3. Grupos Finitos e Técnicas de Enumeração

Um **grupo** G é um par ordenado $(X,\otimes)$ que consiste num conjunto X onde está definida a lei de composição interna (operação) $\otimes$ que satisfaz as seguintes propriedades:

1. $\forall x,y,z\in X,\ x\otimes(y\otimes z)=(x\otimes y)\otimes z$ (associatividade);
2. $\exists e\in X$ tal que $\forall x\in X,\ x\otimes e=e\otimes x=x$ (existe elemento neutro [15]);
3. $\forall x\in X,\ \exists x^{-1}\in X$ tal que $x\otimes x^{-1}=x^{-1}\otimes x=e$ (todos os elementos têm inverso [16]).

O grupo G diz-se finito se X é um conjunto finito. Se $|X|=n$ diz-se que G é de **ordem** n. Por abuso de linguagem, em geral, identificamos o conjunto dos elementos de um grupo G por G e, por economia, escreve-se xy em vez de $x\otimes y$, x^2 em vez de xx, x^{-2} em vez de $x^{-1}x^{-1}$, etc. Algumas vezes também se denota o elemento neutro de G, *e*, por x^0, onde x é um elemento arbitrário de G.

Por exemplo, $G=(X,\oplus)$, onde $X=\mathbf{N}_n\cup\{0\}$ e $x\oplus y=\begin{cases} x+y \text{ se } x+y<n \\ x+y-n \text{ se } x+y\geq n \end{cases}$, é um grupo de ordem n.

Um grupo G diz-se **abeliano** se $xy=yx\ \forall x,y\in G$. No caso contrário G diz-se não abeliano (no exemplo anterior, G é um grupo abeliano).

Existem dois modos de representar as permutações de elementos de um conjunto arbitrário, X. O **modo activo** que consiste na identificação de cada permutação por uma bijecção, $\pi:X\rightarrow X$, e o **modo passivo** que consiste na identificação da permutação por intermédio do n-uplo das imagens por π de cada um dos elementos de X, i. e, considerando que existe uma ordem natural para os elementos de X ($X=\{x_1,\ldots,x_n\}$) a representação passiva da permutação π corresponde ao n-uplo $(\pi(x_1),\ldots,\pi(x_n))$.

O **grupo simétrico**, S_n (de ordem n!), consiste no conjunto de todas as permutações de $\mathbf{N}_n$, identificadas activamente pelas respectivas bijecções entre $\mathbf{N}_n$ e $\mathbf{N}_n$,

---

[15] Prova-se que este elemento neutro é único.

[16] Igualmente se prova que cada elemento tem um único inverso.

munido da lei de composição interna, $\otimes$, que corresponde à composição destas bijecções. Um modo prático e conveniente de escrever cada elemento de S_n consiste na utilização da designada **notação cíclica** ou circular. Por exemplo, a permutação $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 4 & 1 & 5 & 2 \end{pmatrix}$ em representação cíclica (ou circular) toma um das formas (1 3 4)(2 6)(5), (2 6)(1 3 4)(5), (1 3 4)(5)(2 6), (2 6)(5)(1 3 4), (5)(1 3 4)(2 6) ou (5)(2 6)(1 3 4), qualquer delas significando que $\pi(1)=3$, $\pi(3)=4$, $\pi(4)=1$, $\pi(2)=6$, $\pi(6)=2$ e $\pi(5)=5$.

Note-se que, para qualquer permutação de elementos de $X=\{x_1,\ldots,x_i,\ldots,x_n\}$, a representação cíclica $(x_1 \ldots x_{i-1}\ x_i \ldots x_n)$ é uma representação activa (e não passiva), uma vez que os ciclos não são únicos, podendo iniciar-se em qualquer dos seus elementos. Por exemplo, o ciclo anterior pode denotar-se por $(x_i \ldots x_n\ x_1 \ldots x_{i-1})$.

Designa-se por **comprimento de um ciclo** o número dos elementos que o constituem. Por exemplo, o ciclo $(i_1 \ldots i_k)$ tem comprimento k.

Considerando os produtos de ciclos, (1 4 7 6 2)(3 8)(5) e (1 5 4 3 2)(6 7 8), que correspondem, respectivamente, às permutações de S_8 que se definem pelas bijecções, $\pi_1:\mathbf{N}_8\rightarrow\mathbf{N}_8$, tal que $\pi_1(1)=4$, $\pi_1(4)=7$, $\pi_1(7)=6$, $\pi_1(6)=2$, $\pi_1(2)=1$, $\pi_1(3)=8$, $\pi_1(8)=3$ e $\pi_1(5)=5$ e $\pi_2:\mathbf{N}_8\rightarrow\mathbf{N}_8$, tal que $\pi_2(1)=5$, $\pi_2(5)=4$, $\pi_2(4)=3$, $\pi_2(3)=2$, $\pi_2(2)=1$, $\pi_2(6)=7$, $\pi_2(7)=8$ e $\pi_2(8)=6$, a composição das respectivas bijecções vem dada por

$$(1\ 4\ 7\ 6\ 2)(3\ 8)(5)\otimes(1\ 5\ 4\ 3\ 2)(6\ 7\ 8) = (1\ 3\ 6)(2\ 5\ 4\ 8)(7)$$

(tendo em conta que, de acordo com as regras de composição, se obtém $1\rightarrow4\rightarrow3$, $3\rightarrow8\rightarrow6$, $6\rightarrow2\rightarrow1$, $2\rightarrow1\rightarrow5$, $5\rightarrow5\rightarrow4$, $4\rightarrow7\rightarrow8$, $8\rightarrow3\rightarrow2$ e $7\rightarrow6\rightarrow7$).

Dois ciclos, $(i_1 \ldots i_p)$ e $(j_1 \ldots j_q)$, dizem-se **disjuntos** se $\{i_1,\ldots,i_p\}\cap\{j_1,\ldots,j_q\}=\varnothing$.

3.1 Teorema

Toda a permutação $\pi\in S_n$ pode ser escrita, de modo único (a menos da ordem), como produto de ciclos disjuntos.

Prova:

Vamos fazer a prova por indução sobre n, tendo em conta que o resultado é trivialmente verdadeiro para n=1.

Seja $n\geq 2$ e, a partir de um elemento arbitrário i_1, considerem-se as imagens consecutivamente obtidas por π até à primeira repetição de elementos, i. e, sejam $i_2=\pi(i_1)$, $i_3=\pi(i_2)$, … , $i_k=\pi(i_{k-1})$ tais que i_1, i_2, … , i_k são todos elementos de $\mathbf{N}_n$ distintos e $\pi(i_k)=i_{k+1}\in\{i_1,\ldots,i_k\}$. Então pode concluir-se que $i_{k+1}=i_1$, caso contrário $i_{k+1}=i_j\in\{i_2,\ldots,i_k\}$ e, consequentemente, $\pi(i_k)=i_j=\pi(i_{j-1})$, o que contraria a injectividade de π. Deste modo obtém-se o ciclo de elementos distintos

$$c_1=(i_1\ i_2\ i_3\ \ldots\ i_k)=(i_1\ \pi(i_1)\ \pi^2(i_1)\ \ldots\ \pi^{k-1}(i_1))$$

que tem comprimento k e é o único ciclo, da decomposição de π, onde está envolvido i_1.

Se k=n, então o resultado verifica-se. Caso contrário, sendo $I=\{i_1,\ldots,i_k\}$ vem que $J=\mathbf{N}_n\backslash I$ constitui o subconjunto de $\mathbf{N}_n$ que não é afectado pelo ciclo c_1 de comprimento k, logo, uma vez que J tem cardinalidade n-k e é invariante relativamente a π, podemos considerar a restrição de π a J, $\pi_{|J}$, como sendo um elemento de S_{n-k} e, por hipótese de indução, que $\pi_{|J} = c_2\ \ldots\ c_r$, onde c_2, … c_r, são ciclos disjuntos que são únicos (a menos da ordem). Consequentemente, podemos concluir que $\pi=c_1c_2\ldots c_r$ constitui uma decomposição única (a menos da ordem) em produtos de ciclos disjuntos.

♦

Um ciclo de comprimento 2 designa-se por **transposição** e um ciclo de comprimento 1 designa-se por **ponto fixo**.

Em geral, quando se adopta a notação cíclica para representar permutações, por convenção, os pontos fixos não são mencionados explicitamente. Assim, por exemplo, a permutação (1 3 6)(2 5 4 8)(7) denota-se, simplesmente, por (1 3 6)(2 5 4 8).

Prova-se que todo o ciclo pode ser decomposto num produto de transposições e, consequentemente, que S_n é gerado pelo conjunto de todas as transposições. Com efeito, dado um ciclo arbitrário $(j_1\ j_2\ \ldots\ j_{k-1}\ j_k)$, basta considerar a decomposição

$$(j_1\ j_2 \cdots j_{k-1}\ j_k) = (j_1\ j_2)(j_1\ j_3) \cdots (j_1\ j_k).$$

Deve observar-se ainda que a inversa de uma transposição é a propria tansposição, uma vez que do produto $(\alpha\ \beta)(\alpha\ \beta)$ se obtém $\alpha\rightarrow\beta\rightarrow\alpha$ e $\beta\rightarrow\alpha\rightarrow\beta$. Nestas condições, supondo que a permutação identidade se decompõe no produto de um número par de transposições, após reordenação conveniente destas transposições, é possível reduzir o número de transposições até zero. Com efeito, a partir da decomposição da permutação identidade de S_n, $id=(\tau_1\ \tau'_1) \cdots (\tau_p\ \tau'_p)$ (onde p é par), pode obter-se a decomposição, $id=(\alpha_1\ \beta_1)\ldots(\alpha_k\ \beta_k)(\alpha_{k+1}\ n)\ldots(\alpha_{k+s}\ n)$ onde as últimas s transposições são as únicas que envolvem n. Para tal, sendo a, b e c três elementos distintos do conjunto {1,2,…,n-1}, basta utilizar, adequadamente, as igualdades (a n)(a b)=(a b)(b n) e (c n)(a b)=(a b)(c n) (observe-se que $\forall\alpha\in\mathbf{N}_n$ $(\alpha\ n)=(n\ \alpha)$). Consequentemente, tendo ainda em conta que

$$(\alpha'\ n)(\alpha''\ n)=(\alpha'\ \alpha'')(\alpha'\ n),$$

é possível juntar e eliminar, consecutivamente, as transposições que envolvem n e são iguais, o que implica o desaparecimento de todas as transposições onde consta n. Caso contrário, obter-se-ia uma decomposição da forma $id=(\alpha_1\ \beta_1) \cdots (\alpha_k\ \beta_k)(\delta_1\ n) \cdots (\delta_r\ n)$ com $\delta_1, \ldots, \delta_r$ todos distintos, pelo que, uma vez que n não consta em nenhuma das transposições $(\alpha_1\ \beta_1) \cdots (\alpha_k\ \beta_k)$, partindo da transposição $(\delta_1\ n)$ concluir-se-ia que $id(n)\in\{1,\ldots,n-1\}$ [17] o que é contraditório. Procedendo, de um modo idêntico ao anteriormente referido, consecutivamente, para n-1, n-2, … ,1 conclui-se o pretendido. Desta análise decorre, adicionalmente, que o número par mínimo de transposições para a decomposição da permutação identidade é zero e, este facto, vai ser especialmente útil na prova do teorema 3.2 a apresentar mais adiante.

