Repàs de permutacions. Estructures Algebraiques.

Sigui $[n] = \{1, \dots, n\}$. Una **permutació** de $[n]$ és una aplicació bijectiva de $[n]$ en $[n]$. El conjunt de les permutacions de $[n]$ amb la composició té estructura de grup. S'anomena el grup simètric i es denota $\mathfrak{S}_n$. Els elements $\sigma \in \mathfrak{S}_n$ es denoten:

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

Si $\sigma, \tau \in \mathfrak{S}_n$, aleshores $\sigma\tau$ denota l'element $\sigma \circ \tau$ on $\sigma\tau(a) = \sigma(\tau(a))$, per a tot $a \in [n]$. Recordeu que el grup $\mathfrak{S}_n$ té $n!$ elements. A més a més, si $n \geqslant 3$, aleshores $\mathfrak{S}_n$ no és commutatiu.

Dues permutacions σ i τ es diuen **disjuntes** si "mouen" elements diferents. És dir, si $\sigma(a) \neq a$, aleshores $\tau(a) = a$. Comproveu que dues permutacions disjuntes commuten. (Si $\sigma(a) \neq a$, aleshores, per ser injectiva, $\sigma(\sigma(a)) \neq \sigma(a)$. Per tant $\tau(a) = a$ i $\tau(\sigma(a)) = \sigma(a)$. Així, $\sigma\tau(a) = \sigma(a)$ i $\tau\sigma(a) = \sigma(a)$. Anàlogament si $\tau(a) \neq a$. Finalment, si $\sigma(a) = a$ i $\tau(a) = a$, aleshores $\sigma\tau(a) = \tau\sigma(a)$.)

Donats $a_1, \dots, a_r$ elements diferents de $[n]$, $(a_1, a_2, \dots, a_r)$ és la permutació definida per $a_1 \mapsto a_2$, $a_2 \mapsto a_3, \dots, a_r \mapsto a_1$. S'anomena un r-**cicle**. Els cicles (a, b) de longitud 2 s'anomenen **transposicions**. Observem que si $\sigma = (a_1, a_2, \dots, a_r)$, aleshores $\sigma = (a_1, a_2)(a_2, a_3) \cdots (a_{r-2}, a_{r-1})(a_{r-1}, a_r)$, o bé, $\sigma = (a_1, a_r)(a_1, a_{r-1}) \cdots (a_1, a_3)(a_1, a_2)$.

Proveu que tota permutació σ es pot escriure de forma única, llevat ordenació, com a producte de cicles disjunts. L'anomenarem la **descomposició en cicles disjunts** de σ i la denotarem $\mathrm{dcd}(\sigma)$. Denotarem $\mathrm{ncd}(\sigma)$ el **nombre de cicles disjunts** en què descomposa $\sigma \in \mathfrak{S}_n$, comptant els cicles de longitud 1. Per exemple, $\mathrm{ncd}(\mathrm{id}) = n$; $\mathrm{ncd}(\tau) = n - 1$, si τ és una transposició; $\mathrm{ncd}((1, 3)(4, 5, 6)) = 3$, a $\mathfrak{S}_6$.

Com que tot cicle descomposa en producte de transposicions, deduïm que tota permutació descomposa en producte de transposicions.

Comproveu que si τ és una transposició i σ és una permutació qualsevol, aleshores $\mathrm{ncd}(\tau\sigma) = \mathrm{ncd}(\sigma) \pm 1$. Deduïm que si $\sigma_1\sigma_2 \cdots \sigma_r$ i $\tau_1\tau_2 \cdots \tau_s$ són dues descomposicions de σ en producte de transposicions, aleshores r is s tenen la mateixa paritat. Diem que σ és **parell** (**senar**) si r (i s) és parell (senar). El signe de σ és $(-1)^r = \pm 1$. El denotem $\mathrm{sgn}(\sigma)$. Observeu que $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma)\,\mathrm{sgn}(\tau)$.

El subconjunt $\mathfrak{A}_n$ de $\mathfrak{S}_n$ format per les permutacions parells és un subgrup de $\mathfrak{S}_n$. S'anomena el **grup alternat**.

Siguin $\sigma, \tau \in \mathfrak{S}_n$. La permutació $\tau\sigma\tau^{-1}$ es diu la **conjugada** de σ per τ. Proveu que si $\sigma = (a_1, a_2, \dots, a_r)$, aleshores $\tau\sigma\tau^{-1} = (\tau(a_1), \tau(a_2), \dots, \tau(a_r))$. En particular, $\tau(\sigma_1\sigma_2 \dots \sigma_r)\tau^{-1} = (\tau\sigma_1\tau^{-1})(\tau\sigma_2\tau^{-1}) \dots (\tau\sigma_r\tau^{-1})$.

Donat $\sigma \in \mathfrak{S}_n$, aleshores existeix un enter $k \geqslant 1$ tal que $\sigma^k = \mathrm{id}$ (pensar en el subconjunt $\{\sigma^k, k \geqslant 1\}$ de $\mathfrak{S}_n$, el qual és finit). El menor enter complint aquesta condició se l'anomena l'**ordre** de σ. Els enters k tals que $\sigma^k = \mathrm{id}$ són necessàriament múltiples de l'orde de σ. D'aquí, i usant que tota permutació descomposa en cicles disjunts, es demostra que l'ordre d'una permutació és el mínim comú múltiple de les longituds dels cicles disjunts en què descomposa.

