

Feuille 4 : Groupes, groupe Symétrique

Exercice 1. Montrer qu'il n'existe pas de morphisme de groupes non nul de $\mathbb{Z}/2\mathbb{Z}$ vers $\mathbb{Z}/3\mathbb{Z}$.

Exercice 2. Montrer qu'il existe un unique morphisme f de $\mathbb{Z}/10\mathbb{Z}$ vers $\mathbb{Z}/15\mathbb{Z}$ tel que $f(\bar{1}) = \bar{3}$. Déterminer $\text{Im } f$ et $\ker f$. f est-il injectif? surjectif?

Exercice 3. Soit $f : G \rightarrow H$ un morphisme entre deux groupes finis. Montrer que $\forall x \in G$, l'ordre de $f(x)$ divise l'ordre de x . En déduire que si l'ordre de x est premier avec le cardinal de H , alors $x \in \ker f$.

Exercice 4. Calculer le cardinal de $(\mathbb{Z}/30\mathbb{Z})^\times$. Quel est l'ordre multiplicatif de $\bar{11}$?

Exercice 5. On se place dans \mathcal{S}_6 . Soit $\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 3 & 6 & 2 \end{pmatrix}$ et $\tau := (1, 2, 3)(2, 5)$.

Calculer σ^{-1} , σ^2 , τ^2 et la signature de chacune de ces permutations.

Calculer de deux manières différentes $\sigma^{-1}\tau\sigma$.

Exercice 6. Écrire le cycle $(1, 2, \dots, n)$ de \mathcal{S}_n comme un produit de transpositions. Quelle est sa signature?

Exercice 7. On considère dans \mathcal{S}_{16} l'élément

$$S = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 13 & 11 & 16 & 12 & 4 & 14 & 3 & 8 & 1 & 9 & 7 & 5 & 10 & 6 & 15 & 2 \end{pmatrix}.$$

Donner le support, les orbites, la décomposition en cycles disjoints, l'ordre et la signature de S . Cette permutation appartient-elle à \mathcal{A}_{16} ?

Exercice 8.

Soit σ et τ les éléments du groupe symétrique \mathcal{S}_6

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

Déterminer l'ensemble des entiers n tels que $\sigma^n = \tau^n$.

Exercice 9. On se place dans le groupe symétrique \mathcal{S}_{11} et on considère les permutations :

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 2 & 4 & 1 & 6 & 5 & 8 & 9 & 7 & 10 & 3 \end{pmatrix} \text{ et } \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 6 & 4 & 11 & 9 & 7 & 8 & 10 & 5 & 2 & 1 \end{pmatrix}.$$

1. Ecrire π , σ et $\pi \circ \sigma$ comme produit de cycles à supports disjoints.
2. Déterminer l'ordre de π , de σ et de $\pi \circ \sigma$ dans \mathcal{S}_{11} .
3. Quel est l'ordre de \mathcal{S}_{11} ?
4. Existe-t-il dans le groupe \mathcal{S}_{11} un élément d'ordre 13 ou d'ordre 30?

Exercice 10. Soit σ l'élément de S_{11} suivant : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 8 & 11 & 3 & 1 & 2 & 9 & 6 & 4 & 10 & 7 \end{pmatrix}$.

1. Montrer que σ se décompose en produit de 3 cycles à supports disjoints $\sigma_2, \sigma_3, \sigma_5$ de longueur respective 2, 3 et 5. Donner l'ordre et la signature de σ .
2. Caractériser H , le sous-groupe de S_{11} engendré par $\sigma_2, \sigma_3, \sigma_5$. Est-il commutatif ?
3. On pose

$$\begin{array}{rccc} \varphi : & \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} & \longrightarrow & H \\ & (r, s, t) & \mapsto & \sigma_2^r \circ \sigma_3^s \circ \sigma_5^t \end{array}.$$

Montrer que φ est un homomorphisme de groupes surjectif. Caractériser $\ker \varphi$.

Quel est l'ordre de H ? Montrez que H est cyclique et donner un générateur.

Combien existe-t-il de générateurs distincts de H ?

Rappel de cours

Soient $(G, *)$ et (H, \circ) deux groupes.

Un morphisme de groupe f :

$(G, *) \rightarrow (H, \circ)$ est la donnée d'une application d'ensemble $f: G \rightarrow H$ vérifiant

$$\circ \quad f(e_G) = e_H$$

$$\circ \text{ pour tout } x, y \in G, f(x * y) = f(x) \circ f(y)$$

$$\circ \text{ pour tout } x \in G, f(x^{-1}) = f(x)^{-1}$$

Etant donné un morphisme de groupe f :

$(G, *) \rightarrow (H, \circ)$, son image est

$\text{Im}(f)$ est un sous-groupe de H . En effet, $\text{Im}(f)$ contient e_H (par le premier axiome), si y_1, y_2 sont dans $\text{Im}(f)$, alors $y_1 \circ y_2 \in \text{Im}(f)$ et $(y_1)^{-1} \in \text{Im}(f)$.

On définit aussi le noyau de f comme:

$$\text{Ker}(f) = \{x \in G \mid f(x) = e_H\}$$

On montre aussi que $\text{ker}(f) \subset G$ est un sous-groupe de morphisme de groupe $f: (G, *) \rightarrow (H, \circ)$ est

\circ injectif, si $f: G \rightarrow H$ est une application injective. C'est le cas si et seulement si $\text{ker}(f) = \{e_G\}$

o Surjectif, si $f : G \rightarrow H$ est une application surjective
 C'est le cas si et seulement si $\text{Im}(f) = H$

o Bijectif, si $f : G \rightarrow H$ est une bijection (c'est à dire
 à la fois injective et surjective). On dit dans ce cas
 que f est un isomorphisme de groupes

Ex 1

Dans cet exercice, pour un entier n , on note \bar{n}_2 pour
 sa classe d'équivalence dans $\mathbb{Z}/2\mathbb{Z}$ et \bar{n}_3 pour sa classe
 d'équivalence dans $\mathbb{Z}/3\mathbb{Z}$.

