$

e portanto $H = N$. Já sabemos que, neste caso, o grupo H se diz invariante ou normal em G. Pois bem: *nesta última hipótese*, o grupo $\overline{G}$, considerado como grupo de substituições sobre os índices 1, 2,..., m (dos $\varphi\varphi$), chama-se *grupo cociente* de G por H e designa-se pela notação G/H.

Ilustremos estes factos com um exemplo. Consideremos, por um lado, o grupo alternante A_4 e, por outro lado, a função $u = z_1 z_3 + z_2 z_4$, pertencente ao grupo V_4 em A_4.

As conjugadas desta função em A_4 são

$$u_1 = z_1 z_3 + z_2 z_4,$$

$$u_2 = z_1 z_2 + z_3 z_4,$$

$$u_3 = z_1 z_4 + z_2 z_3.$$

No quadro seguinte estão indicadas, na coluna à esquerda, as substituições de A_4 (sobre os zz) e, na coluna à direita, as substituições correspondentes sobre os uu:

A_4	$\overline{A}_4$
I, (1 2) (3 4), (1 3) (2 4), (1 4) (2 3)	I
(1 2 3), (1 3 4), (2 4 3), (1 4 2)	(1 2 3)
(1 3 2), (1 4 3), (2 3 4), (1 2 4)	(1 3 2)

O grupo A_4 é pois constituído pelas potências do ciclo (1 2 3) e, como V_4 é invariante em A_4, podemos escrever $\overline{A}_4 = A_4/V_4$. Na coluna à esquerda, os elementos de A_4 encontram-se repartidos em três classes, que são precisamente as classes laterais de V_4 em A_4, a saber: V_4, (1 2 3) V_4 e (1 3 2) V_4.

Consideremos agora, em vez de A_4, o grupo simétrico S_4. Já sabemos que, em S_4, a função

$$u_1 = z_1 z_3 + z_2 z_4$$

pertence ao grupo Q_4 do quadrado. Mas Q_4 não é invariante em S_4: as substituições de S_4 que deixam invariantes, ao mesmo tempo, as três funções u_1, u_2, u_3 são as da intersecção

$$Q_4 \cap (1\ 2\ 3)\, Q_4 (1\ 3\ 2) \cap (1\ 3\ 2)\, Q_4 (1\ 2\ 3) = V_4 .$$

Neste caso, as substituições obtidas sobre os *uu*, são, além de *I*, (1 2 3), (1 3 2), ainda as transposições (1 2), (1 3), (2 3). Mas então o grupo $\overline{S}_4$, constituído por estas 6 substituições, coincidirá com S_3. Verifica-se pois, em particular, que

$$S_4 \sim S_3$$

27. Teoremas sobre homomorfismos. Noção geral de grupo cociente[1]

Convém, previamente, observar o seguinte facto:

Para que um subgrupo H de G seja invariante em G, é necessário e suficiente que o transformado

$$\theta\, \sigma\, \theta^{-1}$$

de cada elemento σ *de H por meio de cada elemento* θ *de G seja ainda um elemento de H; isto é, em símbolos*:

$$\theta H \theta^{-1} \subset H, \textit{ qualquer que seja } \theta \in H.$$

A condição é evidentemente necessária, pois que, por definição, o grupo *H* se diz invariante em *G* quando resulta,

$$\theta H \theta^{-1} = H, \text{ para todo o } \theta \in G.$$

---

(1) A leitura deste número não é indispensável para a compreensão do capítulo seguinte.

Suponhamos então que se tem

$$\theta H \theta^{-1} \subset H, \text{ qualquer que seja } \theta \in G.$$

Multiplicando ambos os membros, desta inclusão, à esquerda por θ^{-1} e à direita por θ, virá,

$$H \subset \theta^{-1} H \theta. \tag{4}$$

Mas θ^{-1} é um elemento de G; logo, em virtude da hipótese, ter-se-á

$$\theta^{-1} H (\theta^{-1})^{-1} \subset H,$$

donde, por confronto com (4):

$$\theta^{-1} H \theta = H$$

ou ainda

$$H = \theta H \theta^{-1}, \text{ qualquer que seja } \theta \in G.$$

A condição enunciada é pois suficiente.

Para comodidade de linguagem, convém ainda introduzir a seguinte noção: Dada uma transformação *unívoca* $\mathcal{C}$ dum conjunto A sobre um conjunto B, chamaremos *imagem inversa completa* de um qualquer elemento x de B, segundo $\mathcal{C}$, e representaremos por

$$\mathcal{C}^{(-1)}(x),$$

o conjunto de *todos* os elementos de A que são transformados em x por meio de $\mathcal{C}$; analogamente, chamaremos *imagem inversa completa* dum subconjunto M de B, e representaremos por

$$\mathcal{C}^{(-1)}(M),$$

o conjunto de todos os elementos de A que são transformados em elementos de M por meio de $\mathcal{C}$.