Como exemplo de aplicação dos procedimentos referidos na análise anterior, vamos considerar a permutação $\pi=(1\ 3)(3\ 6)(2\ 5)(4\ 6)(4\ 2)\in S_6$, i. e, $\pi=\begin{pmatrix}1&2&3&4&5&6\\2&5&1&6&4&3\end{pmatrix}$,

[17] Deve ter-se em conta que $\delta_1\in\{1,\ldots,n-1\}$.

e proceder à substituição sucessiva dos factores em jogo, até que as transposições onde consta 6 ocupem as posições mais à direita.

1. A partir a igualdade (3 6)(2 5)=(2 5)(3 6), e procedendo à respectiva substituição, obtém-se π=(1 3)(2 5)(3 6)(4 6)(4 2).

2. Por sua vez, a partir da igualdade (4 6)(4 2)=(4 2)(2 6), modificando o produto de transposições, vem π=(1 3)(2 5)(3 6)(4 2)(2 6).

3. Finalmente, a partir da equação (3 6)(4 2)=(4 2)(3 6), obtém-se π na forma pretendida, i. e, π=(1 3)(2 5)(4 2)(3 6)(2 6).

3.2 Teorema

A permutação identidade id$\in S_n$ não se pode escrever como produto de um número impar de transposições.

Prova:

Suponha-se que a permutação identidade de S_n admite a decomposição:

$$id=(\tau_1\ \tau'_1)(\tau_2\ \tau'_2)\ldots(\tau_q\ \tau'_q),$$

onde q é o menor impar em tais condições.

Tal como anteriormente, vamos separar as transposições que envolvem n das restantes, modificando a factorização apresentada de modo a obter

$$id=(\alpha_1\ \beta_1)\ldots(\alpha_k\ \beta_\kappa)(\alpha_{k+1}\ n)\ldots(\alpha_{k+s}\ n).$$

Nestas condições, pode concluir-se que α_{k+1}, … , α_{k+s} são todos distintos (caso contrário, tal como se fez anteriormente, existindo $\alpha_{k+i}=\alpha_{k+j}$, com i,j$\in${1,…,s} e i<j, poder-se-ia "empurrar" a transposição (α_{k+i} n), até ela se tornar vizinha de (α_{k+j} n) o que implicaria o seu anulamento e a contraditória diminuição do número de transposições). Consequentemente, a partir da transposição (α_{k+1} n) conclui-se que id(n)$\in${1,…,n-1}, o que é absurdo.

♦

Deste teorema decorre, de um modo imediato, o seguinte corolário.

3.3 Corolário

Se uma permutação $\pi \in S_n$ se pode escrever como produto de um número par de transposições, então não é possível escreve-la como produto de um número impar de transposições.

Prova:

Supondo que π se pode escrever como produto de um número par de transposições e, também, como produto de um número impar, i. e, $\pi=\tau_1\tau_2\ldots\tau_p=\rho_1\rho_2\ldots\rho_q$, onde τ_i para i=1,…,p e ρ_j para j=1,…,q são transposições, com p par e q impar, vem que

$$id=\tau_p^{-1}\ldots\tau_2^{-1}\tau_1^{-1}\pi=\tau_p^{-1}\ldots\tau_2^{-1}\tau_1^{-1}\rho_1\rho_2\ldots\rho_q=\tau_p\ldots\tau_2\tau_1\rho_1\rho_2\ldots\rho_q,$$

pelo que id admite uma decomposição num produto de p+q (impar) transposições, o que contraria o teorema 3.2.

♦

Com base neste corolário podemos introduzir os conceitos de permutação par e de permutação impar. Assim, designa-se por **permutação par**, toda a permutação que admite uma decomposição num produto de um número par de transposições e por **permutação impar** toda a que se decompõe no produto de um número impar.

Deve observar-se que se uma dada permutação é representada por um ciclo de comprimento k, de acordo com a factorização em transposições, apresentada na página 34, se k é par, então a permutação é impar, e se k é impar, então a permutação é par.

Sendo A_n o subconjunto de S_n que contém todas as permutações pares, prova-se que A_n é um grupo (esta prova é proposta no exercício 3.1) e este grupo designa-se por **grupo alterno** ou **alternante**.

Conforme a seguir se exemplifica, para $n\geq 3$, o grupo simétrico, S_n, não é abeliano. Com efeito, por exemplo

$$(1\ 3\ 2)(1\ 3)(2)=(1)(2\ 3)\neq(1\ 2)(3)=(1\ 3)(2)(1\ 3\ 2),$$

uma vez que no primeiro membro se obtém $1\rightarrow 3\rightarrow 1$, $2\rightarrow 1\rightarrow 3$, $3\rightarrow 2\rightarrow 2$ e, no segundo membro, $1\rightarrow 3\rightarrow 2$, $2\rightarrow 2\rightarrow 1$ e $3\rightarrow 1\rightarrow 3$.

Um **homomorfismo**, f, entre o grupo $G=(X,\otimes_x)$ e grupo $H=(Y,\otimes_y)$ é uma aplicação que preserva a estrutura da operação, i. e, $f(g\otimes_x h)=f(g)\otimes_y f(h)$ $\forall g,h\in X$. No caso do homomorfismo ser uma bijecção, dizemos que se trata de um **isomorfismo** e que G_1 e G_2 são isomorfos, denotando-se esta propriedade por $G_1\approx G_2$. Um homomorfismo injectivo diz-se um **monomorfismo** e um homomorfismo sobrejectivo diz-se um **epimorfismo**. Por sua vez, um isomorfimo de um grupo G em si próprio designa-se por **automorfismo**.

Dados dois grupos $G_1=(X,\otimes)$ e $G_2=(Y,\oplus)$ designa-se por **produto** de G_1 por G_2 e denota-se por G_1xG_2 o conjunto de pares ordenados $\{(x,y): x\in G_1, y\in G_2\}$ sujeitos à operação de multiplicação $(x_1,y_1)*(x_2,y_2)=(x_1\otimes x_2,y_1\oplus y_2)$.

Diz-se que $H=(Y,\otimes_y)$ é um **subgrupo** de $G=(X,\otimes_x)$ e escreve-se $H\leq G$, se $X\supseteq Y$ e, denotando-se a operação $\otimes_x$ restringida aos elementos de Y por $\otimes_y$, $H=(Y,\otimes_y)$ é um grupo. Como exemplo de um subgrupo pode indicar-se o grupo alterno, A_n, o qual constitui, claramente, um subgrupo do grupo simétrico, S_n, i. e, $A_n\leq S_n$.

Com o teorema a seguir evidencia-se a importância do grupo simétrico no contexto dos grupos finitos.

3.4 Teorema (de Cayley)

Todo o grupo de ordem $n\in\mathbf{N}$ é isomorfo a um subgrupo de S_n.

Prova:

Para cada $x \in G$, defina-se f_x como sendo uma aplicação entre G e G tal que $f_x(y)=yx$. Logo, pode concluir-se que f_x é injectiva, uma vez que $f_x(y)=f_x(z) \Leftrightarrow yx=zx \Leftrightarrow y=z$ (bastando, para o efeito, mutltiplicar ambos os membros à direita por x^{-1}). Dado que f é uma aplicação injectiva de G em sí próprio, podemos concluir que f é uma bijecção e, consequentemente, que f_x é uma permutação dos n elementos de G. O conjunto de todas estas permutações (i. e, o conjunto $F=\{f_x: x \in G\}$) munido da operação de composição de aplicações, $\otimes$, é um grupo isomorfo a G. Para se obter uma tal conclusão, basta considerar o isomorfismo $\psi: G \rightarrow F$ tal que $\psi(x)=f_x$, para o qual se verifica que $\psi(xy)=f_{xy}$, com $f_{xy}(z)=(xy)z=x(yz)=f_x(yz)=f_x(f_y(z))$, pelo que $f_{xy}=f_x \otimes f_y$, i. e, $\psi(xy)=\psi(x) \otimes \psi(y)$. Por outro lado, $\psi(x)=\psi(y) \Leftrightarrow f_x=f_y \Leftrightarrow xz=yz \ \forall z \in G \Rightarrow x=y$ (tendo em conta que $xz=yz \Leftrightarrow (xz)z^{-1}=(yz)z^{-1} \Leftrightarrow x(zz^{-1})=y(zz^{-1}) \Leftrightarrow xe=ye \Leftrightarrow x=y$), pelo que ψ é injectiva e como é sobrejectiva (por construção), conclui-se que, efectivamente, se trata de um isomorfismo entre G e F. Uma vez que F munido da operação $\otimes$ é um grupo e existe um isomorfismo entre $(F,\otimes)$ e um subgrupo de S_n pela respectiva composição com ψ conclui-se o pretendido.

♦

De acordo com a demonstração do teorema 3.4, por exemplo, para o grupo $(\{0,1,2,3,4\},+\text{mod}.5)$ obtém-se o conjunto de bijecções $F=\{f_0,f_1,f_2,f_3,f_4\}$ onde $f_0=(0)(1)(2)(3)(4)$, $f_1=(0\ 1\ 2\ 3\ 4)$, $f_2=(0\ 2\ 4\ 1\ 3)$, $f_3=(0\ 3\ 1\ 4\ 2)$ e $f_4=(0\ 4\ 3\ 2\ 1)$, o qual (substituindo 0 por 5) constitui um subgrupo de S_5 (note-se que f_0 constitui o elemento neutro, f_4 o inverso de f_1, f_2 o inverso de f_3 e reciprocamente).

Dado um grupo finito G, $\forall x \in G$, verifica-se que o conjunto $\langle x \rangle = \{x^k: k \in \mathbf{N}\}$ é um subgrupo de G (o qual, habitualmente, se designa por subgrupo de G gerado por x). Os grupos cujos elementos são as potências inteiras positivas de um dado elemento designam-se, habitualmente, por **grupos cíclicos**.