Soit $f : (\mathbb{Z}/2\mathbb{Z}, +) \longrightarrow (\mathbb{Z}/3\mathbb{Z}, +)$ un morphisme
 de groupe. Montrons qu'il est nul. (c'est à dire que
 $f(x) = \bar{0}_3$ pour tout $x \in \mathbb{Z}/2\mathbb{Z}$)

Comme f est un morphisme de ce groupe, l'envoyer
 l'élément neutre de $(\mathbb{Z}/2\mathbb{Z}, +)$ sur l'élément
 neutre de $(\mathbb{Z}/3\mathbb{Z}, +)$.

Autrement dit $f(\bar{0}_2) = \bar{0}_3$. Le groupe
 $(\mathbb{Z}/2\mathbb{Z}, +)$ n'a que deux éléments : $\bar{0}_1$ et $\bar{1}_2$, donc
 il reste à montrer que $f(\bar{1}_2) = \bar{0}_3$. Comme f est
 un morphisme de groupe on doit avoir

$$f(\bar{1}_2 + \bar{1}_2) = f(\bar{1}_2) + f(\bar{1}_2), \text{ mais le calcul}$$

dans $(\mathbb{Z}/2\mathbb{Z}, +)$ donne $\bar{1}_2 + \bar{1}_2 = \bar{2}_2 = \bar{0}_2$

On en déduit que

$$\bar{0}_3 = f(\bar{0}_2) = f(\bar{1}_2 + \bar{1}_2) = f(\bar{1}_2) + f(\bar{1}_2)$$

Ainsi, $f(\bar{1}_2)$ est un élément $y \in \mathbb{Z}/3\mathbb{Z}$, vérifiant
 $y + y = \bar{0}_3$

Or $(\mathbb{Z}/3\mathbb{Z}, +)$ n'a que 3 éléments : $\bar{0}_3, \bar{1}_3$ et $\bar{2}_3$
et On a $\bar{1}_3 + \bar{1}_3 = \bar{2}_3 \neq \bar{0}_3$
 $\bar{2}_3 + \bar{2}_3 = \bar{4}_3 = \bar{1}_3 \neq \bar{0}_3$

On en déduit que la seule valeur possible pour $f(\bar{1}_2)$ est $\bar{0}_3$, et donc que tout morphisme de groupe f :

$f: (\mathbb{Z}/2\mathbb{Z}, +) \rightarrow (\mathbb{Z}/3\mathbb{Z}, +)$ est nul
Autrement dit, qu'il n'existe pas de morphisme de groupe non-nul.

Ex 2

Dans cet exercice, pour un entier n , on notera \bar{n}_{10} pour sa classe d'équivalence dans $\mathbb{Z}/10\mathbb{Z}$ et
 \bar{n}_{15} pour sa classe d'équivalence dans $\mathbb{Z}/15\mathbb{Z}$

Montrons qu'il existe un unique morphisme de groupe
 $f: (\mathbb{Z}/10\mathbb{Z}, +) \rightarrow (\mathbb{Z}/15\mathbb{Z}, +)$ vérifiant
 $f(\bar{1}_{10}) = \bar{3}_{15}$

On commence par montrer l'unicité. Supposons qu'un tel morphisme de groupe existe, et notons le f .

Alors, par définition d'un morphisme de groupe, on doit avoir $f(\bar{0}_{10}) = \bar{0}_{15}$

De plus, pour tout $n \in \mathbb{N}^*$, $\bar{n}_{10} = n\bar{1}_{10} = \bar{1}_{10} + \dots + \bar{1}_{10}$ où l'addition fait apparaître n termes. Puisqu'on a supposé que f était un morphisme de groupe, on doit avoir, pour tout $n \in \mathbb{N}^*$

(1) $f(\bar{n}_{10}) = f(n\bar{1}_{10}) = nf(\bar{1}_{10}) = n\bar{3}_{15} = \bar{3}_{n_{15}}$

En raisonnant sur les inverses, on peut montrer que la formule (1) est aussi vérifiée pour $n \in \mathbb{Z}$

Ainsi on a une formule pour f , autrement dit, si un morphisme de groupe vérifiant $f(\overline{n}_{10}) = \overline{3}_{15}$ existe, il est unique et vérifie la formule (1)

Pour montrer qu'un morphisme de groupe existe, il suffit de montrer que $f: (\mathbb{Z}/10\mathbb{Z}, +) \rightarrow (\mathbb{Z}/15\mathbb{Z}, +)$ définie par la formule (1) est bien un morphisme de groupe. Montrons d'abord que f est bien définie

Soient n, k deux entiers tels que $\overline{n}_{10} = \overline{k}_{10}$. Dans ce cas, il existe $l \in \mathbb{Z}$ tel que $n = k + 10l$.

Et on a alors deux définitions possibles pour l'image par f de $\overline{n}_{10} = \overline{k}_{10}$. On a d'une part

$$f(\overline{k}_{10}) = \overline{3k}_{15}. \quad \text{Or, puisque } n = k + 10l, \text{ on a}$$

$$3n = 3k + 30l = 3k + 15(2l), \text{ et on en déduit que } \overline{3n}_{15} = \overline{3k}_{15}.$$

Finalement, on a :

$$\begin{aligned} f(\overline{n}_{10}) &= \overline{3n}_{15} = \overline{3k + 30l}_{15} \\ &= \overline{3k + 15(2l)}_{15} \\ &= \overline{3k}_{15} = f(\overline{k}_{10}) \end{aligned} \quad (2)$$