Posto isto, podemos demonstrar o seguinte teorema:

Em todo o homomorfismo $G \to \overline{G}$, a imagem inversa completa do elemento I de $\overline{G}$ é um grupo N invariante em G; a imagem inversa completa de cada elemento $\overline{\theta}$ de $\overline{G}$ é uma das classes laterais de N em G.

Seja com efeito T um homomorfismo de G sobre $\overline{G}$ e seja N o conjunto de todos os elementos de G que são transformados em I por meio de T (diz-se então que N é o núcleo do homomorfismo T). Ora, dados arbitrariamente $\sigma, \theta \in N$, virá $T(\sigma\theta) = T(\sigma) \cdot T(\theta) = I \cdot I = I$; logo também $\sigma\theta \in N$. Por outro lado

$$T(\sigma^{-1}) = [T(\sigma)]^{-1} = I,$$

e portanto $\sigma^{-1} \in N$. Podemos pois concluir que N é um grupo.

Sejam agora σ um elemento qualquer de N e θ um elemento qualquer de G. Virá

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

donde $\theta\,\sigma\,\theta^{-1} \in N$, o que significa que N é invariante em G.

Resta-nos provar a segunda parte do teorema. Seja $\overline{\theta}$ um elemento qualquer de $\overline{G}$ e seja θ um dos elementos de G tais que $T(\theta) = \overline{\theta}$. Proponhamo-nos então determinar todos os elementos ξ de G tais que $T(\xi) = \theta$. Ora tem-se

$$T(\theta^{-1}\xi) = [T(\theta)]^{-1}\,T(\xi) = \overline{\theta}^{-1}\,\overline{\theta} = I,$$

e portanto $\theta^{-1}\xi \in N$ ou seja

$$\xi \in \theta N.$$

A imagem inversa completa de $\overline{\theta}$, isto é, o conjunto de todos os elementos ξ de G que são transformados em $\overline{\theta}$ por meio de T, é pois a classe lateral θH de H em G, q.e.d..

Somos agora conduzidos a este outro resultado:

Se existem dois homomorfismos T, T' dum mesmo grupo G sobre dois grupos $\overline{G}$, $\overline{\overline{G}}$, respectivamente, e se os núcleos dos dois homomorfismos coincidem, podemos concluir que $\overline{G}$ é isomorfo a $\overline{\overline{G}}$.

Sejam com efeito T, T' dois homomorfismos nas condições do enunciado e seja N o núcleo comum de T e T'. Então, segundo o teorema precedente, existirá uma correspondência biunívoca $\overline{\theta} \rightarrow \theta N$ entre os elementos de $\overline{G}$ e as classes laterais de N em G; e, analogamente, uma correspondência *biunívoca* $\theta N \rightarrow \overline{\overline{\theta}}$, entre as classes laterais de N em G e os elementos de $\overline{\overline{G}}$; podemos assim definir directamente uma correspondência *biunívoca* $\overline{\theta} \rightarrow \overline{\overline{\theta}}$ entre os elementos de $\overline{G}$ e os de $\overline{\overline{G}}$. Ora esta correspondência é isomórfica. Com efeito, dados arbitrariamente $\overline{\theta}_1, \overline{\theta}_2 \in \overline{G}$, existirão em G pelo menos dois elementos θ_1, θ_2, tais que

$$T(\theta_1) = \overline{\theta}_1, \quad T(\theta_2) = \overline{\theta}_2;$$

então virá

$$T(\theta_1\, \theta_2) = T(\theta_1)\, T(\theta_2) = \overline{\theta}_1\, \overline{\theta}_2,$$

e, por outro lado,

$$T'(\theta_1\, \theta_2) = T'(\theta_1)\, T'(\theta_2) = \overline{\overline{\theta}}_1\, \overline{\overline{\theta}}_2.$$

Logo, ao produto $\overline{\theta}_1\, \overline{\theta}_2$ não pode deixar de corresponder em $\overline{\overline{G}}$ o produto $\overline{\overline{\theta}}_1\, \overline{\overline{\theta}}_2$, o que prova a afirmação feita.

Surge entretanto o seguinte problema:

Dados arbitrariamente um grupo G e um seu subgrupo invariante N, existirá sempre um homomorfismo de G sobre um segundo grupo $\overline{G}$, de modo que o núcleo desse homomorfismo seja precisamente N?

A esta questão responde-se afirmativamente, com a introdução de um conceito geral de "grupo cociente".

