1. Determineu si els conjunts següents amb les operacions que s'indiquen són o no grups.

   (a) El conjunt dels nombres naturals $\mathcal{N}$ amb la suma.

      i. (Operació interna) $\forall x, y \in \mathcal{N}(x + y \overset{?}{\in} \mathcal{N})$
      ii. (Associativa)
      iii. (Element neutre)
      iv. (Inversos)

   (b) El conjunt dels nombres racionals $\mathcal{Q}$ amb:

      i. La suma.
      ii. El producte.

9 Sigui G un grup cíclic d'ordre n, generat per un element a. Per a tot nombre enter k, determineu l'ordre del subgrup generat per a^k i demostreu que a^k és un generador de G si, i només si, $mcd(k, n) = 1$.

Sigui $|G| = n$ i $G = \langle a \rangle$, volem determinar $|\langle a^k \rangle| = ord(a^k)$:

$$(a^k)^l = e \iff a^{kl} = e \implies n \mid kl$$

Definim $d = mcd(n, k)$, $n = n'd$ i $k = k'd$, amb $mcd(n', k') = 1$, llavors:

$$\left.\begin{array}{l} n \mid kl \implies n' \mid k'l \implies \dfrac{n}{mcd(k,n)} = n' \mid l \\ (a^k)^{n'} = a^{kn'} = a^{k'n} = (a^n)^{k'} = e^{k'} = e \end{array}\right\} \implies ord(a^k) = \frac{n}{mcd(k,n)}$$

Per tant, a partir de la conclusió anterior:

$$G = \langle a^k \rangle \iff ord(a^k) = |G| = n \iff mcd(k, n) = 1$$

10 Sigui G un grup cíclic d'ordre n.

   (a) Demostreu que tot subgrup de G és cíclic.
   Sigui $H < G$ i $k \in \mathbb{Z}$ tal que $k = min(\{k \in \mathbb{Z} \mid a^k \in H\})$, volem veure $H = \langle a^k \rangle$:

   $\supset$ | Aquesta implicació és trivial ja que:

   $$(a^k \in H) \wedge (H < G) \implies \langle a^k \rangle \subset H.$$

   $\subset$ | Sigui $a^m \in H$, com $m \in \mathbb{Z}$, podem descomposar $m = kq + r$ amb $(q, r \in Z) \wedge (0 \leq r < k)$:

   $$a^m = a^{kq+r} = (a^k)^q a^r$$

Llavors, tenim $(a^k)^q \in \langle a^k \rangle \subset H$, per tant $a^m \in \langle a^k \rangle \iff a^r \in \langle a^k \rangle$.

$$\left.\begin{aligned} a^m = (a^k)^q a^r \implies a^r = a^m((a^k)^q)^{-1} \in H \\ k = min(\{k \in \mathbb{Z} \mid a^k \in H\}) \wedge (0 \leq r < k) \end{aligned}\right\} \implies r = 0$$

Per tant, $a^r = e \in \langle a^k \rangle \implies a^m \in \langle a^k \rangle$.

(b) Demostreu que, per a cada divisor d de n, existeix un únic subgrup de G d'ordre d.

Per l'exercici 9:

$$\begin{aligned} |\langle a^k \rangle| = d &\iff ord(a^k) = d \\ &\iff ord(a^k) = \frac{n}{mcd(k,n)} = d \\ &\iff mcd(k,n) = \frac{n}{d} \end{aligned}$$

D'aquí deduïm $mcd(k,n) = \frac{n}{d} \implies \frac{n}{d} \mid k$, i llavors, $k =$

11 Sigui $\mu_n = \{z \in \mathbb{C} : \ z^n = 1\}$ el conjunt de les arrels n-èsimes de la unitat complexes. Demostreu que μ_n amb el producte de $\mathbb{C}$ és un grup cíclic.

12 Siguin p, q nombres primers diferents i r, $s \geq 1$ nombres enters.

(a) Determineu quants elements del grup $\mathbb{Z}/p\mathbb{Z}$ el generen.

