01/04/2021 Maths 4 TD 4

Exercice 4

1) $(\mathbb{Z}/30\mathbb{Z})^* = \{\bar{1}, \bar{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{29}\}$ ⟸ les éléments premiers avec 30

donc $\boxed{\text{card} = 8}$

2) ord$(\overline{11})$ dans $(\mathbb{Z}/30\mathbb{Z})^*$

ord $(\overline{11}) = \{2, 4, 8\}$ (diviseurs de 8)

$\overline{11}^2 = \overline{121} = \bar{1}$ car $121 \equiv 1 [30]$

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

Exercice 1

Mq il n'existe pas de morphisme de groupe de $\mathbb{Z}/2\mathbb{Z}$ vers $\mathbb{Z}/3\mathbb{Z}$ non nul.

Soit $\varphi : (\mathbb{Z}/2\mathbb{Z}, +) \to (\mathbb{Z}/3\mathbb{Z}, +)$
$\bar{0} \mapsto \bar{0}$

Rappel : $\varphi : (\mathbb{Z}/2\mathbb{Z}, +) \to (\mathbb{Z}/3\mathbb{Z}, +)$ morph de groupe si $\varphi(x+y) = \varphi(x) + \varphi(y)$ $\forall (x,y) \in (\mathbb{Z}/2\mathbb{Z})^2$

en particulier $\varphi(e) = e$
$(\varphi(\bar{0}) = \bar{0})$

φ est entièrement déterminé par $\varphi(\bar{1})$

- Supposons $\varphi(\bar{1}) = \bar{1}$ (par l'absurde)

$$\varphi(\bar{1}+\bar{1}) = \varphi(\bar{1}) + \varphi(\bar{1})$$

$$\varphi(\bar{1}+\bar{1}) = \varphi(\bar{0}) = \bar{0} \neq \bar{2} = \bar{1} + \bar{1} = \varphi(\bar{1}) + \varphi(\bar{1})$$

CONTRADICTION

- Supposons $\varphi(\bar{1}) = \bar{2}$

$\bar{0} = \varphi(\bar{0}) = \varphi(\bar{1}+\bar{1}) = \varphi(\bar{1}) + \varphi(\bar{1}) = \bar{2} + \bar{2} = \bar{4} = \bar{1}$ CONTRADICTION

⇒ Donc $\varphi(\bar{1})$ ne peut valoir que $\bar{0}$.

et le seul morphisme de groupe de $\mathbb{Z}/2\mathbb{Z}$ vers $\mathbb{Z}/3\mathbb{Z}$ est

$$(\mathbb{Z}/2\mathbb{Z}, +) \to (\mathbb{Z}/3\mathbb{Z}, +)$$
$$\bar{0} \mapsto \bar{0}$$
$$\bar{1} \mapsto \bar{0}$$

Remarque : $\varphi : G \to H$ G, H des groupes
φ un morphisme de groupe

Si G cyclique ($G = \langle x \rangle$, $x \in G$) alors φ est entièrement déterminé par $\varphi(x)$

car Si $y \in G$, $\exists k \in \mathbb{N} \mid y = x^k$ (G cyclique)

Donc $\varphi(y) = \varphi(x^k) = \varphi(x)^k$

Exercice 2

1) Mq $\exists !$ morphisme f de $\mathbb{Z}/10\mathbb{Z}$ vers $\mathbb{Z}/15\mathbb{Z}$ tq $f(\bar{1}) = \bar{3}$

D'après la remarque précédente, $f : (\mathbb{Z}/10\mathbb{Z}, +) \to (\mathbb{Z}/15\mathbb{Z}, +)$ est un morphisme de groupe

donc f est entièrement déterminé par l'image de $\bar{1}$.

car $\mathbb{Z}/10\mathbb{Z} = \langle \bar{1} \rangle$

donc $k \in \mathbb{Z}/10\mathbb{Z}$, $f(\bar{k}) = f(\overbrace{\bar{1}+\bar{1}+\dots+\bar{1}}^{k \text{ fois}})$

$= \underbrace{f(\bar{1}) + \dots + f(\bar{1})}_{k \text{ fois}}$

$\Rightarrow$ Si f existe, il est unique

$\Rightarrow$ La q° qui reste est de savoir si

$\mathbb{Z}/10\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z}$

$\bar{1} \mapsto \bar{3}$

est un morphisme de groupe ?

- $f(\bar{0}) = f(\overline{10}) = f(\underbrace{\bar{1}+\dots+\bar{1}}_{10 \text{ fois}}) = \underbrace{f(\bar{1}) + \dots + f(\bar{1})}_{10 \text{ fois}} = \underbrace{\bar{3} + \dots + \bar{3}}_{10 \text{ fois}} = \overline{30} = \bar{0}$

  donc f envoie bien $\bar{0}$ sur $\bar{0}$.

