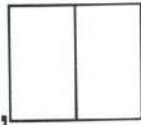
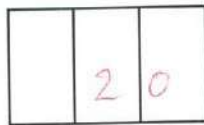


NOM GUEDJ

Prénom Alexandre

Promo 208

Date 23/03/16



GUEDJ Alexandre
L3 - 2015

22
/25

MATIÈRE Théorie des Groupes.

Exercice 1

Dans $(\mathbb{Z}/48\mathbb{Z}, \oplus)$, l'ordre de $\overline{20}$ est un diviseur de 48.

Liste des diviseurs de 48 : $\{1, 2, 4, 6, 8, 12, 24, 48\}$.

Pour trouver l'ordre de $\overline{20}$, on trouve x tel que

$$\overline{20} \times x = \overline{0}.$$

Si 20 et 48 sont premiers entre eux, alors l'ordre est 48.

Or, leur PGCD est 4. On teste donc avec les diviseurs restants.

$$\overline{20} \times 1 = \overline{20}$$

$$\overline{20} \times 2 = \overline{40}$$

$$\overline{20} \times 4 = \overline{32}$$

$$\overline{20} \times 8 = \overline{16}$$

$$\overline{20} \times 12 = \overline{0}.$$

Ainsi, l'ordre de $\overline{20}$ est 12.

Exercice 2.

a. Dans $(\mathbb{Z}/48\mathbb{Z}, \oplus, \odot)$, le nombre d'éléments inversibles est défini par $\varphi(48)$. $48 = 2^4 \times 3$, ainsi :

$$\begin{aligned}\varphi(48) &= 2^4 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \\ &= 16. \quad \text{Il y a 16 éléments inversibles.} \quad (2)\end{aligned}$$

Les éléments inversibles sont ceux qui sont premiers avec 48 et compris entre 0 et 47 :

$$\{\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}, \bar{19}, \bar{23}, \bar{25}, \bar{29}, \bar{31}, \bar{35}, \bar{37}, \bar{41}, \bar{43}, \bar{47}\}$$

Nous obtenons bien 16 éléments inversibles.

b. L'inverse de $\bar{7}$ est x tel que $\bar{7}x = \bar{1}$, ou encore

$$7x - 1 \equiv 0 [48]. \quad 48 \mid 7x - 1, \quad 7x - 48k = 1.$$

On applique l'algorithme afin de trouver x : (2)

K	x	r	q
1	0	48	
0	1	7	
1	-6	6	6
-1	<u>7</u>	1	1
-	-	0	6

Ainsi, l'inverse de $\bar{7}$ est $\bar{7}$.

$$c. \quad \overline{7}x + \overline{12} = \overline{5}$$

$$\text{donc } \overline{7}x + \overline{12} + \overline{36} = \overline{5} + \overline{36}, \quad \overline{36} \text{ étant l'inverse de } \overline{12}.$$

$$\text{donc } \overline{7}x = \overline{41}.$$

$$\text{donc } \overline{7} \times \overline{7}x = \overline{41} \times \overline{7}$$

$$\text{donc } \underline{x = \overline{47}} \quad \textcircled{2}$$

Exercice 3.

a. R_{48} désigne les éléments inversibles dans $\mathbb{Z}/48\mathbb{Z}$. On, le PGCD de 26 et 48 est 2, 26 et 48 n'étant pas premiers entre eux, $\overline{26}$ n'est pas incl. dans R_{48} . $\textcircled{2}$

b. Trouvons $\overset{u}{x}$ tel que $\overline{x}^{13u} = \overline{x}$. D'après le théorème d'Euler, on sait que $\overline{x}^{\phi(n)} = \overline{1} \quad \forall x \in \mathbb{R}_n$.

Ainsi, trouvons u tel que $13u \equiv 1 [16]$, 16 étant $\phi(48)$.

K	u	r	q
1	0	16	
0	1	13	
1	-1	3	1
-4	<u>5</u>	1	4
-	-	0	3

$$u = 5.$$

On a finalement $f^{-1}(x) = x^5$.

(2)

Exercice 4.

a. Si $P(x)$ réductible, alors il peut s'écrire sous la forme

$(X+a)(X^2+bX+c)$. Trouvons les valeurs a, b, c :

$$= X^3 + bX^2 + cX + aX^2 + abX + ac$$

$$= X^3 + X^2(a+b) + X(ab+c) + ac. \text{ Par identification, on a:}$$

$$a+b=1$$

$$ab+c=0$$

$$ac=1. \text{ Si } ac=1, \text{ alors } a=c=1.$$

Dans ce cas, $1+b=1$, $b=0$.

Or, si $a=1$, $b=0$, $c=1$, on a $ab+c=1$, et non 0.

Ainsi, on démontre que $P(x) = X^3 + X^2 + 1$ est irréductible.

b. Il y a 8 éléments du corps $(K = \mathbb{F}_2[x]/P(x), \oplus, \odot)$.

2

NOM GCEDJ

Prénom Alexandre

Promo 2018

Date 23/03/16

MATIÈRE Théorie des Groupes

d. On doit trouver x tel que $\theta x = 1$. Or, on sait que $\theta^3 + \theta^2 + 1 = 0$, ou encore $\theta^3 + \theta^2 = -1$, ou encore $\theta(\theta^2 + \theta) = 1$. Ainsi, on en déduit que l'inverse de θ est $\theta^2 + \theta$.

On aurait pu également utiliser l'algorithme de l'anneau d'Euclide étendu afin de trouver x .

3

e. On sait que $\theta^3 = \theta^2 + 1$. On obtient le tableau suivant:

θ	θ
θ^2	θ^2
θ^3	$\theta^2 + 1$
θ^4	$\theta^2 + \theta + 1$
θ^5	$\theta + 1$
θ^6	$\theta^2 + \theta$
θ^7	1
θ^8	θ

3