La fonction f est bien définie, deux entiers équivalents dans $\mathbb{Z}/10\mathbb{Z}$ sont bien envoyés par f sur deux entiers équivalents dans $\mathbb{Z}/15\mathbb{Z}$. On vérifie maintenant aisément que c'est un morphisme de groupe. Soient $\bar{n}_{10}, \bar{m}_{10}$ deux éléments de $\mathbb{Z}/10\mathbb{Z}$. on a

$$f(\bar{n}_{10} + \bar{m}_{10}) = f(\overline{n+m}_{10}) = \overline{3(n+m)}_{15} = \overline{3n}_{15} + \overline{3m}_{15} = f(\bar{n}_{10}) + f(\bar{m}_{10})$$

et, de même, étant donné $\bar{n}_{10} \in \mathbb{Z}/10\mathbb{Z}$, on a

$$f(-\bar{n}_{10}) = f(\overline{-n}_{10}) = \overline{3(-n)}_{15} = -\overline{3n}_{15} = -f(\bar{n}_{10})$$

Et on a $f(\bar{0}_{10}) = \bar{0}_{15}$. Finalement f est bien un morphisme de groupes

Remarque : par rapport à l'exercice précédent, ce qui a permis de montrer que f était bien définie (et donc qu'il existait un morphisme de groupe avec la condition $f(\bar{1}_{10}) = \bar{3}_{15}$) c'est le fait que l'équation (2) était vérifiée. Autrement dit, on a du vérifier qu'on avait une formule pour f qui ne dépendait pas du choix de représentant dans les classes d'équivalence. A l'inverse, si on essaie de définir un morphisme de groupe $f: (\mathbb{Z}/2\mathbb{Z}, +) \rightarrow (\mathbb{Z}/3\mathbb{Z}, +)$ vérifiant $f(\bar{1}_2) = \bar{1}_3$, les conditions sur un morphisme de groupe donnerait alors $f(\bar{2}_2) = \bar{2}_3$, mais aussi $f(\bar{0}_2) = \bar{0}_3$, or $\bar{0}_2 = \bar{2}_2$ et donc on devrait avoir $\bar{2}_3 = \bar{0}_3$, ce qui est faux ! Ceci montre qu'une telle application ne peut pas exister. (On le sait déjà d'après l'exercice 1).

On répond maintenant à la suite de la question. Calculons d'abord l'image de f . Soit $\bar{y}_{15} \in \mathbb{Z}/15\mathbb{Z}$ un élément. Par définition, $\bar{y}_{15} \in \text{Im}(f)$ si et seulement si, il existe $\bar{x}_{10} \in \mathbb{Z}/10\mathbb{Z}$ tel que $f(\bar{x}_{10}) = \bar{y}_{15}$. Avec la formule (1), on voit que cela revient à demander qu'il existe $n \in \mathbb{Z}$ tel que $\bar{y}_{15} = \overline{3n}_{15}$. Finalement, on en déduit que les éléments de $\text{Im}(f)$ sont exactement les multiples de 3 modulo 15, explicitement :

$$\text{Im}(f) = \{\bar{0}_{15}, \bar{3}_{15}, \bar{6}_{15}, \bar{9}_{15}, \bar{12}_{15}\} \subset \mathbb{Z}/15\mathbb{Z}$$

On note que l'image de f n'est pas $\mathbb{Z}/15\mathbb{Z}$ en entier (par exemple, en voyant que $\bar{1}_{15}$ n'est pas dans l'image) et on en déduit que le morphisme f n'est pas surjectif !

On calcule maintenant le noyau de f . Par définition c'est

$$\ker(f) = \{\bar{x}_{10} \in \mathbb{Z}/10\mathbb{Z} \mid f(\bar{x}_{10}) = \bar{0}_{15}\}$$

Soit $n \in \mathbb{Z}$, alors on a $f(\bar{n}_{10}) = \bar{0}_{15}$ si et seulement si $3n$ est congru à 0 modulo 15. L'équation $3n \equiv 0 \pmod{15}$ est équivalente à $n \equiv 0 \pmod{5}$, et on en déduit que le noyau de f est composé des multiples de 5 modulo 10. Explicitement, on a

$$\ker(f) = \{\bar{0}_{10}, \bar{5}_{10}\} \subset \mathbb{Z}/10\mathbb{Z}$$

En particulier, $\ker(f)$ contient un élément qui n'est pas le neutre (ici $\bar{5}_{10}$) donc le morphisme f n'est pas injectif.

20/03 12h36

Une permutation est une bijection

$$\sigma : \{1, \dots, n\} \longrightarrow \{1, \dots, n\}$$

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

Σ_n

$$e \in G$$

Ordre de x : le plus petit $n \geq 1$ tq

$$x^n = e_G$$

$$\langle x \rangle_G \subset G$$

$$\text{ord}(x) = \text{ord}(\langle x \rangle_G)$$

$$\text{ord}(G) = |G| = \text{nombre d'éléments dans } G$$

$H \subset G$ sous groupe

$\text{ord}(H) \mid \text{ord}(G)$: Théorème de Lagrange

$$\text{ord}(x) = \text{ord}(\langle x \rangle) \mid \text{ord}(G)$$

E_x 3 :

$$f: (G, *) \longrightarrow (H, \circ)$$
$$\underset{x}{\overset{e}{\xrightarrow{\quad}}} f(x) \quad \text{and } (f(x))$$

$$f(x * x) = f(x) \circ f(x)$$

$$f(e_G) = e_H$$

$$f(x^{-1}) = f(x)^{-1}$$

$$\text{Si } n = \text{ord}(x)$$

$$\text{On a } x^n = e_G$$

$$\text{donc } f(x^n) = f(e_G) = e_H$$

$$f(x + \dots + x) = f(x) \circ \dots \circ f(x)$$
$$= (f(x))^n$$

$$\text{donc } (f(x))^n = e_H$$

$$\text{Soit } k = \text{ord}(f(x))$$

$$k \leq n$$

$$n = qk + r \text{ avec } 0 \leq r \leq k$$

$$(f(x))^n = (f(x))^{qk+r}$$
$$= \underbrace{\left((f(x))^k \right)}_{e_H}^q \circ (f(x))^r$$