OPCIO 1

OPCIO 2

Per l'exercici 9, sabem que

$$(|G| = n) \wedge (G = \langle a \rangle) \implies (G = \langle a^k \rangle \iff mcd(k,n) = 1)$$

Llavors, per a tot n tal que $|\mathbb{Z}/n\mathbb{Z}| = n$ i $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$:

$$\mathbb{Z}/n\mathbb{Z} = \langle k \cdot 1 \rangle = \langle k \rangle \iff mcd(k,n) = 1$$

Aplicant-ho, el cardinal del conjunt de generadors de $\mathbb{Z}/n\mathbb{Z}$ serà:

$$\#\{x \in \{1,\ldots,n\} \mid \langle x \rangle = \mathbb{Z}/n\mathbb{Z}\} = \#\{x \in \{1,\ldots,n\} \mid mcd(x,n) = 1\}$$

Aquest conjunt és equivalent al de la funció φ d'Euler per a un n qualsevol. Per tant, el cardinal del conjunt de generadors de $\mathbb{Z}/n\mathbb{Z}$ és $\varphi(n)$.

CONCLUSIO

Llavors, per al grup $\mathbb{Z}/p\mathbb{Z}$:

$$\#\{x \in \{1,\ldots,p\} \mid \langle x \rangle = \mathbb{Z}/p\mathbb{Z}\} = \varphi(p) = p - 1$$

(b) Determineu quants elements del grup $\mathbb{Z}/p^r\mathbb{Z}$ el generen.

Pel raonament de l'apartat anterior:

$$\begin{aligned}\#\{x \in \{1,\ldots,p^r\} \mid \langle x\rangle = \mathbb{Z}/p^r\mathbb{Z}\} &= \#\{x \in \{1,\ldots,p^r\} \mid mcd(x,p^r)=1\}\\ &= \varphi(p^r) = p^{r-1}(p-1) = p^r - p^{r-1}\end{aligned}$$

(c) Determineu quants elements del grup $\mathbb{Z}/p^rq^s\mathbb{Z}$ el generen.
Pel raonament de l'apartat anterior:

$$\begin{aligned}\#\{x \in \{1,\ldots,p^rq^s\} \mid \langle x\rangle = \mathbb{Z}/p^rq^s\mathbb{Z}\} &= \#\{x \in \{1,\ldots,p^rq^s\} \mid mcd(x,p^rq^s)=1\}\\ &= \varphi(p^rq^s)\end{aligned}$$

Llavors, apliquem la següent propietat de la funció φ d'Euler:

$$\forall m,n \in \mathbb{N}: \ (mcd(m,n)=1 \implies \varphi(mn)=\varphi(m)\varphi(n))$$

Per tant, com $mcd(p,q)=1 \implies mcd(p^r,q^s)=1$:

$$\varphi(p^r,q^s) = \varphi(p^r)\varphi(q^s) = (p^{r-1}(p-1))(q^{s-1}(q-1)) = (p^r-p^{r-1})(q^s-q^{s-1})$$

13 Siguin σ, $\tau \in S_9$ les permutacions següents:

$$\sigma = \begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&9&1&8&7&6&3&4&5\end{pmatrix}, \qquad \tau = \begin{pmatrix}1&2&3&4&5&6&7&8&9\\7&1&3&5&8&2&9&6&4\end{pmatrix}$$

(a) Calculeu $\sigma\tau$ i $\tau\sigma$.

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

(b) Descomponeu σ i τ com a producte de cicles disjunts, i també com a producte de transposicions; calculeu les seves signatures.

$$\sigma = (1,2,9,5,7,3)(4,8) = (1,2)(2,9)(5,9)(5,7)(3,7)(4,8)$$
$$\tau = (1,7,9,4,5,8,6,2) = (1,7)(7,9)(4,9)(4,5)(5,8)(6,8)(2,6)$$
$$\varepsilon(\sigma) = 1$$
$$\varepsilon(\tau) = -1$$

(c) Calculeu σ^{2015}.
Siguin $\sigma_1 = (1,2,9,5,7,3)$ i $\sigma_2 = (4,8)$ cicles disjunts a S_9, d'ordre 6 i 2 respectivament, sabem que:

$$\sigma = \sigma_1\sigma_2 = \sigma_2\sigma_1, \qquad (\sigma_1)^6 = Id, \qquad (\sigma_2)^2 = Id$$