A noção de "grupo cociente" dada no n.º anterior tem o inconveniente de fazer intervir funções de $z_1, z_2, \ldots, z_n$, o que restringe a sua aplicabilidade aos grupos de substituições. Ora nós podemos definir tal noção com inteira generalidade: basta, para isso, fazer com que o papel das funções $\varphi_1, \varphi_2, \ldots, \varphi_m$ seja desempenhado pelas classes de H em G.

Seja pois G um grupo qualquer (finito ou infinito) e seja H um seu subgrupo invariante. As classes laterais de H em G:

$$H, \theta_2 H, \theta_3 H, \ldots$$

serão agora em número finito ou infinito. Ponhamos em geral

$$H_i = \theta_i H, \quad \text{com } \theta_1 = I,$$

e designemos por Λ a família destas classes H_i. Seja agora θ um elemento qualquer de G; multiplicando à esquerda por θ cada classe H_i, obter-se-á ainda uma classe lateral de H em G:

$$\theta H_i = \theta(\theta_i H) = (\theta\,\theta_i) H.$$

Ficará pois assim definida uma transformação unívoca $\overline{\theta}$ da família Λ sobre si mesma:

$$\overline{\theta} = \begin{pmatrix} \theta H, & \theta\theta_2 H, & \theta\theta_3 H, \ldots \\ H, & \theta_2 H, & \theta_3 H, \ldots \end{pmatrix},$$

ou seja, abreviadamente:

$$\overline{\theta}(H_i) = \theta \cdot H_i, \quad \text{para cada } H_i \in \Lambda. \tag{5}$$

Ora facilmente se reconhece que esta transformação $\overline{\theta}$ é biunívoca; a sua inversa, $\overline{\theta}^{-1}$, é precisamente,

$$\overline{\theta}^{-1}(H_j) = \theta^{-1} \cdot H_j, \quad \text{para cada } H_j \in \Lambda.$$

Podemos pois assentar em que, a cada elemento θ de G, fica deste modo a corresponder uma transformação biunívoca $\overline{\theta}$ da família Λ sobre si mesma. Ora a correspondência $\theta \rightarrow \overline{\theta}$ assim definida é um homomorfismo, pois que se tem, atendendo a (5)

$$(\overline{\sigma\,\theta})\,(H_i) = (\sigma\,\theta)\cdot H_i = \sigma\cdot(\theta\cdot H_i) =$$

$$= \overline{\sigma}\,(\overline{\theta}(\mathrm{H_i})) = (\overline{\sigma}\;\overline{\theta})\;(H_i),$$

isto é, $\overline{\sigma\,\theta} = \overline{\sigma}\;\overline{\theta}$, quaisquer que sejam σ, $\theta \in G$.

O conjunto $\overline{G}$ de todas as transformações $\overline{\theta}$ assim obtidas (sobre a família Λ) é portanto um grupo, ao qual chamaremos, precisamente, o *grupo cociente*, G/H, de G por H.

Vejamos agora qual o núcleo do homomorfismo $G \rightarrow \overline{G}$, isto é, procuremos determinar a totalidade dos elementos ξ de G que se traduzem na identidade $\overline{G}$:

$$\xi H_i = H_i, \text{ qualquer que seja } H_i \in \Lambda.$$

Ora esta igualdade é equivalente à seguinte

$$\xi\,(\theta_i\,H) = \theta_i\,H,$$

que é, por sua vez, equivalente a esta outra

$$(\theta_i^{-1}\,\xi\,\theta_i)\,H = H.$$

Então, pondo

$$\theta_i^{-1}\,\xi\,\theta_i = \eta,$$

segue-se que η é um elemento de H (pois que só nessa hipótese $\eta\,H = H$). Mas tem-se

$$\xi = \theta_i\,\eta\,\theta_i^{-1};$$

logo, também ξ será um elemento de H, visto ser H invariante em G. Podemos pois concluir que o núcleo do homomorfismo $G \to G/H$ coincide com H.

A tal homomorfismo dá-se, precisamente, o nome de *homomorfismo natural* de G, com o núcleo H.

Em resumo:

Dados um grupo G e um seu subgrupo invariante H, existe sempre um homomorfismo de G com o núcleo H: o homomorfismo natural $G \to G/H$. Para qualquer outro homomorfismo $G \to G'$ com o mesmo núcleo H, tem-se, necessariamente:

$$G' \cong G/H .$$

Esta última proposição é conhecida como o *teorema fundamental dos homomorfismos*.

Como exercício propomos a demonstração dos seguintes factos:

I – Em todo o homomorfismo $G \to \overline{G}$, cada elemento θ de G com período finito é transformado num elemento $\overline{\theta}$ de $\overline{G}$ cujo período é um divisor do período de θ.

II – O grupo cociente S_n/A_n é isomorfo ao grupo S_2, qualquer que seja $n = 2, 3, \ldots$.