$$\text{dans } (f(x))^k = e_H$$

$$r < k$$

or k est le plus petit entier ≥ 1

$$\text{tq } (f(x))^k = e_H \text{ donc } x = 0$$

$$\text{dans } n = qk, \text{ donc ord}(H)$$

$$\text{en lecture } f(x) = e_H (\Leftrightarrow x \in \ker f)$$

On a noté que $\text{ord}(f(x)) \mid \text{ord}(x)$

On sait que $\text{ord}(f(x)) \mid \text{ord}(x)$

$$\text{dans } \text{ord}(f(x)) = 1$$

$$\text{dans } f(x) = e_H$$

Ex 4

$$(\mathbb{Z} / 30\mathbb{Z})$$

$$(\mathbb{Z} / 30\mathbb{Z})^* = \{\bar{n} \mid n \text{ premier avec } 30\}$$

$$\Phi(30) = \# \text{ éléments dans } (\mathbb{Z} / 30\mathbb{Z})^*$$

$$\circ \Phi(mn) = \phi(m) \phi(n) \text{ Vrai si } m \text{ et } n \text{ premiers entre eux}$$

$$\circ \Phi(p) = p - 1 \quad \text{Vrai si } p \text{ premier}$$

11

$$\text{On a } \mathbb{Z}/30\mathbb{Z}$$

$$= \mathbb{Z}(30)$$

$$= \mathbb{Z}(2 \times 3 \times 5)$$

$$= \mathbb{Z}(2) \mathbb{Z}(3) \mathbb{Z}(5)$$

$$\therefore 1 \times 2 \times 4 = 8 \text{ cl}$$

$$(\mathbb{Z}/30\mathbb{Z})^* = \{\overline{1}, \overline{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{29}\}$$

$$\text{On a } \overline{11}^2 = \overline{121} = \overline{1} \leftarrow \text{le neutre}$$

$$\text{ord}(\overline{11}) = 2$$

$$\begin{array}{c|ccccc|ccccc}
& \overline{13} & \overline{-11} & \overline{-7} & \overline{-1} \\
\hline
& \overline{13} & \overline{-11} & \overline{-7} & \overline{-1} \\
\end{array}$$

$$\mathbb{Z}/30\mathbb{Z}$$

$$\begin{array}{c|ccccc|ccccc}
& \overline{1} & \overline{7} & \overline{11} & \overline{13} & \overline{17} & \overline{19} & \overline{23} & \overline{29} \\
\hline
\end{array}$$

ordre

$$\begin{array}{c|ccccc|ccccc}
1 & 4 & 2 & 4 & 4 & 2 & 4 \\
\hline
\end{array}$$

$$\overline{7}^2 = \overline{49} = \overline{-11} \text{ donc } \overline{7}^4 = 1$$

$$(-\overline{7})^2 = \overline{-11} \text{ donc } (-\overline{7})^4 = 1$$

$$\overline{13}^2 = \overline{169} = \overline{-11} \text{ donc } \overline{13}^4 = 1$$

1, 7, 11 et 13 sont premiers avec 30
 donc inversible pour la multiplication
 donc -1, -7, -11 et -13 aussi

$\pi / 30\pi$	1	7	11	13	17	19	23	29
ordre	1	4	2	4	4	2	4	2

car cardinal 8 ne divise pas 3 donc
on travaille avec puissance 2

22/03 8:54

Ex 5

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

Calculer σ^{-1} , σ^2 , τ^2

$$\sigma^{-1} \left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 3 & 1 & 5 \end{array} \right)$$



$$\sigma^2, \quad \sigma = \left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 4 & 3 & 6 & 2 \end{array} \right)$$

$$\sigma = \left(\begin{array}{cccccc} 5 & 1 & 4 & 3 & 6 & 2 \\ 6 & 5 & 3 & 4 & 2 & 1 \end{array} \right)$$

$$\sigma^2 = \left(\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 4 & 2 & 1 \end{array} \right)$$

$$C = \underbrace{(1, 2, 3)}_{\downarrow} \underbrace{(2, 5)}_{\rightarrow}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 5 & 6 \end{pmatrix} \quad \begin{matrix} \\ \\ \parallel \\ Z_2 \end{matrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 4 & 2 & 6 \end{pmatrix} \quad \begin{matrix} \\ \\ \parallel \\ Z_1 \end{matrix}$$

$$G = Z_2 \cdot Z_1$$

$$Z_1 \quad \text{---} \quad \text{---}$$

$$Z_2 \quad \text{---} \quad \text{---}$$

$$G^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 1 & 4 & 3 & 6 \\ 2 & 5 & 1 & 4 & 3 & 6 \\ 5 & 3 & 2 & 4 & 1 & 6 \end{pmatrix}$$

$$G^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 3 & 2 & 4 & 6 \end{pmatrix}$$

$$Z(6) = (-1)^5 \quad \begin{matrix} 5 \\ -1 \end{matrix}$$

$$S = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 1 & 4 & 3 & 6 \\ 5 & 3 & 2 & 4 & 1 & 6 \end{smallmatrix} \right) \quad q(6) = 7$$

$$(1, 2, 3)(2, 5)$$

$$\begin{array}{ccccc} 2 & \longleftarrow & 1 & \longleftarrow & 1 \\ & & & & \\ 5 & \longleftarrow & 5 & \longleftarrow & 2 \\ & & & & \\ 1 & \longleftarrow & 3 & \longleftarrow & 3 \end{array}$$

Def : Signature de σ = # inversions dans σ
une inversion est $i < j$

tq $\sigma(i) > \sigma(j)$

pour σ^{-1} : σ^{-1} a 8 inversions

$$2 > 1$$

$$6 > 4$$

$$6 > 3$$

$$6 > 1$$

$$6 > 5$$

$$4 > 3$$

$$4 > 1$$

$$3 > 1$$

dans

$$\varepsilon(\sigma) = (-1)^8 = 1$$

$$\sigma^{-1} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 3 & 1 & 5 \end{pmatrix}$$