Supondo que H é um subgrupo de G, i. e, $H \leq G$, diz-se que x é congruente com y módulo H, e escreve-se $x \equiv y \pmod{H}$, se $x,y \in G$ e $xy^{-1} \in H$. Prova-se que esta relação de **congruência módulo um subgrupo** ($\equiv \pmod{H}$) é uma relação de equivalência em G.

Com efeito (i) $x \equiv x \pmod{H}$ dado que $\forall x \in G \; e = xx^{-1} \in H$; (ii) se $x \equiv y \pmod{H}$, então $xy^{-1} \in H$, donde $yx^{-1} = (xy^{-1})^{-1} \in H$, pelo que $y \equiv x \pmod{H}$; (iii) se $x \equiv y \pmod{H}$ e $y \equiv z \pmod{H}$, então $xy^{-1} \in H$ e $yz^{-1} \in H$, logo $(xy^{-1})(yz^{-1}) = xz^{-1} \in H$, pelo que $x \equiv z \pmod{H}$.

Sendo H um subgrupo de G designa-se por **classe lateral** (à direita) de H em G e denota-se por Hx, o conjunto $\{hx: h \in H\}$. Por sua vez, designa-se por classe lateral (à esquerda) de H em G o conjunto $xH = \{xh: h \in H\}$.

Quando, $\forall x \in G$, $Hx = xH$, diz-se que H é um **subgrupo normal** de G.

Note-se, porém que, sendo H um subgrupo de um grupo arbitrário G, apesar de nem sempre se verificar a igualdade $Hx = xH$, no que diz respeito à sua cardinalidade (conforme mais adiante se concluirá) $\forall x \in G$, $|Hx| = |xH| = |H|$.

Pode provar-se ainda que a classe lateral (à direita) H em G coincide com o subconjunto de G $\{y \in G: y \equiv x \pmod{H}\}$ (i. e, $Hx = \{y \in G: y \equiv x \pmod{H}\}$), pelo que Hx constitui, também, uma classe de equivalência em G. Com efeito, se $y \in Hx$, então $y = hx$ para algum $h \in H$, pelo que $y \equiv x \pmod{H}$ (uma vez que $yx^{-1} = (hx)x^{-1} = h \in H$), consequentemente $\{y \in G: y \equiv x \pmod{H}\} \supseteq Hx$ (*). Por outro lado, se $z \in \{y \in G: y \equiv x \pmod{H}\}$ vem que $h = zx^{-1} \in H$, logo $z = hx \in Hx$, donde se conclui que $Hx \supseteq \{y \in G: y \equiv x \pmod{H}\}$ (**). Finalmente, de (*) e (**) decorre, imediatamente, que $Hx = \{y \in G: y \equiv x \pmod{H}\}$.

Assim, sendo k o número de classes laterais (à direita) de H em G distintas, as quais, sem perda de generalidade, vamos identificar por $Hx_1, \ldots, Hx_k$, com $x_1, \ldots, x_k \in G$, podemos concluir que $Hx_i \cap Hx_j = \emptyset \; \forall i \neq j$ e $G = Hx_1 \cup \ldots \cup Hx_k$ (ou seja, G é a união disjunta das classes laterais $Hx_1, \ldots, Hx_k$). Adicionalmente, verifica-se que $|Hx_i| = |H| \; \forall i \in \{1, \ldots, k\}$. Com efeito, considerando a aplicação $\psi_i: H \rightarrow Hx_i$ tal que $\psi_i(h) = hx_i$, vem que ψ_i é sobrejectiva (por construção) e, uma vez que $\psi_i(h) = \psi_i(h') \Leftrightarrow hx_i = h'x_i \Leftrightarrow h = h'$,

conclui-se que também é injectiva. Consequentemente, da bijectividade de ψ_i entre H e Hx_i, vem que $|H|=|Hx_i|$. Idêntica conclusão se obtém para qualquer das classes laterais (à esquerda) de H em G, pelo que, agora, se torna óbvio, que $\forall x\in G$, $|Hx|=|H|=|xH|$.

Se denotarmos por $H_{(.)}$ a classe lateral (à direita) de H em G, genérica, o conjunto quociente $G/H_{(.)}=\{Hx: x\in G\}$ é o conjunto de todas as classes laterais (à direita) de H em G (por sua vez, o conjunto quociente $G/_{(.)}H=\{xH: x\in G\}$ será o conjunto de todas as classes laterais (à esquerda) de H em G). Recorrendo a estes conceitos torna-se, agora, fácil provar o teorema a seguir.

3.5 Teorema (de Lagrange)

Se G é um grupo finito e H um seu subgrupo, então |H| é um divisor de |G|

(i. e, a ordem de H divide a ordem de G).

Prova:

Uma vez que H é um subgrupo de um grupo finito G, conclui-se que o conjunto $G/H_{(.)}$ das classes laterais (à direita) de H em G é finito. Se $|G/H_{(.)}|=k$ e $G/H_{(.)}=\{Hx_1,\ldots,Hx_k\}$, então G é a união disjunta de Hx_1, … , Hx_k, pelo que $|G|=|Hx_1|+\ldots+|Hx_k|=k|H|$ (uma vez que $|Hx_i|=|H|$ $\forall i\in\{1,\ldots,k\}$).

♦

Da prova deste teorema decorre, também, que o número de classes laterais à esquerda de H em G é igual ao número de classes laterais à direita (uma vez que, sendo n_e e n_d o número de classes laterais, respectivamente, à esquerda e à direita de H em G, vem que $n_e|H|=|G|=n_d|H| \Rightarrow n_e=n_d$) e este facto proporciona a introdução do conceito de índice de um subgrupo.

Dado um grupo finito G, designa-se por **índice do subgrupo** H, em G, e denota-se por [G:H], o número de classes (à esquerda ou à direita) que ele determina. Desta definição, e da análise anterior, decorre que $[G:H]=\frac{|G|}{|H|}$.

Relativamente ao subgrupo de S_n, A_n, verifica-se que $[S_n:A_n]=2$ (i. e, que A_n é um subgrupo de S_n de índice 2) e, consequentemente, que A_n é um subgrupo normal de S_n (veja-se o exercício 3.2).

Deve observar-se que, embora o teorema de Lagrange nos permita concluir que se G é um grupo finito, então a ordem de qualquer dos seus subgrupos divide a ordem de G, não existe qualquer garantia de que, para cada divisor da ordem de G, haja um subgrupo com tal ordem.

Como consequência imediata do teorema de Lagrange conclui-se que, dado um grupo G de ordem n, $\forall x \in G$, $x^n=e$ (a prova desta afirmação é proposta no exercício 3.3).

Do teorema de Lagrange decorrem, ainda, os seguintes corolários.

3.6 Corolário (do teorema de Lagrange)

Todo o grupo finito de ordem prima é cíclico e (em particular) abeliano.

Prova:

Seja G um grupo de ordem p (i. e, $|G|=p$) com p primo. Se $x \in G$ e $x \neq e$, então $\langle x \rangle$ é um subgrupo de G que contém o subconjunto $\{e,x\}$. Logo, pelo teorema de Lagrange, $|\langle x \rangle|$ é um divisor de $|G|=p$. Consequentemente, uma vez que $|\langle x \rangle|>1$, conclui-se que $|\langle x \rangle|=p$, pelo que $G=\langle x \rangle$.

♦

3.7 Corolário (do teorema de Lagrange)

Se G é um grupo tal que $|G| \leq 5$, então G é abeliano.

Prova:

Para $|G|=1$, vem que $G=\{e\}$.

Para $|G|=2$, 3 ou 5, vem que $|G|$ é primo e, pelo corolário 3.3, G é cíclico, logo abeliano.

Suponha-se que $|G|=4$. Se $\exists x\in G\setminus\{e\}$ tal que $\langle x\rangle=G$, então G é cíclico, logo abeliano. Se $\forall x\in G\setminus\{e\}$, $\langle x\rangle\neq G$, então, pelo teorema de Lagrange, $|\langle x\rangle|=2$ e $x^2=e$ $\forall x\in G$. Consequentemente, todos os elementos de G coincidem com o seu inverso, logo se $x,y\in G$, $xy=(xy)^{-1}=y^{-1}x^{-1}=yx$.

♦

Se G é um grupo finito e H é um seu subgrupo normal, i. e, tal que $G/H_{(.)}=G/_{(.)}H$ (as classes laterais à direita são iguais às classes laterais à esquerda de H em G), então $(G/H,\otimes)$ tal que $\forall Hx,Hy\in G/H_{(.)}$, $Hx\otimes Hy=H(xy)$, é um grupo que se designa por **grupo quociente** de G por H. Com efeito, deve observar-se, primeiramente, que não existe qualquer ambiguidade na operação definida em G/H, uma vez que se Hx=Hx' e Hy=Hy', então $H_{xy}=H_{x'y'}$. Com efeito, se $h(xy)\in H_{xy}$, então h(xy)=(hx)y e dado que $hx\in Hx=Hx'$, $\exists h'\in H$ tal que h(xy)=(h'x')y. Por outro lado, uma vez que Hx'=x'H, $\exists h''\in H$ tal que h'x'=x'h'', logo h(xy)=(x'h'')y=x'(h''y)=x'(h'''y') para algum $h'''\in H$, uma vez que Hy=Hy', adicionalmente, tendo em conta que Hy'=y'H, vem que h(xy)=x'(y'h'''')=(x'y')h'''', para algum $h''''\in H$. Deste modo concluiu-se que $H_{x'y'}\supseteq H_{xy}$ e como de um modo idêntico se conclui que $H_{xy}\supseteq H_{x'y'}$, vem que $H_{xy}=H_{x'y'}$.

No que diz respeito à verificação das propriedades que caracterizam os grupos vem que:

1. ((Hx)(Hy))Hz=(H(xy))Hz=H((xy)z)=H(x(yz))=Hx(H(yz))=Hx((Hy)(Hz)).
2. H(Hx)=(H*e*)(Hx)=H(*e*x)=Hx e (Hx)H=(Hx)(H*e*)=H(x*e*)=Hx.
3. $(Hx)(Hx^{-1})=H(xx^{-1})=H*e*=H=H*e*=H(x^{-1}x)=(Hx^{-1})(Hx)$.

Deste modo (uma vez que a prova de que a operação definida no conjunto das classe laterais é fechada nesse conjunto é imediata), a demonstração de que G/H é um grupo fica completa.

Dado um grupo, G, e um conjunto, X, arbitrários, diz-se que G **opera** sobre X (ou que X é um **conjunto-G**) quando se define uma aplicação $\theta:GxX\rightarrow X$ que satisfaz as seguintes propriedades:

a) $\forall x\in X,\ \theta(e,x)=x$ (onde e é o elemento neutro de G).

b) $\forall g,h\in G$ e $\forall x\in X,\ \theta(g,\theta(h,x))=\theta(gh,x)$.

