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)

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

$\bar{0} \neq \bar{2}$ 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

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

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

$$\begin{aligned} \mathbb{Z}/10\mathbb{Z} &\to \mathbb{Z}/15\mathbb{Z} \\ \bar{1} &\mapsto \bar{3} \end{aligned}$$

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 $f(\bar{0}) = \bar{0}$, $f(\bar{1}) = \bar{3}$, $f(\bar{2}) = \bar{6}$, $f(\bar{3}) = \bar{9}$, $f(\bar{4}) = \overline{12}$, $f(\bar{5}) = \overline{15} = \bar{0}$, $f(\bar{6}) = \overline{18} = \bar{3}$, $f(\bar{7}) = \overline{21} = \bar{6}$, $f(\bar{8}) = \overline{24} = \bar{9}$, $f(\bar{9}) = \overline{27} = \overline{12}$

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 $\mathrm{ord}(x)$.