Signature de $(2, 4)$:

$$\varepsilon: \Sigma_n \rightarrow \mathbb{Z}/2\mathbb{Z}$$

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

$$\sigma(1) = 5$$

$$\sigma(5) = 6$$

$$\sigma(6) = 2$$

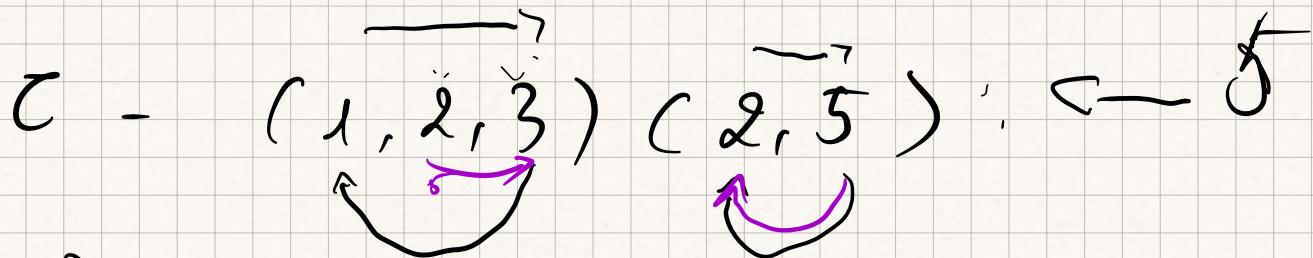
$$\sigma(2) = 1$$

$$\sigma(3) = 4$$

$$\sigma(4) = 3$$

$$\sigma = (5 \ 6 \ 1) (3 \ 4)$$

$$= \underbrace{(3 \ 4)}_{\text{order 2}} \underbrace{(5 \ 6 \ 2 \ 1)}_{\text{order 4}}$$



$$\tau(1) = 2$$

$$\tau(2) = 5$$

$$\tau(3) = 1$$

$$\tau(4) = 4$$

$$\tau(5) = 3 \quad (5 \rightarrow 2 \rightarrow 3)$$

$$\tau(6) = 5$$

$$\tau = (1 \ 2 \ 3)(2 \ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 1 & 4 & 3 & 6 \end{pmatrix}$$

$$= (1 \ 2 \ 5 \ 3)$$

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

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

$$\sigma^{-1} \tau \sigma =$$

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

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

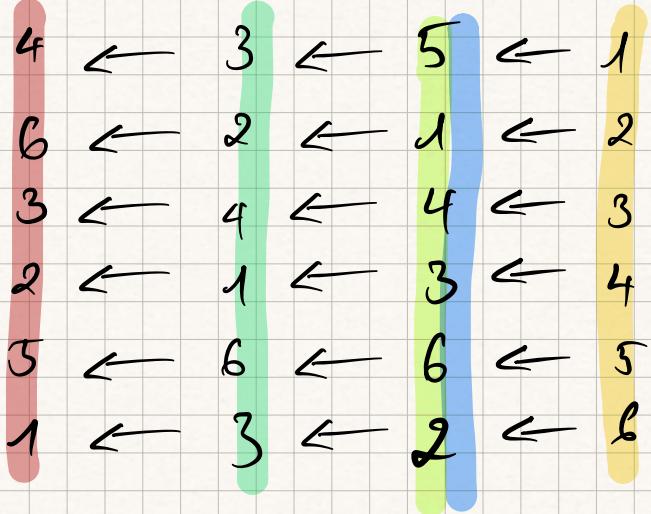
$$\sigma^{-1} = \begin{pmatrix} 3 & 2 & 4 & 1 & 6 & 5 \\ 4 & 6 & 3 & 2 & 5 & 1 \end{pmatrix}$$

$$\sigma^{-1} \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 3 & 2 & 5 & 1 \end{pmatrix}$$

$$= (1\ 4\ 2\ 6)$$

1' >

$$\sigma^{-1} \circ \sigma$$



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

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

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

$$\rightarrow (1\ 4\ 2\ 6)$$

$$\sigma^{-1} \circ (\sigma^{-1})^{-1} = \sigma^{-1} \circ \sigma$$

$$\sigma^{-1} (1\ 2\ 5\ 3) \sigma$$

$$= (\sigma^{-1}(1), \sigma^{-1}(2), \sigma^{-1}(5), \sigma^{-1}(3))$$

$$= (1\ 4\ 2\ 6)$$

Ex 6

$$\sigma = (1 \ 2 \ 3 \ 4 \ 5 \ \dots)$$

$$(1 \ 2)$$

$$(1 \ 2 \ 3)$$

$$(1 \ 2 \ 3 \ 4)$$

$$\delta = (1\ 2)(2\ 3) \dots (n-1 \ n)$$

$$\epsilon((1\ 2 \dots n)) = (-1)^{n-1}$$

$$(1, 2, \dots, n) = (??)(??) \dots (??)$$

$$(1, 2) = (1, 2)$$

$$(1, 2, 3) = (1, 2) \cdot (2, 3) \quad \checkmark$$

=

$$3 \rightarrow 1$$

$$2 \rightarrow 3$$

$$1 \rightarrow 2$$

ou

$$\times (1, 2) \cdot (3, 1) = \begin{matrix} 3 & \rightarrow & 2 \\ 1 & \rightarrow & 3 \\ 2 & \rightarrow & 1 \end{matrix}$$

$$\checkmark (3,1) \circ (1,2) = \begin{matrix} 1 & \rightarrow 2 \\ 2 & \rightarrow 3 \\ 3 & \rightarrow 1 \end{matrix}$$

$$x (2,3) \circ (1,2) = \begin{matrix} 1 & \rightarrow 3 \\ 2 & \rightarrow 1 \\ 3 & \rightarrow 2 \end{matrix}$$

$$(1, 2, 3, 4) = (1,2) \circ (2,3) \circ (3,4)$$

$$= 4 \rightarrow 1$$

$$3 \rightarrow 4$$

$$2 \rightarrow 3$$

$$1 \rightarrow 2$$

$$= (1, 2, 3, 4)$$

Formule 1: $(1, 2, 3, \dots, n)$

$$C_n = (1, 2)(2, 3), \dots, (n-1, n)$$

Par récurrence :