Por economia, em geral, escreve-se gx em vez de θ(g,x), pelo que em a) ter-se-ia $ex=x$ e am b) $g(hx)=(gh)x$. Convém no entanto reter que, enquanto g e h são elementos do grupo G, x é um elemento de X.

Sendo X um conjunto-G (pelo que G opera sobre X por intermédio de uma certa aplicação $\theta:GxX\rightarrow X$) e $x\in X$, designa-se por **órbita** (ou trajectória) de x e denota-se por Orb(x), o conjunto $\{\theta(g,x): g\in G\}$ (em notação mais aligeirada pode escrever-se, simplesmente, $Orb(x)=\{gx: g\in G\}$). Habitualmente, se $y\in Orb(x)$, pelo que $y=gx$ para algum $g\in G$, diz-se que g desloca x para y. Por sua vez, define-se **grupo de isotropia** de $y\in X$ e denota-se por G_y, o conjunto $\{g\in G: \theta(g,y)=y\}$ (i. e, $G_y=\{g\in G: gy=y\}$).

Como exemplo de um conjunto-G, onde G é um grupo finito, podemos considerar que G opera sobre ele próprio por intermédio da aplicação $\theta: G\,x\,G\rightarrow G$, tal que $\theta(g,h)=ghg^{-1}$. Esta operação designa-se por **operação de conjugação** e, neste caso, o grupo de isotropia de $h\in G$ é $G_h=\{g\in G: \theta(g,h)=h\}=\{g\in G: ghg^{-1}=h\}=\{g\in G: gh=hg\}$, e designa-se, usualmente, por conjunto centralizador de G em relação a h.

Com facilidade se verifica, ainda, que a operação de conjugação introduzida define uma relação de equivalência em G (a prova destas afirmação é proposta no exercício 3.4).

3.8 Teorema

Sendo G um grupo finito e X um conjunto-G, são verdadeiras as seguintes afirmações:

(i) $\bigcup_{x\in X} Orb(x)=X$.

(ii) $\forall x,y\in X$ se $Orb(x)\cap Orb(y)\neq\emptyset$, então $Orb(x)=Orb(y)$.

(iii) $\forall x\in X,\ G_x\leq G$.

(iv) $\forall x\in X,\ [G:G_x]=|Orb(x)|$.

Prova:

(i) Pela propriedade a) da operação sobre sobre X, $\forall x\in X$, $x=ex\in Orb(x)$, donde vem que $X=\bigcup_{x\in X} Orb(x)$.

(ii) Suponhamos que $Orb(x)\cap Orb(y)\neq\emptyset$, então $\exists g,h\in G$ tais que $gx=hy$. Seja $z'\in Orb(x)$, então $\exists f'\in G$ tal que $f'x=z'$ e, uma vez que $x=(g^{-1}h)y$, $z'=f'x=(f'(g^{-1}h))y \Rightarrow z'\in Orb(y)$, logo $Orb(y)\supseteq Orb(x)$ (*). Seja $z''\in Orb(y)$, então $\exists f''\in G$ tal que $z''=f''y$ e, uma vez que $y=h^{-1}gx$, $z''=f''y=(f''(h^{-1}g))x \Rightarrow z''\in Orb(x)$, donde $Orb(x)\supseteq Orb(y)$ (**). De (*) e (**) vem, finalmente, que $Orb(x)=Orb(y)$.

(iii) Seja x um ponto arbitrário de X. É claro que $e\in G_x$ (uma vez que, por a) $ex=x$) e, consequentemente, não só $G_x\neq\emptyset$ como tem elemento neutro. $\forall g\in G_x$ de $gx=x$ decorre que $g^{-1}x=x$, pelo que $g^{-1}\in G_x$ (ou seja, todos os elementos de G_x tem inverso em G_x). Finalmente, dados dois elementos arbitrários de G_x, h e f, vem $(hf)x=h(fx)=hx=x$, pelo que $hf\in G_x$, i. e, a operação definida em G ($G\supseteq G_x$) é fechada em G_x, pelo que se conclui que $G_x \leq G$.

(iv) Considere-se o conjunto das classes laterais (à esquerda) de G_x em G, i. e, $\{gG_x: g\in G\}$, e a aplicação $\eta_x:\{gG_x: g\in G\}\rightarrow Orb(x)$, tal que $\eta_x(gG_x)=gx$. Por construção vem que η_x é uma aplicação sobrejectiva em Orb(x). Vamos provar que também é injectiva. Suponhamos que $\exists hG_x,fG_x$ tais que $\eta_x(hG_x)=\eta_x(fG_x) \Leftrightarrow$ que $hx=fx$. Então, vem que $f^{-1}hx=x$ ($h^{-1}fx=x$), pelo que $f^{-1}h\in G_x$ ($h^{-1}f\in G_x$), consequentemente vem que $h=f(f^{-1}h)\in fG_x$ ($f=h(h^{-1}f)\in hG_x$). Uma vez que $h\in hG_x$ ($f\in fG_x$), dado que $e\in G_x$ e $h=he$ ($f=fe$), conclui-se que $h\in hG_x\cap fG_x$ ($f\in hG_x\cap hG_x$), logo, tendo em conta que as classe laterais constituem uma partição de G em subconjuntos disjuntos, vem que $hG_x=fG_x$, o que completa a prova da injectividade de η_x.

Da bijectidade de η_x decorre que $|\{gG_x: g\in G\}|=|Orb(x)| \Leftrightarrow [G:G_x]=|Orb(x)|$.

♦

Como corolário imediato do teorema 3.8 (i) e (ii) decorre que o conjunto das órbitas distintas de X constitui uma partição de X. Por outro lado, da equação orbital (iv),

$[G:G_x]=|Orb(x)| \Leftrightarrow \frac{|G|}{|G_x|}=|Orb(x)| \Leftrightarrow |G|=|G_x||Orb(x)|$, conclui-se que grupos isotrópicos de cardinalidade elevada dão origem a órbitas de pequena cardinalidade e reciprocamente. Esta conclusão é coerente com a interpretação de que sendo G_x um grupo isotrópico de cardinalidade elevada, isso significa que existem muitos elementos do grupo G que deixam x fixo, pelo que restarão poucos que, efectivamente, o deslocam. A este propósito diz-se que G é **transitivo** (relativamente à operação sobre X) se admite uma única órbita em X, caso contrário diz-se **não transitivo**. Deve observar-se que um grupo é sempre transitivo relativamente a cada subconjunto de X que coincide com uma das suas órbitas.

Introduzidos os intrumentos e resultados (da Teoria dos Grupos Finitos) necessários, estamos, agora, em condições de abordar um tema, tipicamente combinatório, relacionado com a enumeração (ou contagem) de diferentes (ou não equivalente) configurações de objectos, para o que se torna imprescindível o desenvolvimento de técnicas adequadas para a respectiva destinção. Uma destas técnicas consiste em interpretar as classes de configurações equivalentes como órbitas de uma certa operação de um grupo sobre o conjunto das diferentes configurações a analisar. Assim, depois de se definirem os critérios segundo os quais duas configurações se distinguem, escolhendo (de um modo conveniente) um grupo que opere adequadamente sobre o conjunto de todas as configurações, o número de configurações não equivalentes corresponderá ao número de órbitas distintas. O teorema a seguir, conhecido por lema de Burnside [18] (mas que, de acordo com (Neumann, 1979), é da autoria de Cauchy e Frobenius) fornece um método para a contagem destas órbitas.

---

[18]Embora este resultado venha referido (sem qualquer atribuição) no livro, publicado por Burnside em 1897, com o título "*The Theory of groups of finite order*", de acordo com (Neumann, 1979), ele é devido a Cauchy e Frobenius.

3.9 Teorema (lema de Burnside)

Seja G um grupo finito que opera sobre um conjunto finito X e, para cada $g\in G$, seja $\chi(g)=|X_g|$ tal que $X_g=\{x\in X: gx=x\}$. Então, sendo k o número de órbitas distintas que G determina em X, $k=\frac{1}{|G|}\sum_{g\in G}\chi(g)$.

Prova:

Sendo $S=\{(g,x)\in GxX: gx=x\}$, a determinação da sua cardinalidade pode ser feita de dois modos distintos. Um deles consiste em contar o número de pares $(g,x)\in S$ para cada $g\in G$ e adicionar os resultados obtidos e o outro consiste em determinar para cada $x\in X$ o número de pares $(g,x)\in S$ e somar, novamente, os resultados obtidos. Assim, vem que

$$|S| = \sum_{x\in X}|\{g\in G: gx=x\}| = \sum_{g\in G}|\{x\in X: gx=x\}|,$$

ou seja,

$$|S| = \sum_{x\in X}|G_x| = \sum_{g\in G}\chi(g)$$

Supondo que $Orb(x_1), \dots , Orb(x_k)$ são as órbitas distintas em X, uma vez que X é a união disjunta destas órbitas, vem que $\sum_{j=1}^{k}\sum_{x\in Orb(x_j)}|G_x| = \sum_{x\in X}|G_x| = \sum_{g\in G}\chi(g)$.

No pressuposto que $\forall x\in Orb(x_j)$, $|G_x|=|G_{x_j}|$ (cuja prova será feita mais adiante) vem que $\sum_{j=1}^{k}\sum_{x\in Orb(x_j)}|G_x| = \sum_{j=1}^{k}|Orb(x_j)||G_{x_j}| = \sum_{j=1}^{k}[G:G_{x_j}]|G_{x_j}| = \sum_{j=1}^{k}\frac{|G|}{|G_{x_j}|}|G_{x_j}| = k|G|$.

Logo, $k|G| = \sum_{g\in G}\chi(g)$, pelo que $k=\frac{1}{|G|}\sum_{g\in G}\chi(g)$.

Resta pois provar que $\forall x\in Orb(x_j)$, $|G_x|=|G_{x_j}|$, para o que basta encontrar uma bijecção entre $G_x=\{f\in G: fx=x\}$ e $G_{x_j}=\{f\in G: fx_j=x_j\}$.

$\forall x\in Orb(x_j)$, defina-se a aplicação $\psi_x:G_x\rightarrow G_{x_j}$, tal que $\psi_x(f)=g^{-1}fg$, onde $g\in G$ e é tal que $gx_j=x$ (note-se que um tal g existe uma vez que $x\in Orb(x_j)$). Nestas condições prova-se que ψ_x é uma bijecção.

1. Para provar a sobrejectividade de ψ_x em G_{x_j}, considere-se $h \in G_{x_j}$. Logo, $hx_j=x_j$ e $gx_j=x \Leftrightarrow x_j=g^{-1}x$. Consequentemente, $hx_j=hg^{-1}x=x_j=g^{-1}x \Rightarrow ghg^{-1}x=x$, donde vem que. $f=ghg^{-1} \in G_x$ é tal que $\psi_x(f)=g^{-1}fg=h$.

