corDE « Groupes »

Pas de machines, pas de documents, pas de téléphone

sauf étudiants chinois : dictionnaire

Tous les résultats seront justifiés (par un calcul, un raisonnement, une définition, un théorème que l'on citera soit par son nom, soit par son contenu)

Exercice 1. (environ 2 pts)

On considère le groupe $(\mathbb{Z}/48\mathbb{Z}, +)$

Déterminer l'ordre de $\overline{20}$.

Solution. on cherche le plus petit k>0 tel que 48 divise 20k

ce qui équivaut à 12 divise 5k

appliquons le th de gauss 12 divise k

donc le plus petit k est 12

Exercice 2.

On considère l'anneau $(\mathbb{Z}/48\mathbb{Z}, +, .)$ (environ 5 pts)

a. Déterminer la liste des éléments inversibles.

b. Déterminer l'inverse de $\bar{7}$.

c. Résoudre l'équation $\bar{7}$x+$\overline{12}$=$\bar{5}$.

Solution.

a. Il s'agit des classes des entiers premiers avec 48: il y en a $\varphi(48) = \varphi(16)\varphi(3) = 8\,2 = 16$

(par paresse vis àvis de mon éditeur j'oublierai les barres mais il faut les mettre)

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

b. l'inverse de $\bar{7}$: soit bezout, soit 7*7=49≡1[48], donc $\bar{7}^{-1}= \bar{7}$

c. $\bar{7}$x+$\overline{12}$=$\bar{5} \Longleftrightarrow x + \overline{12}.\,\bar{7} = \bar{5}.\bar{7} \Longleftrightarrow x + \overline{36} = \overline{35} \Longleftrightarrow x = \overline{47}$

Exercice 3.

On considère le groupe $(R_{48}, .)$ (environ 4 pts)

a. Est-ce que $\overline{26}$ y appartient ?

b. On désigne par f l'application définie pour tout x de R_{48} par x$\longmapsto f(x) =$ x^{13}; déterminer l'application f^{-1}.

Solution.

a. non puisque $26 \wedge 48 \neq 1$

b. c'est le principe de rsa on cherche un entier e tel que 13e≡1[$\varphi(48) = 16$].

pour cela bezout ou 13*5=65≡1[16]; d'où f^{-1}: $x \longmapsto x^5$

Exercice 4.

On considère le corps $(F_2, +, .)$ (environ 12 pts)

a. Soit P(X)= X^3+X^2+1; montrer qu'il est irréductible dans $(F_2[X],+,.)$.

b. Quel est le nombre d'éléments du corps $(K=F_2[X]/P(X),+,.)$?

c. On posera $\theta=$ classe de X; quel est l'ordre de θ dans le groupe $(K\setminus\{0\},.)$?

d. Déterminer l'inverse de θ sous la forme d'une combinaison linéaire de puissances de θ.

e. Déterminer pour chaque combinaison linéaire de puissances de θ son expression sous la forme d'une puissance de θ.

Solution.

a. s'il n'est pas irréductible alors il existe a,b,c dans F_2 tels que X^3+X^2+1=(X+a)(X^2+bX$+c$)

cette égalité équivaut à $\begin{cases} a+b=1 \\ \mathrm{ab}+c=0 \\ \mathrm{ac}=1 \end{cases}$

alors a=c=1 d'où b=0 et b=1 impossible

b. il s'agit des expressions polynomiales en θ de degré inférieur ou égal à 2: comme il y a « deux choix » pour chaque coeff: 2*2*2=8

c. le nombre d'éléments de K*=K$\setminus\{0\}$ est 7, c'est un groupe cyclique engendré par θ , donc l'ordre de θ est 7.

d. $\theta^3+\theta^2=1$ donc $\theta(\theta^2+\theta)=1$ donc $\theta^{-1}=\theta^2+\theta$

e. $$\begin{aligned} \theta &= \theta \\ \theta^2 &= \theta^2 \\ \theta^3 &= \theta^2+1 \\ \theta^4 &= \theta^3+\theta=\theta^2+\theta+1 \\ \theta^5 &= \theta^3+\theta^2+\theta=\theta+1 \\ \theta^6 &= \theta^2+\theta \\ \theta^7 &= 1 \end{aligned}$$