Initialisation $n = 2$

$$(1, 2) = (1, 2) \checkmark$$

Soit $n \geq 2$ tq $(1, \dots, n) = (1, 2) \dots (n-1, n)$

$$(1, \dots, n+1) (n, n+1)$$

$i+1 \leftarrow i \quad i \leftarrow i$

$$1 \leftarrow n+1 \leftarrow n$$

$$n+1 \leftarrow n \leftarrow n+1$$

$$\begin{cases} i \rightarrow i+1 & i \in \{1, \dots, n-1\} \\ 1 \rightarrow 2 \\ 2 \rightarrow 3 \\ \vdots \\ n \rightarrow n+1 \end{cases}$$

$$n+1 \rightarrow n+1 \quad (1, 2, 3, \dots, n)$$

$$C_{n+1}(n, n+1) = C_n$$

$$C_{n+1} = \underbrace{C_n}_{C_n} (n, n+1) (n, n+1) = C_n (C_n, n+1)$$

$$= \text{Id} = (1, 2)(2, 3) \dots$$

$$(n-1, n)(n, n+1)$$

Ainsi de manière $C_{n+1} = C_n (n, n+1)$

$$C_{n+1}(n, n+1) = C_n(n, n+1)^2$$

$$C_{n+1}(n, n+1) = C_n$$

Formule 2 :

$$(1, 2, \dots, n) = (1, n) \circ (1, n-1) \circ (1, n-2) \circ \dots \circ (1, 2)$$

$$\begin{matrix} 1 & & n \\ n & & n-1 \end{matrix} \quad \text{Formule 1}$$

$$\begin{matrix} n-1 & & n-2 \\ n-2 & & n-3 \end{matrix} \quad \text{Formule 1}$$

$$\begin{matrix} n-2 & & n-1 \\ n-3 & & n-4 \end{matrix} \quad \text{Formule 1}$$

Preuve par récurrence :

Initialisation $n=2$ $(1,2) = (1,2)\nu$

Récurrence : On suppose $(1, \dots, n) = (1, n) \circ (1, n-1) \circ \dots \circ (1, 2)$

On calcule : $(1, n+1) \circ (1, \dots, n+1)$

$$= \begin{cases} i \in \{2, \dots, n-1\} \rightarrow i+1 \\ 1 \mapsto 2 \\ n \mapsto 1 \\ n+1 \mapsto n+1 \end{cases} = (1, \dots, n)$$

donc $(1, n+1)C_{n+1} = C_n$

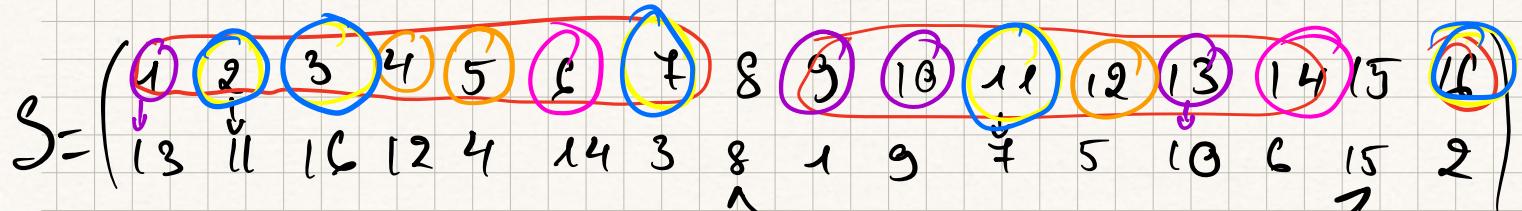
$$\Rightarrow C_{n+1} = (1, n+1)(1, n) \circ \dots \circ (1, 2)$$

□ → fini

Formule 3: $(1, \dots, n) = (n, 1)(n, 2) \dots (n, n-1)$

$$C_{n,i} = (n-1, \dots, n)$$

Ex :



$$\underline{\text{Support}}(S) = \{1, \dots, 16\} \setminus \{8, 15\}$$

Orbites $\{8\}, \{15\}, \{1, 13, 10, 9\}$

$\{2, 11, 7, 3, 16\}, \{4, 12, 5\}, \{6, 14\}$

Cycles : $\{1, 13, 10, 9\}$ $\{2, 11, 7, 3, 16\}$ $\{4, 12, 5\}$ $\{6, 14\}$

Def $x \subset \{1, \dots, n\}$ est une orbite de $\tau \in \Sigma_n$

Si : - $x \neq \emptyset$

- $\tau(x) = x$

- $\forall Y \subset X, Y \neq \emptyset, x$ alors $\tau(Y) = Y$

Contre exemple

$$x = \{1, 9, 10\} \quad S(x) = \{13, 1, 9\}$$
$$x \notin S(x)$$

$$x' = \{1, 13, 9, 10, 8\}$$
$$S(x') = \{1, 13, 9, 10, 8\} \quad S(x') = x'$$

Mais $\{8\} \subset x'$ et $S(\{8\}) = \{8\}$

$\tau \in \Sigma_n$

Ordre(τ) = le plus petit $k \geq 1$ tq $\tau^k = \text{Id}$

ordre((1, ..., m)) = m

$n \rightarrow m$

ordre($\tau \circ \tau$) = le plus petit k tq $(\tau \circ \tau)^k = \text{Id}$

$$\begin{matrix} * \\ \tau^k \circ \tau^k \end{matrix}$$

Ordre de $\tau \circ \tau$

= ppcm(ordre(τ), ordre(τ))

Si τ et τ constant,

Ordre(τ)

= ppcm(4, 5, 3, 2)