2. Por sua vez, a prova da injectividade faz-se supondo que existem $f',f'' \in G_x$ tais que $\psi_x(f')=\psi_x(f'') \Leftrightarrow g^{-1}f'g=g^{-1}f''g \Leftrightarrow f'=f''$.

♦

Este teorema (lema de Burnside) estabelece que o número de órbitas é igual ao número médio de pontos fixos determinados pelos conjuntos $X_g=\{x \in X: gx=x\}$ cuja união $\cup_{g \in G} X_g$ se designa, habitualmente, por conjunto de **pontos fixos da operação de G sobre X** (ou conjunto de **pontos fixos do conjunto-G**).

Como exemplo de aplicação, vamos utilizar o lema de Burnside na resolução do problema a seguir.

3.10 Problema

Em quantas factorizações distintas como produtos de três números naturais se consegue decompôr o número 1000 (considerando que duas factorizações são distintas se não se podem obter uma da outra por permutação dos respectivo factores).

Resolução:

Dado que $1000=2^3 5^3$, qualquer factorização de 1000 no produto de três números naturais é da forma $(2^{\alpha_1}5^{\beta_1})(2^{\alpha_2}5^{\beta_2})(2^{\alpha_3}5^{\beta_3})$, onde o 6-uplo $(\alpha_1,\alpha_2,\alpha_3,\beta_1,\beta_2,\beta_3)$ é tal que $\alpha_i,\beta_i \in \mathbf{N} \cup \{0\}$ $\forall i \in \{1,2,3\}$ e $\alpha_1+\alpha_2+\alpha_3=\beta_1+\beta_2+\beta=3$. Se M é o conjunto de tais 6-uplos, então $M=M_\alpha \times M_\beta$ onde $M_\alpha=\{(\alpha_1,\alpha_2,\alpha_3)$: $\alpha_1,\alpha_2,\alpha_3 \in \mathbf{N} \cup \{0\}$ e $\alpha_1+\alpha_2+\alpha_3=3\}$ e $M_\beta=\{(\beta_1,\beta_2,\beta_3)$: $\beta_1,\beta_2,\beta_3 \in \mathbf{N} \cup \{0\}$ e $\beta_1+\beta_2+\beta_3=3\}$, logo $|M|=|M_\alpha|.|M_\beta|=|M_\alpha|^2$, uma vez que $|M_\alpha|=|M_\beta|$. Consequentemente, dado que $M_\alpha=\{(1,1,1), (2,1,0), (2,0,1), (1,2,0), (0,2,1), (1,0,2), (0,1,2), (3,0,0), (0,3,0), (0,0,3)\}$, conclui-se que $|M|=10^2$.

Tendo em conta que as diferentes factorizações são invariantes relativamente à ordem dos factores ($2^{\alpha_i}5^{\beta_i}$), vamos considerar a operação do grupo gerado pelos ciclos relativos às permutações do conjunto {1,2,3}, G={(i_1 i_2 i_3): i_1,i_2,i_3∈{1,2,3}} (ou seja, S_3) sobre M, definida do seguinte modo:

$$\forall\pi\in G,\ \pi\otimes(\alpha_1,\alpha_2,\alpha_3,\beta_1,\beta_2,\beta_3)=(\alpha_{\pi(1)},\alpha_{\pi(2)},\alpha_{\pi(3)},\beta_{\pi(1)},\beta_{\pi(2)},\beta_{\pi(3)})$$

Nestas condições, duas factorizações são consideradas equivalentes se podem ser obtidas, uma da outra, por permuatações dos ternos de pares (α_1,β_1), (α_2,β_2) e (α_2,β_3). Consequentemente, esta equivalência verifica-se sse os 6-uplos definidos pelas factorizações petencem à mesma órbita, pelo que o resultado pretendido é, precisamente, o número de órbitas de M.

Para se aplicar o lema de Burnside temos de calcular o número de pontos fixos, $\chi(g)$ para cada elemento g∈G. Assim, (1) sendo σ_1=id, o elemento identidade de G, $\chi(\sigma_1)$=100; (2) sendo σ_2∈G uma transposição, vem que $\chi(\sigma_2)$=4 (por exemplo σ_2=(1 2) mantém fixos (1,1,1,1,1,1), (0,0,3,1,1,1), (1,1,1,0,03) e (0,0,3,0,0,3)); finalmente, (3) sendo σ_3 um ciclo de comprimento 3, vem que $\chi(\sigma_3)$=1 (uma vez que, neste caso, apenas o ponto (1,1,1,1,1,1) fica fixo). Consequentemente, denotando por $|\sigma_i|$ o número de elementos de G do tipo σ_i para i=1, 2 e 3, de acordo com o lema de Burnside, o número de órbitas vem dado por

$$\frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{3!}(100|\sigma_1|+4|\sigma_2|+2|\sigma_3|).$$

Tendo em conta que $|\sigma_1|$=1, $|\sigma_2|$=3 ((1 2), (2 3), (1 3)) e $|\sigma_3|$=2 ((1 2 3) e (1 3 2)) [19], o número de órbitas fica $\frac{1}{|G|}\sum_{g\in G}\chi(g) = \frac{1}{6}(100+12+2) = \frac{114}{6} = 19$.

♦

Embora a aplicação do lema de Burnside se torne suficiente na resolução de vários problemas relacionados com contagens de configurações não equivalentes, o facto

[19]Observe-se que, por exemplo, (1 2 3), (2 3 1) e (3 1 2) representam o mesmo ciclo.

de obrigar à determinação do número de pontos fixos do conjunto-G, torna-o, no entanto, impraticável em muitas situações.

Uma técnica muito usual em contagens (ou enumerações) consiste em identificar os objectos a enumerar como funções entre conjuntos apropriadamente escolhidos. Assim, sendo X e Y os conjuntos considerados, os quais vamos supôr finitos e não vazios, o conjunto das funções entre X e Y, Y^X, como é sabido, tem cardinalidade $|Y|^{|X|}$. Algumas destas funções, porém, embora correspondam a diferentes elementos do conjunto Y^X, são consideradas equivalentes no sentido em que, sendo g e h duas funções entre X e Y ($g:X\rightarrow Y$ e $h:X\rightarrow Y$) se verifica uma das seguintes condições:

(i) $g=h$;

(ii) $g=hf_X$, para alguma bijecção $f_X:X\rightarrow X$;

(iii) $g=f_Yh$, para alguma bijecção $f_Y:Y\rightarrow Y$;

(iv) $g=f_Yhf_X$ para um par de bijecções $f_X:X\rightarrow X$ e $f_Y:Y\rightarrow Y$.

Considerando que os elementos de X e de Y não estão devidamente etiquetados no sentido de se poderem distinguir uns dos outros de acordo com determinado ponto de vista [20], em (ii) e (iv) a bijecção f_X tem um papel de etiquetação dos elementos de X (podendo, neste caso, passar a considerar-se X como um conjunto de elementos etiquetados) e em (iii) e (iv) a bijecção f_Y tem um papel idêntico relativamente a Y.

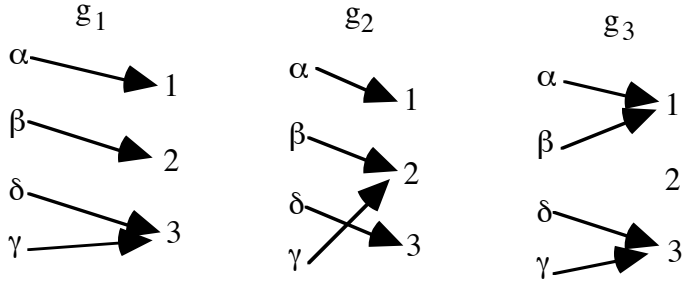


Fig. 3.1

[20]Por exemplo, para um daltónico que observe um conjunto de objectos, iguais na forma mas diferentes nas cores, será difícil distingui-los adequadamente. Porém, se a cada um destes objectos fôr atribuido um número (diferente para cada côr) a distinção passa a ser possível.

Por exemplo, seja $X=\{\alpha,\beta,\delta,\gamma\}$ e $Y=\{1,2,3\}$ e considerem-se as funções de Y^X, $g_1=\{(\alpha,1),(\beta,2),(\delta,3),(\gamma,3)\}$, $g_2=\{(\alpha,1),(\beta,2),(\delta,3),(\gamma,2)\}$ e $g_3=\{(\alpha,1),(\beta,1),(\delta,3),(\gamma,3)\}$ representadas na figura anterior. A partir das bijecções $f_X=\{(\alpha,\alpha),(\beta,\delta),(\delta,\beta),(\gamma,\gamma)\}$ e $f_Y=\{(1,1),(2,3),(3,2)\}$, conclui-se que $f_Y g_1 f_X=\{(\alpha,1),(\beta,2),(\delta,3),(\gamma,2)\}=g_2$, pelo que g_1 é equivalente a g_2 no sentido de (iv). Porém, não existe qualquer bijecção em X nem qualquer bijecção em Y relativamente às quais se obtenha a equivalência entre g_1 e g_3 ou a equivalência entre g_2 e g_3 quer no sentido de (ii), quer no de (iii), quer no de (iv), uma vez que g_1 e g_2 são sobrejectivas e g_3 é não sobrejectiva.

Como consequência da análise feita anteriormente, podemos concluir que, relativamente a um conjunto de funções com o mesmo domínimo e o mesmo contradomínio, quer o domínimo, quer o contradomínio, quer ambos poderão ter os seus elementos etiquetados ou não e, esse facto, dá origem a quatro maneiras distintas de contar as funções em causa. Por outro lado, as diferentes funções ainda se podem classificar em injectivas, sobrejectivas, bijectivas ou não necessariamente injectivas nem sobrejectivas. O objectivo da Teoria da Enumeração de Pólya [21] é obter uma técnica eficiente para este tipo de contagens.

Tendo em vista a utilização de uma terminologia mais apelativa, vamos interpretar uma função $f:X\rightarrow Y$ como uma atribuição aos elementos de X de cores existentes em Y, i. e, consideramos $X=\{x_1, x_2, \ldots, x_m\}$ como sendo o conjunto dos objectos a colorir, $Y=\{y_1, y_2, \ldots, y_n\}$ como sendo o conjunto das cores, e a função f como sendo uma correspondência entre os elementos de X e as cores de Y. Com esta interpretação podemos introduzir o conceito de **tipo de coloração** como sendo o n-uplo

---

[21] George Pólya (1887-1985) foi um matemático Húngaro com trabalhos em Teoria dos Números, Análise Complexa, Combinatória, Teoria das Probabilidades, Geometria e Física Matemática. O seu trabalho mais conhecido é, porém, o livro publicado em co-autoria com G. Szego, em 1924, com o título: "*Problems and Theorems in Analysis*".

