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.*

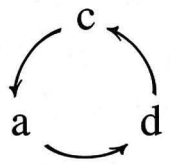
11. Substituições cíclicas

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.

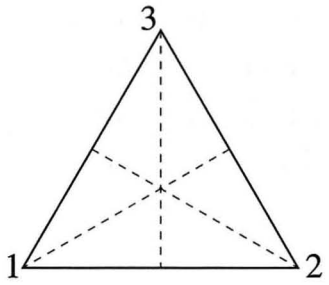


Fig. 1

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).

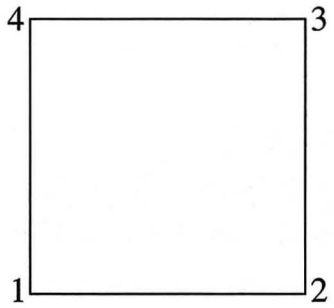


Fig. 2

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.

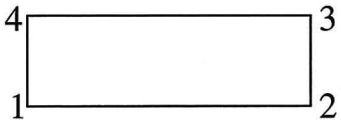


Fig. 3

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.

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)**