0.1. Considereu les permutacions $\sigma, \tau \in \mathfrak{S}_5$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 4 & 3 \end{pmatrix}.$$

Calculeu $\sigma\tau$, $\tau\sigma^2$ i σ^{-1}.

0.2. Trobeu $\sigma, \tau \in \mathfrak{S}_7$ tals que

$$\sigma \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 3 & 4 & 7 & 6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 7 & 6 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 3 & 4 & 7 & 6 & 1 \end{pmatrix} \tau.$$

0.3. Comproveu que tota permutació de $\mathfrak{S}_4$ s'obté com a producte de transposicions $(1,2)$, $(1,3)$ i $(1,4)$.

0.4. Per a cadascuna de les permutacions següents:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 8 & 9 & 4 & 5 & 2 & 1 & 6 \end{pmatrix} \in \mathfrak{S}_9, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 6 & 8 & 2 & 7 & 5 \end{pmatrix} \in \mathfrak{S}_8,$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 10 & 5 & 2 & 4 & 9 & 3 & 1 & 6 & 7 \end{pmatrix} \in \mathfrak{S}_{10},$$

calculeu la descomposició en cicles disjunts, una descomposició en producte de transposicions, l'ordre i el signe. Calculeu també $\sigma_1^{1000}, \sigma_2^{250}$ i σ_3^{611}.

0.5. Trobeu les permutacions $\sigma \in \mathfrak{S}_8$ de la forma:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 6 & x & y & 1 & z & t \end{pmatrix}$$

que tenen ordre 3. Calculeu per a cadascuna d'elles $\sigma^{1457122}$.

0.6. Trobeu l'ordre i el signe de la permutació:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ n & n-1 & n-2 & \ldots & 2 & 1 \end{pmatrix} \in \mathfrak{S}_n.$$

0.7. Calculeu l'ordre i el signe de les permutacions següents:

1. $(4,2)(3,4)(3,7)(2,8)(5,11)(1,6,9) \in \mathfrak{S}_{11}$;
2. $(2,3)(3,4)(2,3,7)(2,8)(5,9,10)(1,6,9) \in \mathfrak{S}_{10}$;
3. $(1,2)(1,3)(1,2)(2,4)(1,2,5)(2,3) \in \mathfrak{S}_5$.

0.8. Quantes permutacions d'ordre 3 hi ha a $\mathfrak{S}_5$? I d'ordre 7?

0.9. Demostreu que tota permutació de $\mathfrak{S}_{10}$ d'ordre 14 és senar.

0.10. Sigui $\sigma \in \mathfrak{S}_{10}$ una permutació senar d'ordre 10. Com és la seva descomposició en cicles disjunts? Trobeu totes les permutacions senars d'ordre 10 de la forma:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 4 & 10 & 7 & a & b & c & d & 1 & 2 \end{pmatrix}.$$

0.11. Quins ordres pot tenir el producte de dues transposicions? I el de tres?

0.12. Demostreu que el nombre de permutacions parells i senars és el mateix: $\frac{1}{2}n!$.

0.13. Al grup $\mathfrak{S}_9$ considereu les permutacions:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 9 & 1 & 8 & 6 & 3 & 2 & 4 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 9 & 6 & 1 & 8 & 2 & 4 & 3 \end{pmatrix}$$

i els cicles $\gamma_1 = (2,4,6)$, $\gamma_2 = (2,7,9)$ i $\gamma_3 = (1,6,3,9)$.

1. Calculeu σ_1^{2015} i σ_2^{2016}.
2. Les permutacions de $\mathfrak{S}_9$ es poden obtenir totes a partir de $\sigma_1, \sigma_2, \gamma_1$ i γ_2?
3. Digueu si les permutacions σ_1 i σ_2 són o no conjugades; si ho són, quantes permutacions $\sigma \in \mathfrak{S}_9$ compleixen $\sigma\sigma_1\sigma^{-1} = \sigma_2$?
4. Digueu si les permutacions $\gamma_1\gamma_2\gamma_3$ i $\gamma_3\gamma_2\gamma_1$ són o no conjugades; si ho són, quantes permutacions $\sigma \in \mathfrak{S}_9$ compleixen $\sigma\gamma_1\gamma_2\gamma_3\sigma^{-1} = \gamma_3\gamma_2\gamma_1$?

0.14. Trobeu totes les permutacions de $\mathfrak{S}_7$ que commuten amb la permutació

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 3 & 5 & 4 & 6 & 2 \end{pmatrix}.$$

0.15. Digueu quantes permutacions de $\mathfrak{S}_{10}$ commuten amb la permutació

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 2 & 3 & 9 & 10 & 6 & 7 & 4 & 8 & 1 \end{pmatrix}.$$

0.16. Siguin $\sigma_1, \ldots, \sigma_k \in \mathfrak{S}_n$ permutacions disjuntes. Demostreu que $\sigma_1\sigma_2\cdots\sigma_k = \mathrm{id} \Leftrightarrow \sigma_i = \mathrm{id}$ per a tot i.