Per tant, aplicant la descomposició de σ en cicles disjunts i la commutativitat d'aquests cicles entre ells:

$$\sigma^n = (\sigma_1\sigma_2)^n = \overbrace{(\sigma_1\sigma_2)(\sigma_1\sigma_2)\ \cdots\ (\sigma_1\sigma_2)}^{n}$$
$$= \overbrace{(\sigma_1\sigma_1\ \cdots\ \sigma_1)}^{n}\overbrace{(\sigma_2\sigma_2\ \cdots\ \sigma_2)}^{n} = (\sigma_1)^n(\sigma_2)^n$$

Llavors, a partit de les propietats anteriors:

$$\sigma^{2015} = \sigma^{(6\cdot 335+5)} = (\sigma^6)^{335}\sigma^5$$
$$\sigma^6 = (\sigma_1\sigma_2)^6 = (\sigma_1)^6(\sigma_2)^6 = Id((\sigma_2)^2)^3 = (Id)^3 = Id$$
$$= (Id)^{335}(\sigma)^5 = Id\ \sigma^5 = \sigma^5 = (\sigma_1\sigma_2)^5 = (\sigma_1)^5(\sigma_2)^5$$
$$= (\sigma_1)^5(\sigma_2)^{(2\cdot 2+1)} = (\sigma_1)^5((\sigma_2)^2)^2\sigma_2 = (\sigma_1)^5(Id)^2\sigma_2$$
$$= (\sigma_1)^5\sigma_2 = (1,3,7,5,9,2)(4,8)$$

14 Determineu la signatura de totes les permutacions de S_3. Determineu tots els subgrups de S_3.

Sigui $t_1 = (1,2)$, $t_2 = (1,3)$, $t_3 = (2,3)$, $c_1 = (1,2,3)$ i $c_2 = (1,3,2)$, llavors

$$S_3 = \{Id,\ t_1,\ t_2,\ t_3,\ c_1,\ c_2\}$$

$$\begin{array}{ll} \varepsilon(Id) = 1 & \varepsilon(t_3) = \varepsilon((2,3)) = -1 \\ \varepsilon(t_1) = \varepsilon((1,2)) = -1 & \varepsilon(c_1) = \varepsilon((1,2,3)) = \varepsilon((1,2)(2,3)) = 1 \\ \varepsilon(t_2) = \varepsilon((1,3)) = -1 & \varepsilon(c_2) = \varepsilon((1,3,2)) = \varepsilon((1,3)(2,3)) = 1 \end{array}$$

Per determinar tots els sugrups de S_3, pel teorema de Lagrange, ordre de qualsevol subgrup de S_3 ha de ser un divisor de l'ordre de S_3. Llavors, com $|S_3| = 6$ i 6 només té com a divisors 1, 2, 3 i 6, sabem que només els subconjunts d'ordre 1, 2, 3 i 6 poden ser subgrups. Sigui $A \subseteq S_3$:

- $|A| = 1$:

  $$\exists A = \{Id\} : ((Id\ Id = Id\ Id = Id) \implies A < S_3)$$

  A més, $\forall A \subseteq S_3 : (A \neq \{Id\} \implies Id \notin A \implies A \not< S_3)$, per tant, $\{Id\}$ és l'únic subgrup d'ordre 1.
- $|A| = 2$: Sabem que $Id \in A$ per a que A sigui un subgrup de S_3, llavors podem distinguir dos casos:
  - $A = \{Id, t_i\}$, $i \in \{1,2,3\}$:

    $$\forall i \in \{1,2,3\} :\ ((Id\, t_i = t_i) \wedge (t_i\, t_i = Id) \implies A = \{Id, t_i\} < S_3)$$
  - $A = \{Id, c_i\}$, $i \in \{1,2\}$:

    $$\forall i,j \in \{1,2\},\ i \neq j :\ ((c_i\, c_i = c_j) \wedge (c_j \notin A) \implies A = \{Id, c_i\} \not< S_3)$$

Per tant, els subgrups d'ordre 2 són $\{Id, t_1\}$, $\{Id, t_2\}$ i $\{Id, t_3\}$.

