UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 3

Corrigé de l'examen du 18 février 2013

Exercice 3

1 $\forall (x,y) \in G^2, \quad \varphi(x \star y) = \varphi(x) \otimes \varphi(y)$

2 Pour $(x,y) \in G^2$, on a

$$\begin{aligned} & (\psi \circ \varphi)(x \star y) \\ \text{(par définition de } \circ) \quad & = \psi(\varphi(x \star y)) \\ \text{(car } \varphi \text{ est un morphisme de groupes)} \quad & = \psi(\varphi(x) \otimes \varphi(y)) \\ \text{(car } \psi \text{ est un morphisme de groupes)} \quad & = \psi(\varphi(x)) \perp \psi(\varphi(y)) \\ \text{(par définition de } \circ) \quad & = (\psi \circ \varphi)(x) \perp (\psi \circ \varphi)(y). \end{aligned}$$

3 Fixons $g \in G$. On considère pour $n \in \mathbf{N}$ l'hypothèse de récurrence

$$\mathcal{H}_n \ : \ \varphi(g^{\star n}) = \varphi(g)^{\otimes n}$$

$\mathcal{H}_0$ est vrai. En effet par définition $g^{\star 0} = e_G$ et $\varphi(g)^{\otimes 0} = e_H$. Or comme φ est un morphisme, on sait qu'on a $\varphi(e_G) = e_H$.

Supposons $\mathcal{H}_n$ vraie et montrons que $\mathcal{H}_{n+1}$ l'est encore. On a

$$\begin{aligned} & \varphi(g^{\star(n+1)}) \\ \text{(par définition de } g^{\star(n+1)}) \quad & = \varphi(g \star g^{\star n}) \\ \text{(car } \varphi \text{ est un morphisme)} \quad & = \varphi(g) \otimes \varphi(g^{\star n}) \\ \text{(d'après } \mathcal{H}_n) \quad & = \varphi(g) \otimes \varphi(g)^{\otimes n} \\ \text{(par définition de } h^{\otimes(n+1)} \text{ pour } h \in H) \quad & = \varphi(g)^{\otimes(n+1)} \end{aligned}$$

et donc $\mathcal{H}_{n+1}$ est vraie.

Ainsi $\mathcal{H}_n$ est vraie pour tout n, ce qui répond à la question.

4 Pour $g \in G$ et $n \in \mathbf{N}$, l'égalité est vraie d'après la question précédente. Soit à présent $n \in \mathbf{Z} \setminus \mathbf{N}$. On sait d'après la question précédente qu'on a $\varphi(g^{\star(-n)}) = \varphi(g)^{\otimes(-n)}$. Par ailleurs le symétrique de $g^{\star(-n)}$ est $g^{\star n}$, et comme l'image par un morphisme de groupes du symétrique d'un élément est le symétrique de l'image de cet élément, $\varphi(g^{\star n})$ est le symétrique de $\varphi(g)^{\otimes(-n)}$, c'est-à-dire $\varphi(g)^{\otimes n}$, ce qu'il fallait démontrer.

5 $\forall g \in G, \quad \forall n \in \mathbf{Z}, \quad \varphi(g^n) = n.\varphi(g)$.

6 Soit n l'ordre de g. Alors n est un entier strictement positif, et on a d'après ce qui précède

$$\varphi(g)^{\otimes n} = \varphi(g^{\star n}) = \varphi(e_G) = e_H$$

Donc $\varphi(g)$ est d'ordre fini, et son ordre divise n, c'est-à-dire l'ordre de g.

7 Il suffit par exemple d'exhiber g d'ordre fini, $g \neq e_G$ (donc l'ordre de g est > 1) avec $\varphi(g) = e_H$. Par exemple on prend $G = H = \mathbf{Z}/2\mathbf{Z}$, $g = [1]_2$ et φ qui envoie tous les éléments de $\mathbf{Z}/2\mathbf{Z}$ sur $[0]_2$. L'ordre de g est 2 et celui de $\varphi(g)$ est 1.