$(|f^{-1}(y_1)|, |f^{-1}(y_2)|,\ldots,|f^{-1}(y_n)|)=(k_1, k_2,\ldots, k_n)$ onde, uma vez que $f^{-1}(y_j)=\{x\in X: f(x)=y_j\}$ (i. e, $f^{-1}(y_j)$ é o conjunto dos elementos de X aos quais é atribuida, por f, a côr y_j), vem que $k_j=|f^{-1}(y_j)|$ correponde ao número de elementos de X com a côr y_j.

Supondo que um dado grupo finito G opera sobre X ($\theta:GxX\rightarrow X$), esta operação induz uma outra operação sobre o conjunto de colorações Y^X ($\otimes:GxY^X\rightarrow Y^X$) definida por $(g\otimes f)(x)=f(g^{-1}x)$, com as seguintes propriedades:

1. $\forall f\in Y^X$, $e\otimes f:X\rightarrow Y$ é tal que $\forall x\in X$, $(e\otimes f)(x)=f(e^{-1}x)=f(x)$.

2. $\forall g_1,g_2\in G \ \ \forall f\in Y^X$, $g_1\otimes(g_2\otimes f):X\rightarrow Y$ é tal que $\forall x\in X$,

$$(g_1\otimes(g_2\otimes f))(x)=(g_2\otimes f)(g_1^{-1}x)=f(g_2^{-1}g_1^{-1}x)=f((g_1g_2)^{-1}x)=((g_1g_2)\otimes f)(x).$$

Com esta operação o conjunto Y^X é particionado em classes de equivalência e as funções que pertencem a diferentes classes designam-se por funções ou colorações G-(não equivalentes). Ainda de acordo com esta operação, com facilidade se verifica que o número de funções G-(não equivalentes) é igual ao número de órbitas determinadas em Y^X.

Antes de prosseguirmos com alguns resultados da Teoria da Enumeração de Pólya, convém introduzir o conceito de **estrutura cíclica** de uma permutação. Assim, dada uma permutação $\pi\in S_n$, representada por um produto de ciclos disjuntos (que, pelo teorema 3.1, é único), designa-se por estrutura cíclica de π o n-uplo $c(\pi)=(c_1(\pi),c_2(\pi),\ldots,c_n(\pi))$, onde $c_i(\pi)$ é igual ao número de ciclos de comprimento i na factorização, única, de π (note-se que $1c_1(\pi)+2c_2(\pi)+\ldots+nc_n(\pi)=n$).

Por exemplo a permutação $\pi\in S_8$ determinada pelo produto (1 3 6)(2 5 4 8) tem a estrutura cíclica $c(\pi)=(1,0,1,1,0,0,0,0)$.

Dado um grupo finito, G, identificado como sendo o grupo de permutações sobre o conjunto X (com $|X|=m$), a cada permutação $g\in G$ sobre X, está associada uma estrutura

cíclica (que é única) $c(g)=(c_1(g),\ldots,c_m(g))$ que, por sua vez, dá origem ao que se designa por **índice cíclico** de g, o qual se denota por $z(g,x_1,\ldots,x_m)$ [22] e se define como sendo

$$z(g,x_1,\ldots,x_m)=x_1^{c_1(g)}x_2^{c_2(g)}\ldots x_m^{c_m(g)},$$

onde os x_is são variáveis. Este conceito de índice cíclio é extensível ao grupo G, denotando-se esta extensão por $Z(G,x_1,\ldots,x_m)$ e definindo-se como sendo o posinómio [23]

$$Z(G,x_1,\ldots,x_m)=\frac{1}{|G|}\sum_{g\in G}x_1^{c_1(g)}x_2^{c_2(g)}\ldots x_m^{c_m(g)}=\frac{1}{|G|}\sum_{g\in G}\prod_{i=1}^{m}x_i^{c_i(g)}=\frac{1}{|G|}\sum_{g\in G}z(g,x_1,\ldots,x_m).$$

Deve observar-se, por um lado, que no posinómio $Z(G,x_1,\ldots,x_m)$ fica registada, simbolicamente, toda a informação relativa aos comprimentos dos ciclos disjuntos em que se decompõem as várias permutações de G ($G\leq S_m$) e, por outro, que a sua determinação depende unicamente de G.

Como exemplos de aplicação, vamos determinar os índices cíclicos de alguns subgrupos do grupo simétrico, S_n, como sejam (1) o grupo gerado pelo elemento neutro, $<e>$, (2) o próprio grupo simétrico, S_n, e (3) o grupo alterno, A_n.

(1) Para o grupo identidade, $<e>$, que fixa todos os elementos do conjunto sobre o qual opera, existem apenas n ciclos de comprimento 1, pelo que

$$z(e,x_1,x_2,\ldots,x_n)=x_1^n x_2^0\ldots x_n^0=x_1^n \Rightarrow Z(<e>,x_1,x_2,\ldots,x_n)=\frac{1}{|<e>|}x_1^n=x_1^n.$$

(2) Relativamente ao grupo simétrico, S_n, cada permutação, $g\in S_n$, apresenta uma estrutura cíclica $c(g)=(c_1(g),c_2(g),\ \ldots\ ,c_n(g))$, tal que $1c_1(g)+2c_2(g)+\ldots+nc_n(g)=n$ (*), donde vem que $Z(S_n,x_1,x_2,\ldots,x_n)=\frac{1}{|G|}\sum_{g\in G}x_1^{c_1(g)}x_2^{c_2(g)}\ldots x_n^{c_n(g)}$. Confinando-se este somatório aos n-uplos $(c_1,c_2,\ldots,c_n)$ que satisfazem a equação (*), teremos de calcular o

---

[22] George Pólya escolheu a letra z por ser a inicial da palavra de origem alemã "zyclenzeiger" (que se traduz por indicador de ciclo).

[23] Designa-se por posinómio, toda a função, p(x), definida para os n-uplos $x=(x_1,x_2,\ldots,x_m)\in\mathbf{R}^m$, tais que $x_j>0$ para j=1, …, m e $p(x)=\sum_{i=1}^{n}c_i\prod_{j=1}^{m}(x_j)^{\tau_{ij}}$, onde os c_is são constantes positivas e os τ_{ij}s são numeros reais.

número de permutações associadas a cada um destes n-uplos [24]. Assim, para se determinar o número de permutações distintas associadas à estrutura cíclica $c\in C=\{c: 1c_1+2c_2+\ldots+nc_n=n\}$ devem considerar-se as n! permutações possíveis dos c_js, e ter em conta que que existem $c_k!$ maneiras de ordenar os diferentes ciclos disjuntos de comprimento c_k (relativamente a uma mesma permutação) e, ainda, que cada um deles se pode escrever de k modos distintos. Consequentemente, conclui-se que, para cada estrutura cíclica, c, o número de permutações de S_n é $\eta(c)=\frac{n!}{\prod_{k=1}^{n} k^{c_k} c_k!}$, pelo que, o índice cíclico de S_n, em função das diferentes estruturas cíclicas, vem dado por

$$Z(S_n)=\frac{1}{n!}\sum_{c\in C}\eta(c)x_1^{c_1}x_2^{c_2}\ldots x_n^{c_n}.$$

(3) Por sua vez a determinação do índice cíclico do grupo alterno, A_n, tem por base o facto de um ciclo ser par ou impar, consoante tenha, respectivamente, comprimento impar ou par. Como consequência, na decomposição de uma permutação par em ciclos disjuntos, o número de ciclos de comprimento par (por dar origem a decomposições num número impar de transposições) é, necessariamente, par [25]. No que diz respeito ao número de ciclos de comprimento impar, este pode ser par ou impar, uma vez que se decompõem num número par de transposições.

Logo, dada uma estrutura cíclica arbitrária $c\in C=\{c: 1c_1+2c_2+\ldots+nc_n=n\}$,

$$\frac{1}{2}(1+(-1)^{c_2+c_4+\cdots}),$$

conta 1 para cada permutação par e 0 para cada permutação impar, donde vem que o índice cíclico de A_n corresponde a

$$Z(A_n,x_1,x_2,\ldots,x_n)=\frac{1}{n!}\sum_{c\in C}\eta(c)\frac{1}{2}(1+(-1)^{c_2+c_4+\cdots})x_1^{c_1}x_2^{c_2}\ldots x_n^{c_n}.$$

---

[24]Por exemplo, relativamente a S_3 o terno (1,1,0) satisfaz (*) e corresponde à estrutura cíclica das permutações (1 2)(3), (2 3)(1) e (1 3)(2).

[25]Este tipo de argumentação é conhecido, na terminologia inglesa, por "handshake principle".

Voltando a considerar que o grupo finito G opera sobre o conjunto de colorações dos elementos de X por intermédio das cores de Y (funções de Y^X), para cada $g \in G$, sendo $a_{k_1 \ldots k_n}(g)$ o número de colorações do tipo $(k_1,\ldots,k_n)$ que ficam invariantes em relação a g (i. e, que são g-equivalentes), designa-se por **posinómio padrão de g** e denota-se por $p_g(y_1,\ldots,y_n)$, o posinómio nas variáveis $y_1, \ldots, y_n$:

$$p_g(y_1,\ldots,y_n) = \sum_{k_1+\ldots+k_n=m} a_{k_1 \ldots k_n}(g) y_1^{k_1} \ldots y_n^{k_n}.$$

Da definição de posinómio padrão de g decorre que o número de colorações (i. e, funções entre X e Y) g-invariantes vem dado por $p_g(1,\ldots,1) = \sum_{k_1+\ldots+k_n=m} a_{k_1 \ldots k_n}(g)$.

Uma vez definido o posinómio padrão de um elemento de G, a extensão deste conceito ao próprio G, designa-se por **posinómio padrão de G** [26] e corresponde ao posinómio nas variáveis $y_1, \ldots, y_n$:

$$P_G(y_1,\ldots,y_n) = \frac{1}{|G|} \sum_{g \in G} p_g(y_1,\ldots,y_n).$$

Deve observar-se que o posinómio padrão de $g \in G$, determina, simbolicamente, o número de colorações g-invariantes de cada um dos tipos. Por exemplo, no termo $a_{k_1 \ldots k_n}(g) y_1^{k_1} \ldots y_n^{k_n}$ o coeficiente $a_{k_1 \ldots k_n}(g)$ dá ao número de colorações g-invariantes cujo tipo é definido por $y_1^{k_1} \ldots y_n^{k_n}$ (ou seja, cujo tipo é $(k_1,\ldots,k_n)$). O interesse desta representação simbólica, em detrimento de uma eventual listagem dos diferentes valores obtidos para as diferentes colorações, reside no facto de $p_g(y_1,\ldots,y_n)$ poder ser deduzido directamente a partir da estrutura cíclica de g. Com efeito, conforme o teorema de Pólya (mais adiante) estabelece, o posinómio P_G (que está definido em função da operação de G sobre o conjunto de colorações) pode exprimir-se em função do índice cíclico $Z(G,x_1,\ldots,x_m)$ o qual depende unicamente de G, quando G é considerado como um subgrupo de S_n.