- $|A| = 3$: Com al cas anterior, sabem que $Id \in A$, llavors tornem a distinguir tres casos:
  - $A = \{Id, t_i, t_j\}$, $i, j \in \{1, 2, 3\}$, $i \neq j$:

    $$\forall i, j \in \{1, 2, 3\},\ i \neq j :\ (\exists k \in \{1, 2\} :\ t_i\, t_j = c_k \notin A) \implies A \not< S_3$$
  - $A = \{Id, c_1, c_2\}$:

    $$(c_1\, c_1 = c_2) \wedge (c_2\, c_2 = c_1) \wedge (c_1\, c_2 = c_2\, c_1 = Id) \implies A < S_3$$
  - $A = \{Id, c_i, t_j\}$, $i \in \{1, 2, 3\}$, $j \in \{1, 2\}$:

    $$\begin{aligned} &\forall i \in \{1, 2, 3\},\ j \in \{1, 2\} :\ \varepsilon(c_i)\ \varepsilon(t_j) = 1 \cdot (-1) = -1 \\ &\quad \implies \exists k \in \{1, 2, 3\} :\ ((c_i\ t_j = t_k) \wedge (c_i \neq Id \implies k \neq j)) \\ &\quad \implies A \not< S_3 \end{aligned}$$

  Per tant, l'únic subgrup d'ordre 3 és $\{Id, c_1, c_2\}$.
- $|A| = 6$: Sabem que l'únic subconjunt de S_3 amb el seu mateix ordre és ell mateix, llavors $A = S_3 < S_3$ és l'unic subgrup d'ordre 6.

Com a conclusió, els subgrups de S_3 són $\{Id\}$, $\{Id, t_1\}$, $\{Id, t_2\}$, $\{Id, t_3\}$, $\{Id, c_1, c_2\}$ i S_3.

15 Demostreu que, per a $n \geq 2$, S_n té el mateix nombre de permutacions parelles que de permutacions senars.

OPCIO1

Definim $\tau \in S_n$ com una permutació senar qualsevol, amb $n \geq 2$, ja que a S_1 no hi ha permutacions senars. Llavors podem definir una aplicació entre les permutacions parelles i les senars de la manera següent:

$$\begin{aligned} f : A_n &\longrightarrow S_n \setminus A_n \\ \sigma &\longmapsto f(\sigma) = \tau\sigma = \gamma \end{aligned}$$

Cal tenir present que:

$$A_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\} \qquad S_n \setminus A_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = -1\}$$

Primer cal demostrar que l'aplicació està ben definida:

$$\forall \sigma \in A_n :\ (\varepsilon(\tau\sigma) = \varepsilon(\tau) \cdot \varepsilon(\sigma) = (-1) \cdot 1 = -1 \implies \tau\sigma \in S_n \setminus A_n)$$

Després, cal provar que és una aplicació bijectiva, i així haurem provat que $|A_n| = |S_n \setminus A_n|$. Per arribar a que f és bijectiva, provarem que és injectiva i exhaustiva:

- f és injectiva $\iff \forall \sigma, \sigma' \in A_n : \ (f(\sigma) = f(\sigma') \overset{?}{\Longrightarrow} \sigma = \sigma')$:

  $$f(\sigma) = f(\sigma') \implies \tau\sigma = \tau\sigma' \implies \tau^{-1}\tau\sigma = \tau^{-1}\tau\sigma' \implies \sigma = \sigma'$$

- f és exhaustiva $\iff \forall \gamma \in S_n \setminus A_n \ \exists \sigma \in A_n : \ f(\sigma) \overset{?}{=} \gamma$:

  $$\begin{aligned}
  &\gamma \in S_n \setminus A_n \implies \tau^{-1}\gamma = \sigma \in S_n \\
  &(\varepsilon(\tau) = -1) \wedge (\varepsilon(Id) = 1) \wedge (\tau\tau^{-1} = Id) \implies \varepsilon(\tau^{-1}) = -1 \\
  &\varepsilon(\sigma) = \varepsilon(\tau^{-1}\gamma) = \varepsilon(\tau^{-1})\varepsilon(\gamma) = 1 \implies \sigma \in A_n \\
  &\forall \gamma \in S_n \setminus A_n : \ (\tau^{-1}\gamma = \sigma \in A_n \implies \tau\tau^{-1}\gamma = \tau\sigma \implies \gamma = \tau\sigma = f(\sigma))
  \end{aligned}$$

Per tant, f és una aplicació bijectiva, i $|A_n| = |S_n \setminus A_n|$.

