Matrius i vectors (grup de matí)

Curs 2018–2019

12.1 Permutacions

Una *permutació* de n elements $x_1, \ldots, x_n$ és una aplicació bijectiva del conjunt $\{x_1, \ldots, x_n\}$ en ell mateix. Per simplificar la notació, estudiarem només les permutacions del conjunt $\{1, \ldots, n\}$. Una permutació d'aquest conjunt és una aplicació bijectiva $\sigma\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$, és a dir,

$$1 \mapsto \sigma(1), \qquad 2 \mapsto \sigma(2), \qquad \ldots, \qquad n \mapsto \sigma(n), \tag{12.1}$$

on $\sigma(1), \ldots, \sigma(n)$ són els mateixos nombres $1, \ldots, n$ però canviats d'ordre. És millor denotar (12.1) així:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

El conjunt de totes les permutacions de $\{1, \ldots, n\}$ es denota per S_n. És un conjunt format per $n!$ elements, on $n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$, ja que $\sigma(1)$ pot ser qualsevol element de $\{1, \ldots, n\}$; llavors $\sigma(2)$ pot ser qualsevol dels $n-1$ restants, etc.

La permutació *identitat* es denota per id i satisfà $\mathrm{id}(k) = k$ per a tot k:

$$\mathrm{id} = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Dues permutacions es poden *compondre* o *multiplicar* tal com es componen les aplicacions:

$$\tau\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \ldots & \tau(\sigma(n)) \end{pmatrix}.$$

Per tant, $\tau\sigma$ és la permutació que consisteix en fer actuar primer σ i a continuació τ. S'anomena *composició* o *producte* de σ i τ.

Un *grup* és un conjunt G amb una operació $G \times G \to G$ que és associativa, té element neutre e i per a tot element $g \in G$ hi ha un invers, és a dir, un element g^{-1} tal que $gg^{-1} = g^{-1}g = e$. Un grup es diu *commutatiu* quan l'operació és, a més, commutativa: $gh = hg$ per a tot parell d'elements g i h.

Proposició 12.1. *El conjunt S_n de permutacions de $\{1, \ldots, n\}$ és un grup amb l'operació de composició.*

Demostració. La composició d'aplicacions és associativa: $(\omega\tau)\sigma = \omega(\tau\sigma)$, i la permutació identitat id és un element neutre: $\mathrm{id}\,\sigma = \sigma\,\mathrm{id} = \sigma$ per a tota σ. A més, cada permutació σ té una inversa, ja que σ és una aplicació bijectiva. Així doncs, la inversa σ^{-1} està caracteritzada per $\sigma^{-1}(\sigma(k)) = k$ per a tot $k \in \{1, \ldots, n\}$. □

El conjunt S_n amb l'operació de composició s'anomena *grup simètric* sobre n elements. És important observar que S_n només és commutatiu quan $n = 1$ o bé $n = 2$. El grup S_1 només té la permutació identitat i el grup S_2 té dos elements: la identitat i la permutació que envia $1 \mapsto 2$ i $2 \mapsto 1$.

12.2 Descomposició en transposicions

Una *transposició* és una permutació que deixa fixos tots els elements excepte dos. Una transposició σ es denota per (i,j) si $\sigma(i)=j$, $\sigma(j)=i$ i $\sigma(k)=k$ per a tot $k\notin\{i,j\}$. Per exemple, amb $n=8$,

$$(2,5)=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 3 & 4 & 2 & 6 & 7 & 8 \end{pmatrix}.$$

Més en general, un *cicle d'ordre* p és una permutació σ tal que existeixen $i_1,\ldots,i_p$ tals que

$$\sigma(i_1)=i_2,\quad \sigma(i_2)=i_3,\quad \ldots,\quad \sigma(i_{p-1})=i_p,\quad \sigma(i_p)=i_1$$

i a més $\sigma(k)=k$ per a tot $k\notin\{i_1,\ldots,i_p\}$. Aleshores s'escriu $\sigma=(i_1,\ldots,i_p)$. Una transposició és un cicle d'ordre 2.

Teorema 12.2. *Tota permutació és composició de cicles disjunts, i els cicles disjunts commuten entre ells.*

Demostració. Donada una permutació $\sigma\in S_n$, si tots els elements de $\{1,\ldots,n\}$ són fixos per σ, aleshores σ és la identitat. Si no, escollim j_1 mínim amb $\sigma(j_1)\neq j_1$. Posem $j_2=\sigma(j_1)$, $j_3=\sigma(j_2)$ i així successivament fins a trobar un j_r tal que $\sigma(j_r)=j_1$ (com que σ és bijectiva, aquest j_r ha d'existir). Aleshores $(j_1,\ldots,j_r)$ és un cicle. Si tots els elements diferents de $j_1,\ldots,j_r$ són fixos per σ, ja hem acabat. En cas contrari, escollim k_1 mínim tal que $k_1\notin\{j_1,\ldots,j_r\}$ i $\sigma(k_1)\neq k_1$. Posem $k_2=\sigma(k_1)$, $k_3=\sigma(k_2)$ i així successivament fins a trobar un k_s tal que $\sigma(k_s)=k_1$. Aleshores $(k_1,\ldots,k_s)$ és un cicle que no té cap element en comú amb $(j_1,\ldots,j_r)$ i, per tant, es compleix

$$(j_1,\ldots,j_r)(k_1,\ldots,k_s)=(k_1,\ldots,k_s)(j_1,\ldots,j_r).$$

Si tots els elements diferents de $j_1,\ldots,j_r,k_1,\ldots,k_s$ són fixos per σ, ja hem acabat. En cas contrari, continuem aquest procés mentre sigui possible, i ens quedarà σ expressada com una composició de cicles disjunts. $\square$