= ppcm(4, 5, 3) = 60

Cycles: $\{1, 3, 10, 8\}$ $\{2, 11, 4, 3, 16\}$ $\{9, 12, 5\}$ $\{6, 14\}$

σ_4

σ_5

σ_3

σ_2

$$S = \sigma_2 \sigma_3 \sigma_4 \sigma_5$$

$$\#_n > 1$$

$$S^n = \sigma_2^n \sigma_3^n \sigma_4^n \sigma_5^n \quad (\text{can } \sigma_i \sigma_j \text{ cancel} \ i, j \in \{2, 3, 4, 5\})$$

$$S^n = \text{Id}$$

$$\Leftrightarrow \sigma_2^n = \text{Id}, \sigma_3^n = \text{Id}, \sigma_4^n = \text{Id} \text{ and } \sigma_5^n = \text{Id}$$

$$\Leftrightarrow n \equiv 0 \pmod{2}, \quad n \equiv 0 \pmod{3}, \quad n \equiv 0 \pmod{4}$$

$$n \equiv 0 \pmod{5}$$

$$\Leftrightarrow n \equiv 0 \pmod{\text{lcm}(2, 3, 4, 5)}$$

$$\Leftrightarrow n \equiv 0 \pmod{60}$$

$$\varepsilon(\sigma_2) = -1$$

$$\varepsilon(\sigma_3) = (-1)^{3-1} = 1$$

$$\varepsilon(\sigma_4) = -1$$

$$\varepsilon(\sigma_5) = 1$$

$$\text{Danc } \varepsilon(S) = 1$$

29/03 8:36

Ex 10

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 8 & 11 & 3 & 1 & 2 & 9 & 6 & 4 & 10 & 7 \end{pmatrix}$$

$$E(\tau_2) = 1 \quad E(\tau_3) = 1$$

$$E(\tau_5) = 1$$

$$\tau = (\begin{matrix} 1 & 5 \\ \uparrow & \\ \tau_2 & \end{matrix}) (\begin{matrix} 2 & 8 & 6 \\ \uparrow & \\ \tau_3 & \end{matrix}) (\begin{matrix} 3 & 11 & 7 & 9 & 4 \\ \uparrow & \\ \tau_5 & \end{matrix}) \setminus \{10\}$$

$$H = \langle \tau_2, \tau_3, \tau_5 \rangle \cong_{11} S_{11}$$

$H = ?$ (Sous-groupe engendré par τ_2, τ_3, τ_5)

Def : G un groupe

$$g_1, g_2, g_3 \in G \quad \xrightarrow[\text{sous groupe}]{} \quad$$

$$H = \langle g_1, g_2, g_3 \rangle \subset G$$

H est

- (1) - un sous-groupe de G
- (2) - H contient g_1, g_2 et g_3
- H est le plus petit sous-groupe qui vérifie (1) et (2)

$$H = \bigcap_{k \in G} K$$

sous-groupe, $g_1, g_2, g_3 \in K$

$$\text{Ord } (\tau) = \text{ppcm}(2, 3, 5)$$

$$\cong(G) = 30$$

$$\cong(G) = -1 \quad (-1 \times 1 \times 1)$$

2) Si $\sigma \in H$

$\exists (i_1, \dots, i_{11}), (n_{i_1}, \dots, n_{i_k})$
suite dans $\{2, 3, 5\}$ suite dans \mathbb{Z}

$h \in H$

$$\Leftrightarrow h = g_{i_1}^{n_{i_1}} \cdot g_{i_2}^{n_{i_2}} \cdots g_{i_k}^{n_{i_k}}$$

Où $g_{i_n} = g_1$ ou g_2 ou g_3

$$n_{i_n} \in \mathbb{Z}^*$$

Par exemple :

$$h = g_1^3 g_2^{-2} g_3^{-1} g_4^4 \in H$$

on peut avoir plus de termes

tel que :

$$\tau = \tau_{i_1}^{n_{i_1}} \circ \cdots \circ \tau_{i_k}^{n_{i_k}}$$

Mq $\exists m_2, m_3, m_5 \in \mathbb{Z}$ tq

$$\tau = \tau_2^{m_2} \tau_3^{m_3} \tau_5^{m_5}$$

$$\text{Si } i_j = 2$$

$$\tau_{i_1}^{n_{i_1}} \circ \cdots \circ \tau_2^{n_j} \circ \cdots \circ \tau_{i_k}^{n_{i_k}}$$

τ_2 commute avec τ_3 et τ_5

(car ce sont des cycles à support disjoints). Et τ_2 commute avec τ_2 donc τ_2 commute avec τ_3^n et τ_5^n + n

$$\tau_3^n \tau_2 = \tau_3^{n-1} \tau_3 \tau_2$$

$$= \tau_3^{n-1} \tau_2 \tau_3$$

$$= \tau_2 \tau_3^{n-1} \tau_3$$

$$= \tau_2 \tau_3^n$$

de même $\tau_2^{n_j}$ commute avec τ_3^n et τ_5^n

$$\text{dans } \bar{\tau} = \tau_2^{n_j} \circ \tau_1^{n_1} \circ \cdots \circ \widehat{\tau}_{i_j}^{n_{i_j}} \circ \cdots \circ \tau_{i_k}^{n_{i_k}}$$

On fait ça pour tous les $j, k, i = 2$

$$\tau = \tau_2^{(n_{j_1} + \cdots + n_{j_l})} \circ \tau_{i_1}^{n_{i_1}} \circ \cdots \circ \widehat{\tau}_{i_{j_1}}^{n_{i_{j_1}}} \circ \cdots \circ \widehat{\tau}_{i_k}^{n_{i_k}}$$

$$\text{On peut réécrire } \bar{\tau} = \tau_2^{m_2} \circ \tau_{i_1}^{m_{i_1}} \circ \cdots \circ \widehat{\tau}_{i_{j_1}}^{m_{i_{j_1}}} \circ \cdots \circ \widehat{\tau}_{i_k}^{m_{i_k}}$$

On fait pareil pour les termes sur \mathbb{J}_5 (on les passe à droite) Possible car \mathbb{J}_3 et \mathbb{J}_5 s'annulent entre eux

$$\begin{aligned}\tau &= \mathbb{J}_2^{m_2} \circ \dots \circ \mathbb{J}_5^{m_5} \\ &= \mathbb{J}_2^{m_2} \mathbb{J}_3^{m_3} \mathbb{J}_5^{m_5}\end{aligned}$$