---

[26] Na terminologia utilizada por Pólya, este posinómio é designado por inventário padrão de G.

3.11 Teorema

Dado um grupo finito G que opera sobre o conjunto de funções Y^X (onde $|X|=m$ e $|Y|=n$), para cada $g\in G$, com estrutura cíclica $c(g)=(c_1(g),\ldots,c_m(g))$, verifica-se que

a) $P_g(y_1,\ldots,y_n)=z(g,\sum_{j=1}^{n}y_j,\sum_{j=1}^{n}y_j^2,\ldots,\sum_{j=1}^{n}y_j^m)=\prod_{i=1}^{m}(\sum_{j=1}^{n}y_j^i)^{c_i(g)}$.

b) $z(g,n,\ldots,n)=n^{c_1(g)+c_2(g)+\ldots+c_m(g)}$ corresponde ao número de colorações g-invariantes.

Prova:

a) Seja $g=\sigma_1\sigma_2\ldots\sigma_r$, onde σ_1, σ_2, … σ_r são ciclos disjuntos de comprimento, respectivamente, $|\sigma_1|$, $|\sigma_2|$, … , $|\sigma_r|$. Interpretando as funções de Y^X como colorações dos elementos de X pelas cores de Y, para que os m elementos de X sejam g-invariantes, torna-se necessário que os $|\sigma_1|$ elementos afectados por σ_1 tenham a mesma côr, de entre as n possíveis. Consequentemente, apenas para os $|\sigma_1|$ elementos afectados por σ_1, obtém-se o posinómio padrão (preliminar)

$$a_{|\sigma_1|,0,\ldots,0}y_1^{|\sigma_1|}+a_{0,|\sigma_1|,\ldots,0}y_2^{|\sigma_1|}+\ldots+a_{0,0,\ldots,|\sigma_1|}y_n^{|\sigma_1|}=1y_1^{|\sigma_1|}+1y_2^{|\sigma_1|}+\ldots+1y_n^{|\sigma_1|}.$$

De modo análogo, para os $|\sigma_2|$ elementos afectados por σ_2 obtém-se $1y_1^{|\sigma_2|}+1y_2^{|\sigma_2|}+\ldots+1y_n^{|\sigma_2|}$. Porém, uma vez que cada côr atribuida aos elementos de σ_1 é compatível com qualquer das cores atribuidas aos elementos de σ_2, a totalidade das colorações g-invariantes dos $|\sigma_1|+|\sigma_2|$ elementos de X vem (simbolicamente) determinada pela adição de todos os possíveis produtos de $y_i^{|\sigma_1|}$ por $y_j^{|\sigma_2|}$ com $i,j\in\{1,\ldots,n\}$, a qual corresponde ao produto $(1y_1^{|\sigma_1|}+1y_2^{|\sigma_1|}+\ldots+1y_n^{|\sigma_1|})(1y_1^{|\sigma_2|}+1y_2^{|\sigma_2|}+\ldots+1y_n^{|\sigma_2|})$. Da repetição deste argumento para os restantes ciclos da decomposição $g=\sigma_1\sigma_2\ldots\sigma_r$, decorre o posinómio padrão determinado pelo produtório $\prod_{k=1}^{r}(y_1^{|\sigma_k|}+y_2^{|\sigma_k|}+\ldots y_n^{|\sigma_k|})$.

Tendo em atenção que o número de ciclos de comprimento $|\sigma_k|$ da decomposição de g é $c_{|\sigma_k|}(g)$ com $1\le|\sigma_k|\le m$, para $1\le i\le m$, vem, finalmente, que

$$P_g(y_1,y_2,\ldots,y_n)=\prod_{k=1}^{r}(y_1^{|\sigma_k|}+y_2^{|\sigma_k|}+\ldots y_n^{|\sigma_k|})=\prod_{i=1}^{m}(y_1^i+y_2^i+\ldots+y_n^i)^{c_i(g)}.$$

b) Uma vez que g apresenta a estrutura cíclica $c(g)=(c_1(g),c_2(g), \ldots , c_m(g))$ as funções (colorações) que ficam fixas quando operadas com g, são as funções constantes para todos os elementos de cada ciclo de g. Dado que existem $c_1(g)+\ldots+c_m(g)$ ciclos, a cada um dos quais é associado um dos n elemento de Y, o número de funções invariantes por g é $\chi(g)=n^{c_1(g)+\ldots+c_m(g)}=z(g,n,\ldots,n)$.

♦

Deste teorema, mais precisamente da a), decorre, de modo imediato, o seguinte relacionamento entre o posinómio padrão de G e o seu índice cíclico

$$P_G(y_1,\ldots,y_n)=Z(G,\sum_{j=1}^{n}y_j,\sum_{j=1}^{n}y_j^2,\ldots,\sum_{j=1}^{n}y_j^m).$$

Esta igualdade será utilizada na demonstração do teorema fundamental da enumeração de Pólya, que a seguir se apresenta, e que foi introduzido em 1937 num artigo com o título "Kombinatorish Angahlbestimmungen fur Gruppen und chemisch Verbindungen", Acta Math. 68, 145-254.

3.12 Teorema (de Pólya)

Supondo que m objectos (elementos de um conjunto X) são coloridos com n cores (elementos de um conjunto Y), qualquer que seja o subgrupo G de S_m ($G\leq S_m$), o número de colorações (funções de Y^X) G-(não equivalentes) do tipo $(k_1,k_2,\ldots,k_n)$ (onde $k_j=|f^{-1}(y_j)|$ para $j=1,\ldots,n$) é o coeficiente de $y_1^{k_1}y_2^{k_2}\ldots y_n^{k_n}$ no posinómio

$$P_G(y_1,y_2,\ldots,y_n)=Z(G,\sum_{j=1}^{n}y_j,\sum_{j=1}^{n}y_j^2,\ldots,\sum_{j=1}^{n}y_j^m),$$

e o número total de colorações G-(não equivalentes) vem dado por $P_G(1,1,\ldots,1)=Z(G,n,n,\ldots,n)$.

Prova:

Pelo lema de Burnside, o número de colorações G-(não invariantes) do tipo $(k_1,\ldots,k_n)$ é $\frac{1}{|G|}\sum_{g\in G} a_{k_1\ldots k_n}(g)$. Como consequência, tendo em conta que

$$P_G(y_1,\ldots,y_n) = \frac{1}{|G|}\sum_{g\in G} p_g(y_1,\ldots,y_n) = \frac{1}{|G|}\sum_{g\in G}\Big(\sum_{k_1+\ldots+k_n=m} a_{k_1\ldots k_n}(g) y_1^{k_1}\ldots y_n^{k_n}\Big),$$

vem que $\frac{1}{|G|}\sum_{g\in G} a_{k_1\ldots k_n}(g)$ corresponde ao coeficiente de $y_1^{k_1}y_2^{k_2}\ldots y_n^{k_n}$ em $P_G(y_1,\ldots,y_n)$. Logo, dado que, pelo teorema 3.11, $P_G(y_1,\ldots,y_n)=Z(G,\sum_{j=1}^{n} y_j,\sum_{j=1}^{n} y_j^2,\ldots,\sum_{j=1}^{n} y_j^m)$, obtém-se o pretendido. No que diz respeito à conclusão final, ela decorre do facto do número total de colorações G-(não equivalentes) ser igual à soma dos coeficientes de P_G, a qual vem dada por $P_G(1,1,\ldots,1)=Z(G,n,\ldots,n)$.

♦

Da última conclusão do teorema de Pólya decorre que o número total de colorações G-(não equivalentes) vem dado por $Z(G,n,\ldots,n)=\frac{1}{|G|}\sum_{g\in G} n^{c_1(g)+\ldots+c_m(g)}$.

A resolução do problema a seguir vai ilustrar a aplicação do teorema 3.12 (de Pólya).

3.13 Problema

Considerando que se pretendem colorir os vértices de um quadrado, utilizando apenas duas cores (preto e branco) e supondo que duas colorações são consideradas equivalentes se uma se pode obter da outra por uma rotação rígida arbitrária do quadrado, segundo qualquer dos eixos tridimensionais, quantas colorações não equivalentes são possíveis?

Resolução:

Nestas condições podemos considerar que duas colorações são equivalentes se uma se consegue obter da outra, pela operação de um elemento do subgrupo de S_4,

G={id, (1 2 3 4), (1 3)(2 4), (1 4 3 2), (1 2)(3 4), (1 4)(2 3), (1 3) e (2 4)},

sobre o conjunto dos vértices do quadrado.

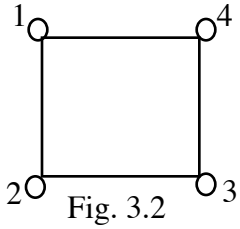


Fig. 3.2

Na figura a seguir listam-se as 16 possíveis colorações dos vértices do quadrado e os respectivos tipos de coloração.

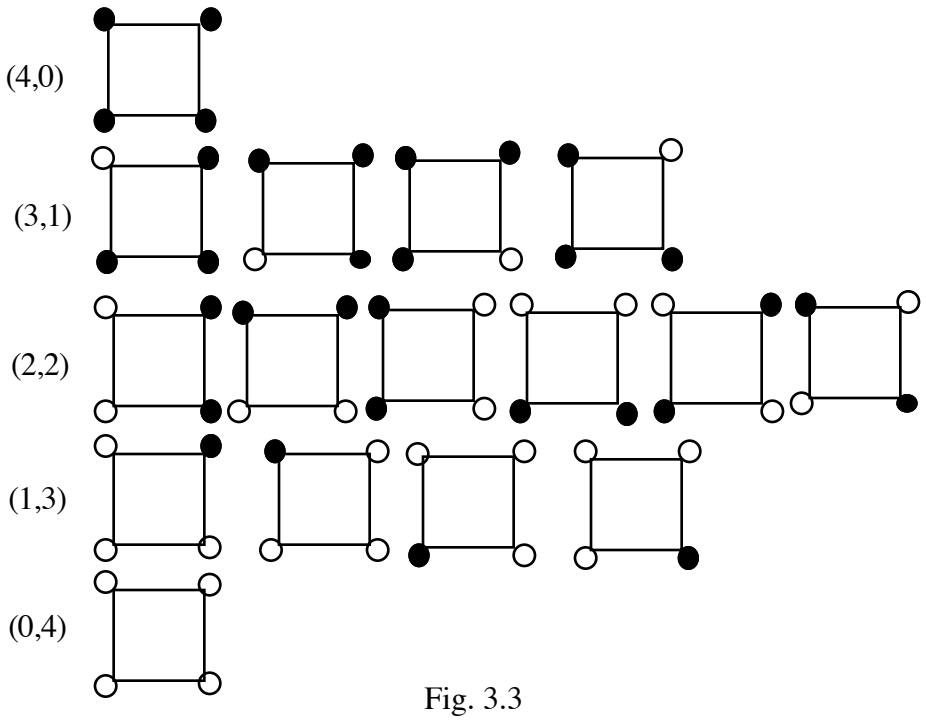


Fig. 3.3

A partir da tabela, a seguir indicada, vamos determinar o posinómio padrão de cada um dos elementos g∈G.