III – O grupo *T das translações* é um subgrupo invariante no grupo G_d dos deslocamentos, o qual, por sua vez, é invariante no grupo $\overline{G}_s$ das semelhanças. O grupo *$G_d/\overline{T}$ é isomorfo ao grupo R_c das rotações em torno dum ponto c. O grupo G_s/G_d é isomorfo ao grupo H_c das homotetias em relação a um mesmo centro c.*

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:

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

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

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:

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

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

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

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

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

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

$$P = s_1^{3-1} s_2^{1-1} s_3^{1-1} s_4^1 = s_1^2 s_4$$
$$= (z_1 + z_2 + z_3 + z_4)^2 z_1 z_2 z_3 z_4 .$$

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 $z_1, z_2, \ldots, z_n$, e seja $u = \varphi(z_1, z_2, \ldots, z_n)$ uma qualquer função racional de $z_1, z_2, \ldots, z_n$. Representando por $u_1 (= u)$, $u_2, \ldots, u_m$ as funções conjugadas de u, podemos afirmar que *toda a função* $R(u_1, u_2, \ldots, u_m)$ *racional e simétrica em* $u_1, u_2, \ldots, u_m$ *será ainda, por intermédio destas variáveis, uma função racional e simétrica de* $z_1, z_2, \ldots, z_n$. Com efeito, visto que $u_1, u_2, \ldots, u_m$ 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 $R(u_1, u_2, \ldots, u_m)$, suposta simétrica em $u_1, u_2, \ldots, u_m$.

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

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

Pondo $\quad S_1 = \sum u_1,\ S_2 = \sum u_1 u_2,\ \ldots,\ S_m = u_1 u_2 \cdots u_m,$

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 $S_1, S_2, \ldots, S_m$ *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:

$$u_1 (= u),\quad u_2 = z_1 z_3 + z_2 z_4,\quad u_3 = z_1 z_4 + z_2 z_3.$$

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*

$$u = \frac{a z + b}{c z + d}$$

(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 $u_1 (= u)$, $u_2, \ldots, u_m$ as funções conjugadas de u, e por $v_1 (= v)$, $v_2, \ldots, v_m$, as funções correspondentes que se obtém a partir de v. Visto que o grupo G' da função $v = \varphi(z_1, z_2, \ldots, z_n)$ não coincide necessariamente com G, pode acontecer que as funções $v_1, v_2, \ldots, v_m$ 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 $c_1, c_2, \ldots, c_m$, por meio das condições

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

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

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

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 $z_1, z_2, \ldots, z_n$), seria necessário que duas, pelo menos, das funções $u_1, u_2, \ldots, u_m$ fossem idênticas. Mas, por hipótese, as funções $u_1, u_2, \ldots, u_m$ 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 $c_1, c_2, \ldots, c_m$ em *função racional* de $u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_m$, e portanto em *função racional* de $z_1, z_2, \ldots, z_n$. 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 $u = \varphi(z_1, z_2, \ldots, z_n)$ e $v = \psi(z_1, z_2, \ldots, z_n)$ podem reduzir-se a funções duma só variável:

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

Pode mesmo acontecer que se tenha

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

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

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

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

($i = 1, 2, \ldots, n$), sendo $c_1, c_2, \ldots, c_n$ 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 $\alpha_1, \alpha_2, \ldots, \alpha_n$).

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 obtém 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 $z_1, z_2, \ldots, z_n$ pelas raízes $\alpha_1, \alpha_2, \ldots, \alpha_n$ da equação considerada, vêm para $u_1, u_2, \ldots, u_n$ valores *finitos e determinados*:

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

Por comodidade de linguagem, continuaremos a dizer que β_1 é uma função racional de $\alpha_1, \alpha_2, \ldots, \alpha_n$ (muito embora os $\alpha\alpha$ sejam constantes) e que $\beta_1, \beta_2, \ldots, \beta_m$ 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* $\alpha_1, \alpha_2, \ldots, \alpha_n$ 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 $\mathcal{T}$. 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 $\mathcal{T}$.

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:

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

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:

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

Ter-se-á, como é fácil verificar:

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

Daqui resulta imediatamente que

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

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

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

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

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

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

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.° 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

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

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, $\mathscr{T}$ 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 $\mathcal{T}$ 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

$$G=\{I,\ (12),\ (34),\ (12)\ (34),\ (13)\ (24),\ (14)\ (23),\ (1324),\ (1423)\},$$

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

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

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

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.