Exercice 4

1

1. Écrivons $x = [n]_N$, $y = [m]_N$, avec $n, m \in \{0, \dots, p^2 - 1\}$. On a

$$x.y = [0]_N \Leftrightarrow [m.n]_N = [0]_N \Leftrightarrow p^2 \text{ divise } m.n$$

Comme p est un nombre premier, cette dernière condition équivaut à

$$(p^2 \text{ divise } m) \quad \text{ou} \quad (p^2 \text{ divise } n) \quad \text{ou} \quad (p \text{ divise } n \text{ et } m)$$

Finalement compte tenu de $n, m \in \{0, \dots, p^2-1\}$, l'ensemble des couples solution est

$$\{[0]_N\} \times \mathbf{Z}/N\mathbf{Z} \ \cup \ \mathbf{Z}/N\mathbf{Z} \times \{[0]_N\} \ \cup \{([k.p]_N, [\ell.p]_N)\}_{k,\ell \in \{1,\dots,p-1\}}$$

2. Pour $x \in \mathbf{Z}/N\mathbf{Z}$, on a

$$x^2 - [12]_N.x + [11]_N = (x - [6]_N)^2 - [36]_N + [11]_N = (x - [6]_N)^2 - [5]_N^2 = (x - [11]_N)(x - [1]_N)$$

Ainsi en posant $X = x - [11]_N$ et $Y = x - [1]_N$, on voit que x est solution de l'équation proposée si et seulement si (X, Y) est solution de l'équation $X.Y = [0]_N$.
D'après la question précédente, ceci sera vérifié si et seulement si

$$x = [11]_N \quad \text{ou} \quad x = [1]_N \quad \text{ou} \quad (\exists (k,\ell) \in \{1,\dots,p-1\}^2,\ x = [11+k.p]_N \text{ et } x = [1+\ell.p]_N) \quad (*)$$

Maintenant une condition nécessaire pour que la troisième éventualité se produise est

$$\exists (k,\ell) \in \{1,\dots,p-1\}^2,\ [11 + k.p]_N = [1 + \ell.p]_N$$

soit

$$\exists (k,\ell) \in \{1,\dots,p-1\}^2,\ [10 + (k-\ell).p]_N = [0]_N.$$

Si un tel (k, ℓ) existe, $N = p^2$ divise $10 + (k-\ell)p$, donc p divise $10 + (k-\ell)p$, donc p divise 10, donc $p = 2$ ou 5.
Ainsi si $p \notin \{2, 5\}$, la troisième éventualité ne peut jamais se produire et x est solution de l'équation proposée si et seulement si $x \in \{[1]_N, [11]_N\}$.
Si $p = 2$, x est solution de l'équation proposée si et seulement si

$$x = [11]_4 = [3]_4 \quad \text{ou} \quad x = [1]_4 \quad \text{ou} \quad (x - [11]_4 = [2]_4 \text{ et } x - [1]_4 = [2]_4)$$

Finalement l'ensemble des solutions est $\{[1]_4, [3]_4\}$ (on pouvait tout aussi bien traiter rapidement le cas $p = 2$ à la main en calculant les carrés dans $\mathbf{Z}/4\mathbf{Z}$).
Si $p = 5$, on peut aussi regarder ce qui se passe pour chaque valeur de $x \in \mathbf{Z}/4\mathbf{Z}$ mais c'est plus long ! On peut reprendre le raisonnement au niveau de $(*)$, en le simplifiant un peu en remarquant que l'équation s'écrit alors $(x - [6]_{25})^2 = [25]_{25} = [0]_{25}$. D'après la question précédente, x sera solution de l'équation proposée si et seulement si

$$\exists k \in \{0,\dots,4\}^2,\ x - [6]_{25} = [k.p]_{25}$$

d'où l'ensemble des solutions

$$\{[6]_{25}, [11]_{25}, [16]_{25}, [21]_{25}, [26]_{25} = [1]_{25}\}.$$

2 Comme 7 est premier, un entier n'est pas premier avec 7 si et seulement si c'est un multiple de 7. Comme $49 = 7^2$, il y a 7 multiples de 7 compris entre 0 et 48, ainsi $\varphi(49) = 49 - 7 = 42$.

Si $x^{42} = [1]_{49}$, on a $x.x^{41} = [1]_{49}$ donc $x \in (\mathbf{Z}/49\mathbf{Z})^\times$ (de même si $x^{11} = [1]_{49}$). Mais d'après le théorème d'Euler (ou le théorème de Lagrange et le fait que $(\mathbf{Z}/49\mathbf{Z})^\times$ soit de cardinal $\varphi(49)$), tout élément $x \in (\mathbf{Z}/49\mathbf{Z})^\times$ vérifie l'équation proposée. Ainsi l'ensemble des solutions de la première équation est $(\mathbf{Z}/49\mathbf{Z})^\times$.

Les éléments x de $(\mathbf{Z}/49\mathbf{Z})^\times$ qui vérifient $x^{11} = [1]_{49}$ ont un ordre qui divise 11. Comme cet ordre divise aussi $\varphi(49) = 42 = 2.3.7$, il divise $\text{pgcd}(11, 42) = 1$. Nécessairement $x = [1]_{49}$ (qui est bien solution). L'ensemble des solutions de la deuxième équation est $\{[1]_{49}\}$.