Adicionando os posinómios do quadro a seguir indicado e dividindo a soma obtida por |G|=8, determina-se o posinómio padrão $P_G(y_1,y_2)=y_1^4+y_1^3y_2+2y_1^2y_2^2+y_1y_2^3+y_2^4$, do qual se conclui existirem 6 colorações G-(não equivalentes), uma de cada um dos tipo (4,0), (3,1), (1,3) e (0,4) e duas do tipo (2,2).

$g\in G$	$a_{k_1k_2}(g)$	k_1	k_2	$y_1^{k_1}y_2^{k_2}$	$P_g(y_1,y_2)$
id	1	4	0	$y_1^4y_2^0$	
	4	3	1	$y_1^3y_2^0$	
	6	2	2	$y_1^2y_2^2$	
	4	1	3	$y_1^0y_2^3$	
	1	0	4	$y_1^0y_2^4$	$y_1^4+4y_1^3y_2+6y_1^2y_2^2+4y_1y_2^3+y_2^4$
(1 2 3 4)	1	4	0	$y_1^4y_2^0$	
(1 2 3 4)	1	0	4	$y_1^0y_2^4$	$y_1^4+y_2^4$
(1 3)(2 4)	1	4	0	$y_1^4y_2^0$	
(1 3)(2 4)	2	2	2	$y_1^2y_2^2$	
(1 3)(2 4)	1	0	4	$y_1^0y_2^4$	$y_1^4+2y_1^2y_2^2+y_2^4$
(1 4 3 2)	1	4	0	$y_1^4y_2^0$	
(1 4 3 2)	1	0	4	$y_1^0y_2^4$	$y_1^4+y_2^4$
(1 2)(3 4)	1	4	0	$y_1^4y_2^0$	
(1 2)(3 4)	2	2	2	$y_1^2y_2^2$	
(1 2)(3 4)	1	0	4	$y_1^0y_2^4$	$y_1^4+2y_1^2y_2^2+y_2^4$
(1 4)(2 3)	1	4	0	$y_1^4y_2^0$	
(1 4)(2 3)	2	2	2	$y_1^2y_2^2$	
(1 4)(2 3)	1	0	4	$y_1^0y_2^4$	$y_1^4+2y_1^2y_2^2+y_2^4$
(1 3)	1	4	0	$y_1^4y_2^0$	
(1 3)	2	3	1	$y_1^3y_2^1$	
(1 3)	2	2	2	$y_1^2y_2^2$	
(1 3)	2	1	3	$y_1^1y_2^3$	
(1 3)	1	0	4	$y_1^0y_2^4$	$y_1^4+2y_1^3y_2+2y_1^2y_2^2+2y_1y_2^3+y_2^4$
(2 4)	1	4	0	$y_1^4y_2^0$	
(2 4)	2	3	1	$y_1^3y_2^1$	
(2 4)	2	2	2	$y_1^2y_2^2$	
(2 4)	2	1	3	$y_1^1y_2^3$	
(2 4)	1	0	4	$y_1^0y_2^4$	$y_1^4+2y_1^3y_2+2y_1^2y_2^2+2y_1y_2^3+y_2^4$

Em alternativa, tendo em conta que os elementos de G apresentam as estruturas cíclicas e os consequentes índices cíclicos indicados no quadro a seguir,

$g \in G$	$c(g)$	$z(g,x_1,x_2,x_3,x_4)$
id	(4,0,0,0)	x_1^4
(1 2 3 4)	(0,0,0,1)	x_4^1
(1 3)(2 4)	(0,2,0,0)	x_2^2
(1 4 3 2)	(0,0,0,1)	x_4^1
(1 2)(3 4)	(0,2,0,0)	x_2^2
(1 4)(2 3)	(0,2,0,0)	x_2^2
(1 3)	(2,1,0,0)	$x_1^2x_2^1$
(2 4)	(2,1,0,0)	$x_1^2x_2^1$

vem que

$$Z(G,x_1,x_2,x_3,x_4)=\frac{1}{8}[x_1^4+(x_2^2+x_2^2+x_2^2)+(x_4^1+x_4^1)+(x_1^2x_2^1+x_1^2x_2^1)]=\frac{1}{8}(x_1^4+3x_2^2+2x_4^1+2x_1^2x_2^1).$$

Por aplicação o teorema de Pólya, da equação

$$P_G(y_1,y_2)=Z(G,y_1+y_2,y_1^2+y_2^2,y_1^3+y_2^3,y_1^4+y_2^4),$$

conclui-se que $P_G(y_1,y_2)=\frac{1}{8}[(y_1+y_2)^4+3(y_1^2+y_2^2)^2+2(y_1^4+y_1^4)+2(y_1+y_2)^2(y_1^2+y_2^2)]$, onde o número de colorações do tipo (k_1,k_2) corresponde ao coeficiente de $y_1^{k_1}y_2^{k_2}$.

	y_1^4	$y_1^3y_2^1$	$y_1^2y_2^2$	$y_1^1y_2^3$	y_2^4
$(y_1+y_2)^4$	1	4	6	4	1
$3(y_1^2+y_2^2)^2$	3	0	6	0	3
$2(y_1^4+y_1^4)$	2	0	0	0	2
$2(y_1+y_2)^2(y_1^2+y_2^2)$	2	4	4	4	2
$\sum$	8	8	16	8	8

$$P_G(y_1,y_2)=\frac{1}{8}(8y_1^4+8y_1^3y_2+16y_1^2y_2^2+8y_1y_2^3+8y_2^4)=y_1^4+y_1^3y_2+2y_1^2y_2^2+y_1y_2^3+y_2^4.$$

Vamos finalizar este capítulo com a algumas referências aos conceitos de quasigrupo e de quadrado latino, os quais, como veremos, estão intimamente relacionados.

Um grupoide $(S,\otimes)$ (i. e, um conjunto não vazio S munido de uma lei de composição interna $\otimes$) diz-se um **quasigrupo** de ordem n, se $|S|=n$ e $\forall a,b\in S$, existe um único elemento $x\in S$, tal que $x\otimes a=b$ e existe um único elemento $y\in S$, tal que $a\otimes y=b$. De acordo com esta definição, sendo $S=\mathbf{N}_n$ e definindo-se matricialmente a operação dos diferentes elementos de S, obtém-se uma matriz $A=[\alpha_{ij}]_{\substack{i=1,\ldots,n,\\ j=1,\ldots,n}}$ tal que $\forall i,j\in\mathbf{N}_n$, $\alpha_{ij}=i\otimes j$, onde cada elemento de $\mathbf{N}_n$ ocorre exactamente uma vez em cada uma das linhas e colunas. Com efeito, supondo que $\exists j\in\mathbf{N}_n$ e $\exists i_1,i_2\in\mathbf{N}_n$ ($\exists j_1,j_2\in\mathbf{N}_n$ e $\exists i\in\mathbf{N}_n$) tais que $i_1\otimes j=i_2\otimes j$ ($i\otimes j_1=i\otimes j_2$), pela definição de quasigrupo vem que $i_1=i_2$ ($j_1=j_2$). Consequentemente, não existem elementos repetidos em qualquer das linhas ou colunas de A e, uma vez que cada uma tem n componentes, conclui-se, também, que cada linha e cada coluna contém todos os elementos de S. Este tipo de matrizes (arranjos quadrangulares de n elementos, onde cada elemento ocorre exactamente uma vez em cada linha e coluna) designam-se por **quadrados latinos** de ordem n. A matriz que a seguir se apresenta constitui um exemplo de um quadrado latino de ordem 5.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{bmatrix}.$$

Usualmente denota-se por L(n) o número total de quadrados latinos distintos de ordem n (o qual, naturalmente, coincide com o número de quasigrupos de ordem n) e, até ao momento, apenas se conhecem os valores exactos de L(n), para $n\leq 9$ [27].

3.14 Problema (em aberto)

Determinar L(n), para $n>9$.

[27] Por exemplo, $L(5)=56.5!.4!$

Exercícios

3.1 - Sendo A_n o conjunto de todas as permutações pares de elementos $\mathbf{N}_n$ prove que A_n munido do produto de transposições é um grupo.

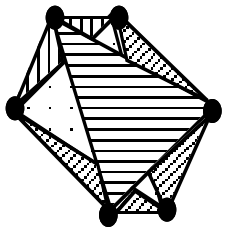
3.2 - Prove que A_n é um subgrupo de S_n de índice 2 e que, consequentemente, é um subgrupo normal de S_n.

3.3 - Dado um grupo arbitrário G de ordem n, onde *e* denota o lemento neutro, e $x \in G$, prove que a) $\langle x \rangle$ é um grupo; b) $k=|\langle x \rangle|$ é o menor inteiro positivo tal que $x^k=e$; c) $x^n=e$.

3.4 Dado um grupo G, prove que a relação de conjugação em G, R, definida por $(f,h) \in R$ sse $\exists g \in G$ tal que $f=g^{-1}hg$, é uma relação de equivalência.

3.5 - Supondo que G é um grupo finito, que $\leq$ define uma relação linear em G e que X é um conjunto-G, prove que a relação $\sim$, definida em GxX por $(g_1,x_1) \sim (g_2,x_2) \Leftrightarrow (g_1x_1=g_2x_2$ e $g_1 \leq g_2)$, é uma relação de ordem parcial.

3.6 - Supondo que se pretende colorir os 6 vértices de um octaedro regular utilizando três cores distintas (por exemplo, verde, azul e vermelho), quantas colorações, de diferentes tipos, são possíveis e (em particular) quantas, de entre estas, têm 3 vértices verdes, 1 azul e 2 vermelhos)?



Sugestão: Identifique o grupo simétrico do octaedro com o subgrupo de S_6, associando cada movimento rígido do octaedro com a correspondente permutação dos vértices.