Página em branco

CAPÍTULO V

NOÇÕES GERAIS DE GRUPO E CORPO

53. Axiomatização do conceito de grupo

Inicialmente, o conceito de "grupo", tal como o considerou GALOIS, dizia respeito unicamente a conjuntos de substituições. Mais tarde, por obra de SOPHUS LIE e de FELIX KLEIN, o conceito foi extendido a famílias de transformações biunívocas dum conjunto qualquer (finito ou infinito) sobre si mesmo. Sob esta forma o definimos no n.° 12: uma família não vazia de transformações diz-se um grupo, quando é fechada a respeito da multiplicação e da divisão (bastaria dizer "a respeito da divisão").

Mas o conceito de grupo extende-se expontaneamente a muitos outros domínios. Assim, por exemplo, é natural dizer que um conjunto não vazio de números, desprovido do elemento 0, forma um *grupo multiplicativo*, quando é fechado a respeito da divisão: o conjunto dos números racionais, excluído o zero, é um grupo multiplicativo; mas já o não é o conjunto dos inteiros. Um grupo multiplicativo – e até cíclico – é ainda o conjunto das raízes de índice n da unidade.

Por outro lado, é natural dizer que um conjunto não vazio de números forma um *grupo aditivo*, quando é fechado a respeito da adição e da subtracção (bastaria dizer "a respeito da subtracção"). É um grupo aditivo, por exemplo, o conjunto dos números inteiros,

positivos e negativos, o qual admite como subgrupo, entre outros, o conjunto dos números pares.

Este e muitos outros exemplos mostram a vantagem que pode haver numa definição geral de "grupo" e na construção de uma teoria abstracta, unificada, que englobe todas as possíveis concretizações deste conceito. O que desde logo se consegue por tal processo é uma notável economia de pensamento, evitando a repetição de raciocínios análogos em campos diversos, com terminologia e notações diversas. Por outro lado, este avizinhamento de ramos distintos da Matemática sob uma teoria comum é um dos mais fecundos recursos de que se têm valido até hoje o espírito criador dos matemáticos. Não se trata apenas de sistematizar, ou porventura assentar em base mais sólida, conhecimentos já adquiridos: trata-se dum autêntico método de investigação e descoberta, o chamado *método abstracto, formal ou axiomático*, que caracteriza todo o movimento das matemáticas modernas, desde a Álgebra à Topologia. Com tal orientação, a Matemática aproxima-se, por um lado, do campo da Lógica pura, ganhando em rigor e em beleza; enquanto, por outro lado, afastando-se só aparentemente da realidade concreta, se torna mais apta a penetrar no âmago das questões, por um maior poder de esquematização e de separação entre o que é essencial e o que é acidental.

Pode bem dizer-se, portanto, que a Matemática atinge, por esta via, um mais alto nível de racionalidade.

Vejamos pois como se define modernamente o conceito de "grupo" (segundo DEDEKIND). Seja H um conjunto não vazio de elementos $a, b, c, \ldots$ de natureza qualquer, e seja ϕ uma operação binária definida entre elementos de H, isto é, um processo de composição, pelo qual, a cada par ordenado (a, b) de elementos de H, devidamente escolhido, fique associado um terceiro elemento c de H.

Os elementos a, b dizem-se os *dados da operação* ϕ e o elemento c chama-se *resultado da operação* ϕ *aplicada aos elementos* a, b. Este elemento c pode ser representado indiferentemente pelos símbolos $\phi(a, b)$ ou $a \phi b$. Posto isto, diz-se que o conjunto H é um *grupo a respeito da operação* ϕ se, e só se, resultam verificadas as três seguintes condições:

g_1) A operação ϕ é *univocamente definida* em todo o conjunto H; isto é, para cada par ordenado (a, b) de elementos de H, existe um e um só elemento $c = a\phi b$.

g_2) A operação ϕ é *associativa*; isto é, tem-se

$$(a\phi b)\phi c = a\phi(b\phi c),$$

quaisquer que sejam $a, b, c \in H$.

g_3) A operação ϕ é *invertível*; isto é, dados dois elementos a, b quaisquer de H, é sempre possível encontrar em H elementos x, y tais que

$$a\phi x = b, \quad y\phi a = b.$$

Pode acontecer que, além destas, seja ainda verificada em H a condição seguinte:

g_c) $a\phi b = b\phi a$, quaisquer que sejam $a, b \in H$.

Neste caso, H diz-se um grupo *comutativo ou abeliano*. (Em geral, dois elementos a, b de H dizem-se *permutáveis*, quando se tem $a\phi b = b\phi a$).

Por exemplo, o conjunto dos números inteiros (positivos e negativos, incluido o zero) é um grupo comutativo a respeito da adição, mas já não é um grupo a respeito da subtracção, pelo facto de esta operação não ser associativa: não é lícito escrever em geral $(a-b)-c = a-(b-c)$.

