DS n°1 Plus dur

mercredi 16 septembre 2015 (durée 4 heures)

Toute calculatrice interdite

Rappel : Bien traiter quelques questions rapporte des points, les bâcler toutes n'en rapporte aucun.

Problème

Notations et rappels

Pour $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$ on note $a \wedge b$ le Pgcd de a et b, et $a \vee b$ le Ppcm de a et b.
L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est noté $\{\overline{0}, \overline{1}, ...\overline{n-1}\}$

Partie I.

1. Soir $p \in \mathbb{N}^* \setminus \{1, 2, 3, 4\}$. Montrer que si p et $p + 2$ sont premiers, alors $p \equiv -1[6]$
2. Montrer que le polynôme $X^2 - \overline{5}$ n'a pas de racine dans $\mathbb{Z}/13\mathbb{Z}$
3. Montrer que $\forall x \in \mathbb{Z}/13\mathbb{Z},\ \forall y \in \mathbb{Z}/13\mathbb{Z} \setminus \{\overline{0}\}$ alors $(xy^{-1})^2 - \overline{5} \neq \overline{0}$

Partie II.

Soit $(A, +, *)$ un anneau commutatif d'élément unité 1_A.
On note $U(A)$ l'ensemble des éléments inversibles de A. On sait que $(U(A), *)$ est un groupe, on ne demande pas de le redémontrer

1. Démontrer que le groupe $U(\mathbb{Z}/n\mathbb{Z})$ est l'ensemble

$$V = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \ / \ a \wedge n = 1\}$$

2. On dit qu'un élément a de $\mathbb{Z}/n\mathbb{Z}$ est un diviseur de zéro si et seulement si

$$a \neq \overline{0} \text{ et } \ \exists b \in \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\} \text{ tel que } ab = \overline{0}$$

   Pour $n \in \mathbb{N}^*$ montrer que l'ensemble des diviseurs de zéro de $\mathbb{Z}/n\mathbb{Z}$ est égal à l'ensemble

$$D = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} \setminus \{\overline{0}\} \ / \ a \wedge n \neq 1\}$$

Partie III.

On note K_{13} l'ensemble $\mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}$ que l'on munit des lois de composition suivantes :
$(x, y) \oplus (x', y') = (x + x', y + y')$
$(x, y) \otimes (x', y') = (xx' + \overline{5}yy', xy' + x'y)$
Pour $\alpha \in K_{13}$ on note $\alpha^2 = \alpha \otimes \alpha$

1. Montrer que $(K_{13}, \oplus\otimes)$ est un corps commutatif. Quel est son cardinal ?
2. Soit $H_{13} = \{(x, \overline{0}) \in \mathbb{Z}/13\mathbb{Z} \times \mathbb{Z}/13\mathbb{Z}\}$ un sous-ensemble de K_{13}. Montrer que $(H_{13}, \oplus, \otimes)$ est un corps isomorphe à $(\mathbb{Z}/13\mathbb{Z}, +, .)$.
3. Désormais on identifie H_{13} et $\mathbb{Z}/13\mathbb{Z}$ en identifiant x et $(x, \overline{0})$. Trouver les éléments α de K_{13} tels que $\alpha^2 = \overline{5}$ et factoriser le polynôme $X^2 - \overline{5}$ dans $K_{13}[X]$.

Partie IV.

Soit $(G, *)$ un groupe commutatif fini, x un élément de G, on note $o(x)$ l'ordre de l'élément x de G.

1. Soit $x \in G,\ \ell \in \mathbb{N}^*$ tels que $o(x) = \ell$. Vérifier que x^{-1} est aussi d'ordre ℓ.

2. Soient maintenant a et b deux éléments de G d'ordre m et n respectivement. Montrer que si $m \wedge n = 1$ alors $o(ab) = mn$.

3. Montrer que même si m et n ne sont pas premiers entre eux il existe c dans G tel que $o(c) = m \vee n$.
   On pourra remarquer que ce ppcm s'écrit $m'n'$ avec m' divisant m, n' divisant n et m' et n' premiers entre eux.

4. Considérons le ppcm r des ordres des éléments de G. r est parfois appelé l'exposant de G, c'est le plus petit entier $n \in \mathbb{N}^*$ tel que $\forall x \in G,\ x^n = 1$. Montrer qu'il existe $c \in G$ tel que $o(c) = r$.

5. Soit $(F, +, .)$ un corps et $(G, .)$ un sous-groupe fini de $(F^*, .)$, montrer que G est cyclique.

6. On note $K_{13}^* = K_{13} \setminus \{(\overline{0}, \overline{0})\}$. Déterminer le nombre de générateurs du groupe $(K_{13}^*, \otimes)$

Exercice

Soit G un groupe abélien dont la loi de groupe est notée additivement. Si A, B sont des parties de G, on note respectivement $A + B$ et $A - B$ l'ensemble des sommes $a + b$ et l'ensemble des différences $a - b$ quand a parcourt A et b parcourt B.

1. Soit t un entier naturel non nul et soit N un entier naturel.
   (a) Soit n et p des entiers naturels tels que $n \geqslant p$. Démontrer l'égalité :
   $$\binom{p}{p} + \binom{p+1}{p} + ... + \binom{n}{p} = \binom{n+1}{p+1}$$
   (b) Démontrer que l'ensemble des $t-$uplets $(a_1, ..., a_t)$ d'entiers naturels tels que $a_1 + ... + a_t = N$ a pour cardinal $\binom{N+t-1}{N}$

2. Soit G un groupe abélien fini et soit A, B des parties non vides de G telles que $\text{Card}(A) + \text{Card}(B) > \text{Card}(G)$.
   (a) Démontrer que $G = A + B$
   (b) Donner un exemple où on a $\text{Card}(A) + \text{Card}(B) = \text{Card}(G)$ mais $G \neq A + B$

3. Soit G un groupe abélien, et A, B des parties finies non vides de G. Démontrer les inégalités :
   $$\max(\text{Card}(A), \text{Card}(B)) \leqslant \text{Card}(A + B) \leqslant \text{Card}(A)\text{Card}(B)$$