OPCIO 2

Per a tot grup simètric S_n, podem definir:

$$\begin{aligned} \varepsilon : S_n &\longrightarrow \{\pm 1\} \\ \sigma &\longmapsto \varepsilon(\sigma) \end{aligned} \qquad \text{on } \ \varepsilon(\sigma) = \begin{cases} 1 & \text{si } \sigma \in A_n \\ -1 & \text{si } \sigma \in S_n \setminus A_n \end{cases}$$

Com ja hem demostrat a teoria, aquesta aplicació és un morfisme de grups i és exhaustiva per tot $n \geq 2$. A més:

$$\left.\begin{array}{l} \forall \sigma \in A_n : \ \varepsilon(\sigma) = 1 \\ \forall \tau \in S_n \setminus A_n : \ \varepsilon(\tau) = -1 \\ \text{L'element neutre de } \{\pm 1\} \text{ és } 1 \end{array}\right\} \implies Ker(\varepsilon) = A_n$$

Llavors, teorema d'isomorfia, tenim que:

$$\begin{aligned} \tilde{\varepsilon} : S_n/A_n &\longrightarrow \{\pm 1\} \\ [\bar{\sigma}] &\longmapsto \varepsilon(x) \end{aligned}$$

També per propietats demostrades a teoria, totes les classes d'una relació d'equivalencia associada a un subgrup tenen el mateix cardinal que el subgrup. Com, $\tilde{\varepsilon}$ només pot ser 1 o -1, hi ha dos classes associades al subgrup A_n, i són el mateix A_n i $S_n \setminus A_n$. Llavors aquestes dos classes han de tenir el mateix cardinal; per tant $|A_n| = |S_n \setminus A_n|$.

OPCIO 3

Tot grup simètric S_n, amb $n \geq 2$, conté almenys una permutació parella, per exemple Id, i almenys una senar, per exemple el cicle $(1, 2)$. A més, com $|S_n| = n!$, hi haura un nombre finit de permutacions senar i parelles.

Siguin $A_n = \{\sigma_1, \sigma_2, \ldots, \sigma_r\}$ el conjunt de totes les permutacions parelles de S_n, i $S_n \setminus A_n = I = \{\tau_1, \tau_2, \ldots, \tau_s\}$ el conjunt de totes les permutacions senars de S_n, cal veure $r = s$:

$$\left.\begin{array}{l} \forall i \in \{1, \ldots, r\}: \ \varepsilon(\sigma_i \tau_1) = -1 \implies \sigma_i \tau \in I \implies r \leq s \\ \forall j \in \{1, \ldots, s\}: \ \varepsilon(\tau_j \tau_1) = 1 \implies \tau_j \tau_1 \in A_n \implies r \geq s \end{array}\right\} \implies r = s$$

Per tant, com $r = s$, $|A_n| = |I| = |S_n \setminus A_n|$.

17 Demostreu que S_n admet el sistema de generadors següents:

(a) $A = \{(1,2),\ (1,3), \ldots,\ (1,n)\}$

Volem demostrar $S_n = \langle A \rangle$, sigui $A = \{(1,a) \in S_n\}$. $\langle A \rangle \subseteq S_n$ és trivial, ja que $\forall \sigma \in A: \ \sigma \in S_n$.
Només ens cal demostrar que $S_n \subseteq \langle A \rangle$, per fer-ho, utilitzarem el fet que $\forall a, b \in \mathbb{N}: \ (a \neq b) \wedge (S_n \subseteq \langle (a,b) \rangle)$, ja que, qualsevol permutació és pot expressar com a producte de transposicions.
Llavors, només cal provar que $\langle \{(a,b) \in S_n\} \rangle \subseteq \langle A \rangle$:

$$\exists (1,a), (1,b) \in A: \ (a,b) = (1,a)(1,b)(1,a) \implies (a,b) \in \langle A \rangle$$

(b) $B = \{(1,2),\ (2,3), \ldots,\ (n-1,n)\}$

Volem demostrar $S_n = \langle B \rangle$, sigui $B = \{(a, a+1) \in S_n\}_a$. $\langle B \rangle \subseteq S_n$ és trivial, ja que $\forall \sigma \in B: \ \sigma \in S_n$.
Només ens cal demostrar que $S_n \subseteq \langle B \rangle$, per fer-ho:
OPCIO 1

$$S_n \subseteq \langle B \rangle \iff S_n = \langle \{(1,a) \in S_n\}_a \rangle = \langle A \rangle \subseteq \langle B \rangle$$