Sempre que, num conjunto H, se encontra definida uma operação ϕ, o conjunto H diz-se *algebrizado* por esta operação, mesmo que não forme um grupo a respeito dela.

Observemos desde já que a família S de todas as transformações biunívocas dum conjunto A sobre si mesmo, algebrizada com a operação usual de produto, constitui um grupo segundo a presente definição, visto que nessa família são verificadas as condições g_1), g_2), g_3). Posto isto, para saber se uma dada subfamília M de S constitui ainda um grupo conforme a definição geral (a respeito da mesma operação de produto), basta averiguar se a família M é fechada a respeito da divisão, pois que, nessa hipótese, e só nessa, as condições g_1), g_2), g_3) resultam verificadas em M. O conceito actual de grupo é pois uma generalização do conceito definido no n.° 12.

Outros exemplos:

a) Seja R o conjunto dos números reais e φ a operação definida pela fórmula

$$x\varphi y = \sqrt[3]{x^3 + y^3};$$

facilmente se reconhece que R é um grupo a respeito de φ. Mas, a respeito da operação θ definida por

$$x\theta y = + \sqrt{x^2 + y^2}$$

já R não é um grupo, pela simples razão de que θ não é invertível.

b) Seja $\mathfrak{F}$ a família de todos os subconjuntos dum dado conjunto A não vazio. Em $\mathfrak{F}$ são definidas univocamente duas equações binárias – a intersecção ($\cap$) e a reunião ($\cup$) – ambas associativas e comutativas, mas nenhuma delas invertível. O conjunto $\mathfrak{F}$ não é portanto um grupo a respeito de qualquer destas operações.

c) Consideremos o conjunto $U = \{a, b\}$ e as operações φ, θ, definidas em U mediante as seguintes tabelas:

$x\varphi y$

x \ y	a	b
a	a	b
b	b	a

$x\theta y$

x \ y	a	b
a	a	a
b	a	b

É fácil ver que o conjunto U forma um grupo a respeito de φ, mas não já a respeito de θ, pois que não existe em U nenhum elemento x tal que $x\theta a = b$.

54. Primeiras consequências da axiomática dos grupos

A partir dos axiomas g_1), g_2), g_3) pode desenvolver-se, por dedução lógica, toda a teoria formal dos grupos.

Seja H um grupo a respeito duma dada operação ϕ. Tomado em H um elemento c qualquer, existirá necessariamente em H, por força de g_3), um elemento μ tal que $\mu\phi c = c$. Ora é de notar que este elemento μ goza da propriedade

$$\mu\phi a = a, \text{ qualquer que seja } a \in H.$$

Com efeito, ainda em virtude de g_3), existirá em H pelo menos um elemento x, tal que $c\phi x = a$, donde, atendendo a g_2):

$$\mu\phi a = \mu\phi(c\phi x) = (\mu\phi c)\phi x = c\phi x = a.$$

Ao elemento μ chamaremos *módulo da operação* ϕ (à esquerda). Analogamente se demonstra a existência de (pelo menos) um elemento υ de H, tal que

$$a\phi\upsilon = a, \text{ qualquer que seja } a \in H,$$

ao qual poderíamos chamar *módulo de operação* θ *à direita*. Simplesmente, o módulo à direita coincide com o módulo à esquerda, pois que:

$$\mu\phi\upsilon = \upsilon, \ \mu\phi\upsilon = \mu, \text{ donde } \mu = \upsilon.$$

Este mesmo raciocínio mostra que não pode haver mais de um módulo de cada lado.

Note-se que, usualmente, a operação grupal se apresenta umas vezes com o nome de "multiplicação", outras vezes com o nome de "adição". No primeiro caso, tem lugar a *linguagem multiplicativa*: o resultado da operação aplicada aos elementos dados *a, b* chama-se *produto* de *a* por *b* e representa-se por $a \cdot b$ ou ab; o módulo da operação chama-se *unidade* e pode representar-se por 1 (muitos autores usam o símbolo *e*), etc. No segundo caso, emprega-se a *linguagem aditiva*: em vez de *produto* (ab), diz-se *soma* ($a+b$); em vez de *unidade* (1), diz-se *zero* (0), etc.

Continuemos a usar ϕ como símbolo genérico de operação grupal em H. O axioma g_3) habilita-nos ainda a afirmar que, *para cada*

$a \in H$, *existe (pelo menos) um elemento* $\bar{a}$ *de* H, *tal que* $\bar{a}\phi a = \mu$ (*continuando a designar por* μ *o módulo de* ϕ).

