I.1

INTRODUÇÃO ÀS MODERNAS TEORIAS ALGÉBRICAS

(Apenas o esboço dum curso de iniciação)

Página em branco

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.

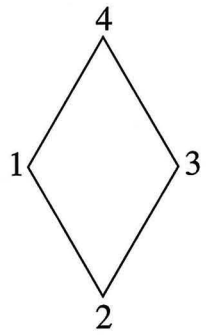

Fig. 4

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

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

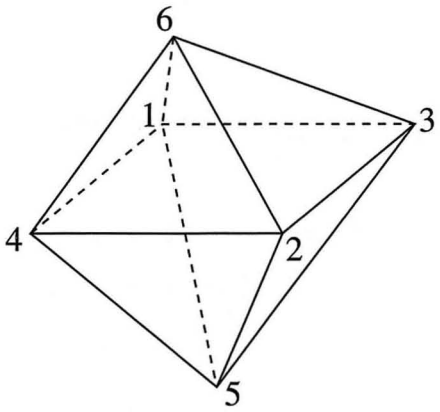

Fig. 5

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.*

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)**