Corol·lari 12.3. *Tota permutació és composició de transposicions.*

Demostració. Tot cicle es pot escriure com una composició de transposicions:

$$(i_1,\ldots,i_p)=(i_1,i_p)\cdots(i_1,i_3)(i_1,i_2).$$

Aleshores l'enunciat és conseqüència del teorema 12.2. $\square$

La descomposició d'una permutació en composició de transposicions no és única, ja que, per exemple, $\mathrm{id}=(1,2)(1,2)=(1,2)(1,2)(3,4)(3,4)$. Ara bé, es compleix el fet següent, que és fonamental en la teoria de permutacions:

Teorema 12.4. *La paritat del nombre de transposicions en les descomposicions d'una permutació donada és sempre la mateixa.*

En altres paraules, si σ admet una descomposició en un nombre parell de transposicions, llavors totes les descomposicions de σ estan formades per un nombre parell de transposicions, i si σ admet una descomposició en un nombre senar de transposicions, llavors totes les descomposicions de σ estan formades per un nombre senar de transposicions.

Demostració del teorema. Considerem el nombre enter

$$P(n) = \prod_{1 \leq i < j \leq n} (j - i), \tag{12.2}$$

que és positiu ja que $j - i > 0$ si $i < j$. Per a cada permutació $\sigma \in S_n$, podem definir

$$\sigma(P(n)) = \prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i)).$$

Com que σ és una permutació dels elements del conjunt $\{1, \ldots, n\}$, es compleix

$$\sigma(P(n)) = \pm P(n),$$

ja que després d'aplicar σ a (12.2) podem reordenar els factors resultants per tornar a tenir-los en el mateix ordre en què estaven, i descobrirem que alguns factors $j - i$ han quedat idèntics i d'altres s'han invertit, en el qual cas han passat a $i - j$ i per tant han canviat de signe.

A continuació, observem que si τ és una transposició aleshores $\tau(P(n)) = -P(n)$. Això és degut als fets següents: si $\tau = (k, \ell)$ amb $k < \ell$, aleshores

- El factor $\ell - k$ es converteix en $k - \ell$ i canvia de signe.
- Els factors $j - i$ amb i i j diferents de k i ℓ no varien.
- Els factors $k - i$ amb $i < k$ es converteixen en $\ell - i$ i no canvien de signe.
- Els factors $\ell - i$ amb $i < k$ es converteixen en $k - i$ i no canvien de signe.
- Els factors $\ell - i$ amb $k < i < \ell$ es converteixen en $k - i$ i canvien de signe; d'aquests factors n'hi ha $\ell - k - 1$.
- Els factors $j - k$ amb $k < j < \ell$ es converteixen en $j - \ell$ i canvien de signe; d'aquests factors n'hi ha també $\ell - k - 1$.
- Els factors $j - k$ amb $j > \ell$ es converteixen en $j - \ell$ i no canvien de signe.
- Els factors $j - \ell$ amb $j > \ell$ es converteixen en $j - k$ i no canvien de signe.

En definitiva, el nombre de canvis de signe ha estat de $2(\ell - k - 1) + 1$, que és un nombre senar. Per tant, $\tau(P(n)) = -P(n)$, tal com havíem afirmat.

Si una permutació σ es descompon en transposicions com $\sigma = \tau_r \cdots \tau_1$, aleshores $\sigma(P(n)) = P(n)$ si r és parell i $\sigma(P(n)) = -P(n)$ si r és senar. Això demostra, tal com volíem, que si $\sigma = \tau'_s \cdots \tau'_1$ per a un altre conjunt de transposicions, llavors s té la mateixa paritat que r. $\square$

Les permutacions que es descomponen en un nombre parell de transposicions s'anomenen *permutacions parelles* i les que es descomponen en un nombre senar de transposicions es diuen *permutacions senars*.

El *signe* d'una permutació σ es denota per $\varepsilon(\sigma)$ i es defineix com 1 si σ és una permutació parella i -1 si σ és una permutació senar. Observem que $\varepsilon(\mathrm{id}) = 1$ i que

$$\varepsilon(\omega\sigma) = \varepsilon(\omega)\,\varepsilon(\sigma) \tag{12.3}$$

per a qualsevol parell de permutacions ω i σ, ja que $\omega\sigma$ és parella si i només si ω i σ són totes dues parelles o bé totes dues senars. En conseqüència, $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$ per a qualsevol σ.

L'expressió (12.3) ens indica que el subconjunt de S_n format per les permutacions parelles és un *subgrup* de S_n, que es denota per A_n i s'anomena *grup alternat* sobre n elements. Així doncs,

$$A_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}.$$

Com que el nombre de permutacions parelles és el mateix que el nombre de permutacions senars (ja que si σ és parella i τ és una transposició llavors $\tau\sigma$ és senar), resulta que A_n té $\frac{1}{2}n!$ elements.