Llavors, només cal provar que $\langle A \rangle \subseteq \langle B \rangle$:

$$\begin{aligned} (1,a) &\stackrel{?}{=} [(1,2)(2,3)\cdots(a-2,a-1)](a-1,a)[(a-1,a-2)\cdots(3,2)(2,1)] \\ &= (1,2,3,\ldots,a-2,a-1)(a-1,a)(a-1,a-2,\ldots,3,2,1) \\ &= \sigma(a-1,a)\sigma^{-1} \\ &= (\sigma(a-1), \sigma(a)) \\ &= (1,a) \end{aligned}$$

OPCIO 2

$$S_n \subseteq \langle B \rangle \iff S_n = \langle \{(a,b) \in S_n\}_{a,b} \rangle \subseteq \langle B \rangle$$

Llavors, només cal provar que $\langle\{(a,b)\in S_n\}_{a,b}\rangle \subseteq \langle B\rangle$:

$$\begin{aligned}(a,b) &\stackrel{?}{=} [(a,a+1)(a+1,a+2)\cdots(b-2,b-1)](b-1,b)\\ &\qquad [(b-1,b-2)\cdots(a+2,a+1)(a+1,a)]\\ &= (a,a+1,a+2,\ldots,b-2,b-1)(b-1,b)\\ &\qquad (b-1,b-2,\ldots,a+2,a+1,a)\\ &= \tau(b-1,b)\tau^{-1}\\ &= (\tau(b-1),\tau(b))\\ &= (a,b)\end{aligned}$$

(c) $C = \{(1,2,\ldots,n),\ (1,2)\}$

Volem demostrar $S_n = \langle C\rangle$. $\langle C\rangle \subseteq S_n$ és trivial, ja que $\forall\sigma\in C$: $\sigma\in S_n$.
Només ens cal demostrar que $S_n\subseteq\langle C\rangle$, per fer-ho:
OPCIO 1

$$S_n\subseteq\langle C\rangle \iff S_n = \langle\{(a,a+1)\in S_n\}\rangle = \langle B\rangle \subseteq \langle C\rangle$$

Llavors, només cal provar que $\langle B\rangle\subseteq\langle C\rangle$:

$$\begin{aligned}(a,a+1) &\stackrel{?}{=} (1,2,\ldots,n)^{a-1}(1,2)(1,2,\ldots,n)^{n-a+1}\\ &= (1,2,\ldots,n)^{a-1}(1,2)(1,2,\ldots,n)^{-(a-1)}\\ &= \gamma^{a-1}(1,2)(\gamma^{a-1})^{-1}\\ &= (\gamma^{a-1}(1),\gamma^{a-1}(2))\\ &= (a,a+1)\end{aligned}$$

OPCIO 2

$$S_n\subseteq\langle C\rangle \iff S_n = \langle\{(1,a)\in S_n\}\rangle = \langle A\rangle \subseteq \langle C\rangle$$

Llavors, només cal provar que $\langle A\rangle\subseteq\langle C\rangle$:

$$\begin{aligned}(1,a) &\stackrel{?}{=} ((1,2)(1,2,\ldots,n))^{a-2}(1,2)((1,2)(1,2,\ldots,n))^{n-a+2}\\ &= (2,3,\ldots,n)^{a-2}(1,2)(2,3,\ldots,n)^{-(a-2)}\\ &= \sigma^{a-2}(1,2)\sigma^{-(a-2)}\\ &= (\sigma^{a-2}(1),\sigma^{a-2}(2))\\ &= (1,a)\end{aligned}$$

OPCIO 3

$$S_n\subseteq\langle C\rangle \iff S_n = \langle\{(a,b)\in S_n\}\rangle \subseteq \langle C\rangle$$

Llavors, només cal provar que $\langle\{(a,b)\in S_n\}\rangle \subseteq \langle C\rangle$:

$$\begin{aligned}(a,b) &\stackrel{?}{=} (1,2,\dots,n)^{a-1}(2,\dots,n)^{b-a-1}(1,2)(2,\dots,n)^{-(b-a-1)}(1,2,\dots,n)^{-(a-1)}\\ &= \tau^{a-1}\sigma^{b-a-1}(1,2)\sigma^{-(b-a-1)}\tau^{-(a-1)}\\ &= \tau^{a-1}(\sigma^{b-a-1}(1),\sigma^{b-a-1}(2))\tau^{-(a-1)}\\ &= \tau^{a-1}(1,b-a+1)\tau^{-(a-1)}\\ &= (\tau^{a-1}(1),\tau^{a-1}(b-a+1))\\ &= (a,b)\end{aligned}$$

22 Demostreu que, si G és un grup, el seu centre $Z(G) := \{g \in G :\ gh = hg,\ \text{per a tot } h \in G\}$ és un subgrup normal de G.