Daqui resulta a univocidade da operação inversa de ϕ: *quaisquer que sejam* $a, b \in H$, *não pode haver mais de um elemento* x *tal que* $a\phi x = b$, *nem mais dum elemento* y *tal que* $y\phi a = b$. Com efeito, se for $a\phi x = a\phi x'$, virá, sucessivamente,

$$\bar{a}\phi(a\phi x) = \bar{a}\phi(a\phi x') \text{ ou seja } \mu\phi x = \mu\phi x',$$

donde, finalmente, $x = x'$. Analogamente se demonstra a segunda parte da proposição.

Em particular, podemos garantir que, para cada $a \in H$, existe *um, e um só*, elemento a de H, tal que $\bar{a}\phi a = \mu$. Em linguagem multiplicativa, o elemento a chama-se *o inverso* (à esquerda) de a e representa-se por a^{-1}; em linguagem aditiva, $\bar{a}$ chama-se o *simétrico* (*à esquerda*) de a e representa-se por $-a$. *Mas o inverso à esquerda também é inverso à direita*; isto é, tem-se não só

$$a^{-1}a = 1,$$

mas ainda $a\,a^{-1} = 1$. Com efeito, de $a^{-1}a = 1$, vem

$$(a^{-1}a)\,a^{-1} = a^{-1}$$

ou seja

$$a^{-1}(a\,a^{-1}) = a^{-1},$$

donde, multiplicando à esquerda por a:

$$a\,a^{-1} = 1, \qquad \text{q.e.d.}$$

Este mesmo resultado mostra que $(a^{-1})^{-1} = a$.

55. Representação dum grupo qualquer mediante um grupo de transformações

As noções de "homomorfismo", "isomorfismo" e "automorfismo" atrás formuladas para os grupos de transformações extendem-se automaticamente ao novo conceito de grupo. Sejam G_1, G_2 dois

grupos quaisquer, relativos a operações ϕ_1, ϕ_2, definidas respectivamente em G_1 e G_2; chamaremos *homomorfismo* do grupo G_1 sobre o grupo G_2 toda a transformação unívoca τ do primeiro sobre o segundo, tal que

1) $\tau(G_1) = G_2$,

2) $\tau(a \phi_1 b) = \tau(a) \phi_2 \tau(b)$ quaisquer que sejam $a, b \in G_1$.

Se τ é além disto reversível, diz-se um *isomorfismo*, e prova-se que a sua inversa τ^{-1} é também um isomorfismo.

Assim, por exemplo, o operador *log* estabelece um isomorfismo entre o grupo multiplicativo dos números positivos e o grupo aditivo dos números reais:

$$log\,(x \cdot y) \equiv log\, x + log\, y\,.$$

No desenvolvimento da teoria geral dos grupos, é cómodo adoptar uma só das linguagens – aditiva ou multiplicativa. Comummente opta-se pela segunda, e é o que faremos a partir deste momento.

Consideremos um grupo G qualquer. Designando por a um elemento arbitrário de G, é fácil ver que a fórmula

$$y = ax \tag{26}$$

define uma transformação biunívoca do conjunto G sobre si mesmo, pois que; 1) a cada $x \in G$ fica a corresponder um e um só elemento $y (= ax)$ de G; 2) reciprocamente, para cada elemento y de G, existe um e um só elemento x de G, tal que $ax = y$: o elemento $x = a^{-1}y$.

Mas o elemento a de G é arbitrário. Deste modo, para cada $a \in G$, tem-se uma transformação biunívoca de G sobre si mesmo, transformação que designaremos por f_a:

$$f_a(x) = ax, \text{ para cada } x \in G\,.$$

(Assim, por exemplo, se G for o grupo multiplicativo dos números positivos, f_2 será o operador que transforma 1 em 2, -3 em -6, 3/4 em 3/2, etc.)

Não oferece agora dificuldade demonstrar que: *o conjunto* $\overline{G}$ *de todas as transformações* f_a *assim obtidas (quando a percorre G) é um grupo*; e que: *a correspondência* $a \to f_a$ *é um isomorfismo de G sobre* $\overline{G}$.

Com efeito, dados dois elementos a, b quaisquer de G, tem-se:

$$f_a(x) = ax, \quad f_b(x) = bx, \quad \text{para cada } x \in G,$$

e portanto

$$(f_a f_b)(x) = f_a(f_b(x)) = a(bx) = (ab)x = f_{ab}(x).$$

Tem-se pois que, no produto ab, corresponde precisamente o produto $f_a f_b$ ou seja, em símbolos

$$f_{ab} = f_a \cdot f_b,$$

o que significa, precisamente, que a correspondência $a \to f_a$ é um homomorfismo de G sobre $\overline{G}$. Daqui resulta logo que $\overline{G}$ também é um grupo. Finalmente, é fácil ver que a referida correspondência é biunívoca, pois que a desigualdade $a \neq b$ implica $f_a \neq f_b$. Com efeito, se fosse $f_a = f_b$, ter-se-ia em particular $f_a(1) = f_b(1)$ ou seja $a \cdot 1 = b \cdot 1$, donde $a = b$.