- on a $f(\bar{0}) = \bar{0}$ $\quad f(\bar{2}) = \bar{6}$ $\quad f(\bar{4}) = \overline{12}$ $\quad f(\bar{6}) = \overline{18} = \bar{3}$ $\quad f(\bar{8}) = \overline{24} = \bar{9}$

  $f(\bar{1}) = \bar{3}$ $\quad f(\bar{3}) = \bar{9}$ $\quad f(\bar{5}) = \overline{15} = \bar{0}$ $\quad f(\bar{7}) = \overline{21} = \bar{6}$ $\quad f(\bar{9}) = \overline{27} = \overline{12}$

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

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

4) Est ce que f est injectif ? NON $\to \mathrm{Ker}(f) \neq \{e\}$

——————— surjectif ? NON $\quad \bar{2} \notin \mathrm{Im}(f)$

Exercice 3

$f : G \to H$ un morphisme de groupe, G et H finis

Mq $\forall x \in G$, $\mathrm{ord}(f(x))$ divise $\mathrm{ord}(x)$

On veut montrer que $f(x)^{\mathrm{ord}(x)} = e_H$

$f(x)^{\mathrm{ord}(x)} = f(x^{\mathrm{ord}(x)})$ car f morphisme de groupe.

$= f(e_G) = e_H$ car f morphisme de groupe

$\Rightarrow$ on a bien $\mathrm{ord}(f(x))$ divise $\mathrm{ord}(x)$.

08.04.2021

Exercice 7

cycles disjoints : $\overset{s_1}{(1\ 13\ 10\ 9)}\overset{s_2}{(2\ 11\ 7\ 3\ 16)}\overset{s_3}{(4\ 12\ 5)}\overset{s_4}{(6\ 14)}$

orbites : $\{1\ 13\ 10\ 9\}, \{2\ 11\ 7\ 3\ 16\}, \{4\ 12\ 5\}, \{6, 14\}, \{8\}, \{15\}$

support : $[\![1, 16]\!] \setminus \{8, 15\}$

ordre : $ord(s_1) = 4 \quad ord(s_2) = 5 \quad ord(s_3) = 3 \quad ord(s_4) = 2$

Donc $ord(s) = ppcm(ord(s_1), ord(s_2), ord(s_3), ord(s_4)) = 60$

signature : $\varepsilon(s_1) = (-1)^{4-1} = -1$ $\qquad \varepsilon(s) = +1 = (-1)^2$ ← nb de cycles disjoints pairs

$\varepsilon(s_2) = (-1)^{5-1} = +1$

$\varepsilon(s_3) = (-1)^{3-1} = +1$

$\varepsilon(s_4) = (-1)^{2-1} = -1$

Donc $s \in A_{16}$ car $\varepsilon(s) = +1$

$A_{16} = \{\sigma \in S_{16}$ tq $\varepsilon(\sigma) = +1\}$

Exercice 8

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

On cherche $\{n \in \mathbb{Z}$ tq $\sigma^n = \tau^n\}$

$\sigma^n = \tau^n \Rightarrow \{$orbites de $\sigma^n\} = \{$orbites de $\tau^n\}$

$\Rightarrow$ support de σ^n = support de τ^n

$\sigma = (1\ 4\ 3)(2\ 6\ 5) \qquad \tau = (1\ 3)(4\ 6)$

$\sigma^2 = (1\ 3\ 4)(2\ 5\ 6) \qquad \tau^2 = e$

$\sigma^3 = e$

$\tau^n = \begin{cases} e & \text{si } n \text{ pair} \\ \tau & \text{si } n \text{ impair} \end{cases}$ $\qquad$ Donc $\sigma^n = \tau^n \Rightarrow \sigma^n = \tau^n = e$ car $\tau \neq \sigma$ et $\tau \neq \sigma^2$

$\sigma^n = \begin{cases} e & \text{si } n \equiv 0\ [3] \\ \sigma & \text{si } n \equiv 1\ [3] \\ \sigma^2 & \text{si } n \equiv 2\ [3] \end{cases}$

Donc $n \in \mathbb{Z}$ tq $3|n$ et $2|n \Rightarrow$ lemme de Gauss $(2 \wedge 3 = 1)$

$6|n$

<u>Réciproque</u> : si $n = 6k$

$(\sigma^{6k}) = (\sigma^3)^{2k} = e^{2k} = e$

$(\tau^{6k}) = (\tau^2)^{3k} = e^{3k} = e$

Donc $\boxed{\{n \in \mathbb{Z} \mid \sigma^n = \tau^n\} = 6\mathbb{Z}}$

Exercice 9

1) $\pi = (1\ 11\ 3\ 4)(5\ 6)(7\ 8\ 9)$

$\sigma = (1\ 3\ 4\ 11)(2\ 6\ 7\ 8\ 10)(5\ 9)$

$\pi \circ \sigma = (1\ 4\ 3)(2\ 5\ 7\ 9\ 6\ 8\ 10)$

2) $\operatorname{ord}(\pi) = \operatorname{ppcm}(4, 2, 3) = 12$

$\operatorname{ord}(\sigma) = \operatorname{ppcm}(4, 5, 2) = 20$

$\operatorname{ord}(\pi \circ \sigma) = \operatorname{ppcm}(3, 7) = 21$

3) $|S_{11}| = 11!$

4) Existe-t'il un elt d'ord 13 dans S_{11} ?

NON $\to$ par le th de Lagrange, on devrait avoir 13 divise 11!.