MP – CPGE Mohammed VI-Kénitra

Année scolaire 24/25

Devoir surveillé $n^\circ 1$

01/10/2024

Durée 3 heures

La qualité de la rédaction et de la présentation, la clarté et la précision des raisonnements entreront pour une part importante dans l'appréciation des copies. L'usage des calculatrices n'est pas autorisé. Tout résultat fourni dans l'énoncé peut être admis et utilisé par la suite, même s'il n'a pas été démontré.

NOTATIONS ET RAPPELS.

Soit $n \in \mathbf{N}^*$, $(a, b) \in \mathbf{Z}^2$, on dit que a est congru à b modulo n, et on note $a \equiv b[n]$ si et seulement si n divise $b - a$.

Pour $(a, b) \in \mathbf{Z}^* \times \mathbf{Z}^*$, on note $a \wedge b = \text{pgcd}(a, b)$ et $a \vee b = \text{ppcm}(a, b)$.

On note $\mathbf{Z}/n\mathbf{Z}$ l'ensemble quotient de $\mathbb{Z}$ par la relation $\equiv [n]$. $\mathbf{Z}/n\mathbf{Z}$ est un ensemble fini, à n éléments : $\mathbf{Z}/n\mathbf{Z} = \left\{ \overline{0}, \overline{1}, \ldots, \overline{n-1} \right\}$.

On définit les deux lois de composition interne usuelles dans $\mathbf{Z}/n\mathbf{Z}$, notées + et . par :

$$\forall (x, y) \in \mathbf{Z}^2, \overline{x} + \overline{y} = \overline{x + y} \text{ et } \overline{x}.\overline{y} = \overline{xy}.$$

Il est facile de montrer (non demandé) que $(\mathbf{Z}/n\mathbf{Z}, +, .)$ est un anneau commutatif.

- PREMIÈRE PARTIE -

1. Lister les éléments inversibles (en précisant leur inverse) de $\mathbf{Z}/6\mathbf{Z}$ et ceux de $\mathbf{Z}/13\mathbf{Z}$.

2. Soit $p \in \mathbf{N}^* \setminus \{ 1, 2, 3, 4 \}$. Montrer que si p et $p + 2$ sont premiers, alors $p \equiv -1[6]$.

3. Montrer que le polynôme $X^2 - \overline{5}$ est irréductible sur $\mathbf{Z}/13\mathbf{Z}[X]$.

- DEUXIÈME PARTIE -

Soit $(A, *, \diamond)$ un anneau d'élément unité 1_A, on note $\mathbf{U}(A) = \{ a \in A \mid \exists c \in A \text{ tel que } a \diamond c = c \diamond a = 1_A \}$ l'ensemble des éléments inversibles de A.

1. Montrer que $(\mathbf{U}(A), \diamond)$ est un groupe.

2. Montrer en utilisant le théorème de Bezout que le groupe $\mathbf{U}(\mathbf{Z}/n\mathbf{Z})$ est l'ensemble :

$$V = \{ \overline{a} \in \mathbf{Z}/n\mathbf{Z} \mid a \wedge n = 1 \}.$$

3. Pour $n \in \mathbb{N}^*$ montrer que l'ensemble des diviseurs de zéro de $\mathbf{Z}/n\mathbf{Z}$ est l'ensemble :

$$D = \left\{ \overline{a} \in \mathbf{Z}/n\mathbf{Z} \setminus \{ \overline{0} \} \;\middle|\; a \wedge n \neq 1 \right\}.$$

- TROISIÈME PARTIE -

On note $\mathbf{K}_{13}$ l'ensemble $\mathbf{Z}/13\mathbf{Z} \times \mathbf{Z}/13\mathbf{Z}$ que l'on munit des lois de composition suivantes :

$(x, y) \oplus (x', y') = (x + x', y + y')$

$(x, y) \bullet (x', y') = \left(xx' + \overline{5}yy', xy' + x'y\right)$

Pour $\alpha \in \mathbf{K}_{13}$, on note $\alpha^2 = \alpha \bullet \alpha$.

1. Montrer que $(K_{13}, \oplus, \bullet)$ est un corps commutatif à 169 éléments.

2. Soit $H_{13} = \left\{ \left(x, \overline{0}\right) \in \mathbf{Z}/13\mathbf{Z} \times \mathbf{Z}/13\mathbf{Z} \right\}$ un sous-ensemble de $\mathbf{K}_{13}$. Montrer que $(H_{13}, \oplus, \bullet)$ est un sous-corps isomorphe à $(\mathbf{Z}/13\mathbf{Z}, +, .)$.

3. Désormais, on identifie H_{13} et $\mathbf{Z}/13\mathbf{Z}$ en identifiant x et $\left(x, \overline{0}\right)$. Trouver les éléments α de $\mathbf{K}_{13}$ tels que $\alpha^2 = \overline{5}$ et factoriser $X^2 - \overline{5}$ dans $\mathbf{K}_{13}[X]$.

- QUATRIÈME PARTIE -

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 $x \in G$, $l \in \mathbf{N}^*$ tels que $o(x) = l$. Vérifier que x^{-1} $\left(= x^{l-1}\right)$ 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 $o(a.b) = mn$.

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 $n \in \mathbf{N}^*$ tel que $x^n = 1$, $\forall x \in G$. Montrer qu'il existe $c \in G$, tel que $o(c) = r$.

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

6. On note $\mathbf{K}_{13}^* = \mathbf{K}_{13} \setminus \{ \left(\overline{0}, \overline{0}\right) \}$. Déterminer les 48 générateurs du groupe $\left(\mathbf{K}_{13}^*, \bullet\right)$.

Fin de l'épreuve