O facto que acabamos de estabelecer tem grande importância e pode enunciar-se nestes termos: *todo o grupo G é representável isomorficamente mediante um grupo de transformações*. Deste modo, uma vez que os isomorfismos respeitam (por definição) as propriedades algébricas dos grupos, somos levados a concluir que *todos os anteriores teoremas com carácter exclusivamente algébrico, relativos a grupos de transformações, podem ser transportados ao domínio geral dos grupos abstractos que não se encontre já representado na teoria dos grupos de transformações*.

56. Axiomatização do conceito de corpo

Observemos que todo o corpo numérico Δ é um grupo comutativo a respeito da adição e que, privado do elemento 0, é ainda um grupo (comutativo) a respeito da multiplicação; além disso, a multiplicação

é, em Δ, distributiva a respeito da adição. Daqui se parte para a noção geral de corpo: Seja M um conjunto de elementos quaisquer, algebrizado por meio de duas operações, uma das quais convencionaremos chamar *adição* e a outra *multiplicação*; diz-se que M é um *corpo* a respeito destas operações, quando são verificadas as seguintes condições:

c_1) O conjunto M é um grupo comutativo a respeito da adição;
c_2) Privado do elemento 0, o conjunto M é um grupo a respeito da multiplicação;
c_3) Em M, a multiplicação é *distributiva à direita e à esquerda* a respeito da adição; isto é, tem-se, quaisquer que sejam $a, b, c \in M$:

$$a(b+c) = ab + ac; \quad (b+c)a = ba + ca.$$

c_4) $a \cdot 0 = 0$, qualquer que seja $a \in M$.
Esta condição pode ainda ser substituída pela condição mais fraca:
c_4') O produto de 0 por cada elemento de M é sempre um determinado elemento de M (que se demonstra depois ser 0).

Se, além disto, a multiplicação for comutativa em M, dir-se-á que M é um *corpo comutativo*.

Os corpos de números e de funções atrás considerados reentram, manifestamente, na actual definição. Mas note-se que, por exemplo, o conjunto C de todas as funções contínuas num intervalo (a, b) não é um corpo, a respeito das noções usuais de soma e do produto de funções; com efeito, se designarmos por f uma função que se anule em metade do intervalo (a, b), mas não na outra metade (existam tais funções em C), o elemento $1/f$ não pertencerá a C, e tem-se, contudo, $f \neq 0$.

Exemplos notáveis de corpos são os seguintes:

Representando por E o conjunto dos inteiros, positivos e negativos, zero incluído, e fixado em E um elemento m qualquer, já sabemos (n.° 18) que a relação de congruência a respeito do módulo m determina em E uma repartição. Suponhamos, para fixar ideias, $m = 3$, e convencionemos representar por $\overline{a}$ o conjunto dos elementos de E congruentes a a mod. 3, sendo a um elemento arbitrário de E.

É claro que, neste caso, se tem uma repartição de E apenas em três classes: $\overline{0}$, $\overline{1}$, $\overline{2}$. (Note-se que é $\overline{0} = \overline{3} = \overline{6} = \cdots$, $\overline{1} = -\overline{2} = \overline{7} \cdots$, $\overline{2} = -\overline{4} = \overline{8} = \cdots$). Representemos por $\overline{E}$ o conjunto $\{\overline{0}, \overline{1}, \overline{2}\}$. É natural agora definir soma e produto de dois elementos $\overline{a}$, $\overline{b}$ de $\overline{E}$, mediante as fórmulas:

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a}\,\overline{b} = \overline{a\,b}.$$

Teremos então as duas seguintes tabelas de adição e multiplicação em $\overline{E}$:

$x + y$

x \ y	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$x \cdot y$

x \ y	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

É fácil constatar que o conjunto E assim algebrizado é um corpo comutativo.

Ter-se-ia obtido ainda um corpo comutativo (e finito), se, em vez de $m = 3$, se tivesse tomado para m um valor primo qualquer. Todavia, se m não for um número primo, o sistema algébrico obtido por este processo não será um corpo, como se pode verificar.

Uma das questões centrais da moderna Álgebra abstracta é esta: sendo C um corpo arbitrário, determinar uma condição necessária e suficiente para que a teoria de GALOIS seja válida para as equações algébricas com os coeficientes em C.

Para um estudo desenvolvido das teorias dos grupos, dos corpos, bem como de outros sistemas algébricos, podem consultar-se várias obras, nomeadamente a de VAN DER WAERDEN, *Moderne Algebra.*

O presente curso não pretende ser mais do que uma introdução às referidas teorias.

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)**