Primer, comprovem que $Z(G)$ és un subgrup de G.

$$\begin{aligned}&\forall g \in Z(G),\ h \in G :\ ((gh = hg \implies hg^{-1} = g^{-1}h) \implies g^{-1} \in Z(g))\\ &\forall x, y \in Z(G),\ h \in G :\ (xy^{-1}h = xhy^{-1} = hxy^{-1} \implies xy^{-1} \in Z(G))\end{aligned}$$

Per tant, $Z(G)$ és subgrup de G, i només cal comprovar que sigui normal:

$$\begin{aligned}Z(G) \text{ és subgrup normal} &\iff \forall h \in G :\ hZ(G) \stackrel{?}{=} Z(G)h\\ &\iff \forall h \in G :\ (hZ(G) \stackrel{?}{\subset} Z(G)h) \wedge (hZ(G) \stackrel{?}{\supset} Z(G)h)\end{aligned}$$

$\subset$ | $$\begin{aligned}x \in hZ(G) &\implies \exists z \in Z(G) :\ x = hz\\ &\implies x = zh \in Z(G)h\end{aligned}$$

$\supset$ | $$\begin{aligned}x \in Z(G)h &\implies \exists z \in Z(G) :\ x = zh\\ &\implies x = hz \in hZ(G)\end{aligned}$$

24 Demostreu que, si $n \geq 3$, el centre de S_n només conté la identitat.

OPCIO 1

Suposem $\exists \sigma \in Z(S_n) :\ ((\sigma \neq Id) \wedge (n \geq 3) \implies \forall \tau \in S_n :\ \tau\sigma = \sigma\tau)$:

$$\begin{aligned}n \geq 3 &\implies \exists a, b, c \in \mathbb{N}_n :\ (a \neq b) \wedge (a \neq c) \wedge (b \neq c) \wedge (\sigma(a) = b)\\ &\implies \exists \tau \in S_n :\ (\tau(b) = c) \wedge (\tau(a) = a)\\ &\implies (\tau\sigma)(a) = \tau(\sigma(a)) = \tau(b) = c\\ & (\sigma\tau)(a) = \sigma(\tau(a)) = \sigma(a) = b\\ &\implies \tau\sigma \neq \sigma\tau \implies \perp\\ &\implies \nexists \sigma \in Z(S_n) :\ (\sigma \neq Id) \wedge (n \geq 3)\end{aligned}$$

OPCIO 2

Suposem $\exists \sigma \in S_n :\ \sigma \neq Id$, i volem veure que $\exists \tau \in S_n :\ \sigma\tau = \tau\sigma$:

$$\sigma \neq Id \implies \exists \alpha, \beta \in S_n, (\alpha \neq \beta \wedge \alpha\sigma = \beta)$$

Llavors, definim $\tau, \gamma \in S_n$ amb $\gamma \neq \alpha$, $\gamma \neq \beta$, com:

$$\begin{cases} \alpha\tau = \alpha \\ \beta\tau = \gamma \end{cases}$$

Aleshores:

$$\left.\begin{aligned} \alpha(\sigma\tau) = (\alpha\sigma)\tau = \beta\tau = \gamma \\ \alpha(\tau\sigma) = (\alpha\tau)\sigma = \alpha\sigma = \beta \end{aligned}\right\} \implies \alpha(\sigma\tau) \neq \alpha(\tau\sigma) \implies \sigma\tau \neq \tau\sigma$$

OPCIO 3

Suposem $\exists \sigma \in S_n : \ (\sigma \neq Id) \wedge (\forall \tau \in S_n : \ \sigma\tau = \tau\sigma)$. Per demostrar que $\sigma \notin Z(S_n)$ només cal demostrar que $\exists \sigma' \in S_n$ tal que:

$$\sigma\tau = \tau\sigma \implies \sigma = \tau\sigma\tau^{-1}$$
$$\sigma' = \tau\sigma\tau^{-1} \neq \sigma \implies \sigma \notin Z(S_n)$$

Per l'exercici 16, sabem que