2x On a montré que $\tau \in H$

$$\Leftrightarrow \exists (m_2, m_3, m_5) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \text{ t.q.}$$

$$\tau = \mathbb{J}_2^{m_2} \mathbb{J}_3^{m_3} \mathbb{J}_5^{m_5}$$

ordre $(\mathbb{J}_2) = 2$

$$\Rightarrow \text{Si } m_2 \equiv m'_2 \pmod{2} \quad \mathbb{J}_2^{m_2} = \mathbb{J}_2^{m'_2} \quad (\text{car } \exists k, m_2 = 2k + m'_2)$$

$$\text{et donc } \mathbb{J}_2^{m_2} = \mathbb{J}_2^{m'_2+k} = \mathbb{J}_2^{m'_2} \cdot \mathbb{J}_2^{2k} = \mathbb{J}_2^{m'_2} \circ (\mathbb{J}_2^2)^k = \mathbb{J}_2^{m'_2}$$

ordre $(\mathbb{J}_3) = 3$

$$\Rightarrow \text{Si } m_3 \equiv m'_3 \pmod{3} \quad \mathbb{J}_3^{m_3} = \mathbb{J}_3^{m'_3}$$

ordre $(\mathbb{J}_5) = 5$

$$\Rightarrow \text{Si } m_5 \equiv m'_5 \pmod{} \quad \mathbb{J}_5^{m_5} = \mathbb{J}_5^{m'_5}$$

Les éléments de H sont donnés par la liste

$$\mathbb{J}_2^{m_2} \mathbb{J}_3^{m_3} \mathbb{J}_5^{m_5}$$

$$0 \leq m_2 \leq 1, \quad 0 \leq m_3 \leq 2, \quad 0 \leq m_5 \leq 4$$

H commutatif ? oui

- Si $x, y \in H$ $x \cdot y = ?$ $y \cdot x$

Soient $x, y \in H$

$\exists (m_2, m_3, m_5) \cdot (m'_2, m'_3, m'_5)$

$$x = \sigma_2^{m_2} \cdot \sigma_3^{m_3} \cdot \sigma_5^{m_5}$$

$$y = \sigma_2^{m'_2} \cdot \sigma_3^{m'_3} \cdot \sigma_5^{m'_5}$$

$$\begin{aligned} x \cdot y &= \sigma_2^{m_2} \cdot \sigma_3^{m_3} \cdot \sigma_5^{m_5} \cdot \sigma_2^{m'_2} \cdot \sigma_3^{m'_3} \cdot \sigma_5^{m'_5} \\ &= \sigma_2^{m_2 + m'_2} \cdot \sigma_3^{m_3 + m'_3} \cdot \sigma_5^{m_5 + m'_5} \\ &\stackrel{\text{def}}{=} y \cdot x \end{aligned}$$

3y

$$\varphi = \mathbb{Z} + \mathbb{Z} + \mathbb{Z} \rightarrow H$$
$$(r, s, t) \mapsto \sigma_2^r \cdot \sigma_3^s \cdot \sigma_5^t$$

Mq φ isomorphisme

$$\text{Mq } \varphi(0, 0, 0) = \text{Id}$$

$$\therefore \#(r, s, t) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$$

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

$$\therefore \#(r, s, t), (r', s', t') \in \mathbb{Z}^3$$

$$\varphi((r, s, t) + (r', s', t')) = \varphi(r, s, t) \cdot \varphi(r', s', t')$$

$$\begin{aligned} \varphi((r, s, t) + (r', s', t')) &= \varphi(r + r', s + s', t + t') \\ &= \sigma_2^{r+s} \cdot \sigma_3^{s+s'} \cdot \sigma_5^{t+t'} \end{aligned}$$

$$\begin{aligned}
 &= \mathcal{T}_2^r \cdot \mathcal{T}_3^s \cdot \mathcal{T}^t \cdot \mathcal{T}_2^{r'} \cdot \mathcal{T}_3^{s'} \cdot \mathcal{T}_5^{t'} \\
 &= \varphi(r, s, t) \cdot \varphi(r', s', t')
 \end{aligned}$$

Suspectif : fait élément de H s'écrit

$$\mathcal{T}_2^{m_2} \mathcal{T}_3^{m_3} \mathcal{T}_5^{m_5}$$

$$\ker \varphi = \{ (r, s, t) \mid \varphi(r, s, t) = \text{Id} \}$$

$$= \{ (r, s, t) \mid r \equiv 0 \pmod{2}$$

$$s \equiv 0 \pmod{3}$$

$$t \equiv 0 \pmod{5}$$

$$= 2\mathbb{Z} \times 3\mathbb{Z} \times 5\mathbb{Z}$$

$$\frac{\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}}{2\mathbb{Z} \times 3\mathbb{Z} \times 5\mathbb{Z}} = \underbrace{\frac{\mathbb{Z}}{2\mathbb{Z}}}_{\text{1 générateur}} \times \underbrace{\frac{\mathbb{Z}}{3\mathbb{Z}}}_{\text{2 gen}} \times \underbrace{\frac{\mathbb{Z}}{5\mathbb{Z}}}_{\text{4 gen}} \xrightarrow{\cong} H$$

$G \xrightarrow{\varphi} H$ morphisme de groupe

$$\frac{G}{\ker \varphi} \xrightarrow{\text{iso}} \text{Image } \varphi$$

$$\text{ordre } (\varphi) = 30$$

Mq H est cyclique, $\mathcal{T} \in H$ ordre $(\mathcal{T}) = 30$
dans $\langle \mathcal{T} \rangle = H$

$$\mathcal{T} = \mathcal{T}_2 \cdot \mathcal{T}_3 \cdot \mathcal{T}_5 \in t$$

Theoreme reste divisibles

$$\frac{2}{2\pi} \times \frac{2}{3\pi} \times \frac{2}{5\pi} \simeq \frac{\pi}{30\pi}$$