0.17. Proveu que tota permutació σ es pot escriure de forma única, llevat ordenació, com a producte de cicles disjunts.

0.18. Comproveu que si $\tau = (a, b)$ és una transposició i σ és una permutació qualsevol, aleshores $\operatorname{ncd}(\tau\sigma) = \operatorname{ncd}(\sigma) \pm 1$. Per a fer-ho, estudieu els casos següents: a i b no estan en cap cicle de la $\operatorname{dcd}(\sigma)$; a està en un cicle de la $\operatorname{dcd}(\sigma)$ i b no està en cap cicle de la $\operatorname{dcd}(\sigma)$; a i b estan en diferents cicles de la $\operatorname{dcd}(\sigma)$; a i b estan en el mateix cicle de la $\operatorname{dcd}(\sigma)$.

0.19. Siguin $\sigma, \tau \in \mathfrak{S}_n$. Proveu que si $\sigma = (a_1, a_2, \ldots, a_r)$, aleshores

$$\tau(a_1, a_2, \ldots, a_r)\tau^{-1} = \tau\sigma\tau^{-1} = (\tau(a_1), \tau(a_2), \ldots, \tau(a_r)).$$

Indicació. Feu el cas $r = 2$ i useu $\tau(\sigma_1\sigma_2 \cdots \sigma_r)\tau^{-1} = (\tau\sigma_1\tau^{-1})(\tau\sigma_2\tau^{-1}) \cdots (\tau\sigma_r\tau^{-1})$. Deduïu que el conjugat d'un r-cicle és un r-cicle i que dos r-cicles qualssevol sempre són conjugats.

0.20. Donats $\sigma, \tau \in \mathfrak{S}_n$, denotarem $\tau(\sigma) := \tau\sigma\tau^{-1}\sigma^{-1}$. Suposem que $\sigma \in \mathfrak{A}_n$, $\sigma \neq \mathrm{id}$, amb $n \geqslant 5$. Proveu que passa una de les dues coses següents:

(a) Existeix un 3-cicle $\tau \in \mathfrak{A}_n$ tal que $\tau(\sigma)$ és un 3-cicle.

(b) Existeixen dos 3-cicles $\tau_1, \tau_2 \in \mathfrak{A}_n$ tals que $\tau_2(\tau_1(\sigma))$ és un 3-cicle.

Indicació. Estudieu els casos següents.

1. La $\operatorname{dcd}(\sigma)$ conté un r-cicle, amb $r \geqslant 4$. En aquest cas, existeix un 3-cicle $\tau \in \mathfrak{A}_n$ tal que $\tau(\sigma)$ és un 3-cicle.
2. La $\operatorname{dcd}(\sigma)$ és en dues transposicions. En aquest cas, existeix un 3-cicle $\tau \in \mathfrak{A}_n$ tal que $\tau(\sigma)$ és un 3-cicle.
3. La $\operatorname{dcd}(\sigma)$ és en $2k$ transposicions, $k \geqslant 2$. En aquest cas existeix un 3-cicle $\tau_1 \in \mathfrak{A}_n$ tal que $\tau_1(\sigma)$ és un producte de dues transposicions. Pel Cas 2, es dedueix que existeix un 3-cicle $\tau_2 \in \mathfrak{A}_n$ tal que $\tau_2(\tau_1(\sigma))$ és un 3-cicle.
4. σ és un 3-cicle. En aquest cas existeix un 3-cicle $\tau_1 \in \mathfrak{A}_n$ tal que $\tau_1(\sigma)$ és un producte de dues transposicions. Pel Cas 2, es dedueix que existeix un 3-cicle $\tau_2 \in \mathfrak{A}_n$ tal que $\tau_2(\tau_1(\sigma))$ és un 3-cicle.
5. La $\operatorname{dcd}(\sigma)$ és en un 3-cicle i $2k$ transposicions. En aquest cas existeix un 3-cicle $\tau_1 \in \mathfrak{A}_n$ tal que $\tau_1(\sigma)$ és un 5-cicle. Pel Cas 1, es dedueix que existeix un 3-cicle $\tau_2 \in \mathfrak{A}_n$ tal que $\tau_2(\tau_1(\sigma))$ és un 3-cicle.

6 La $\operatorname{dcd}(\sigma)$ és en k 3-cicles i $2l$ transposicions, $k \geqslant 2$, $l \geqslant 0$. En aquest cas existeix un 3-cicle $\tau_1 \in \mathfrak{A}_n$ tal que $\tau_1(\sigma)$ és un 5-cicle. Pel Cas 1, es dedueix que existeix un 3-cicle $\tau_2 \in \mathfrak{A}_n$ tal que $\tau_2(\tau_1(\sigma))$ és un 3-cicle.

(*Aquest exercici s'usarà més endavant per a deduir que $\mathfrak{A}_n$ és simple, si $n \geqslant 5$.*)