UNIVERSITÉ DE LILLE

Enseignant responsable: **Pierre DÈBES**
Filière: **Licence 5ème Semestre**
Matière: **M51**
Année universitaire: **2020/2021 - Session 2**
Date, heure et lieu: **Mercredi 9 Juin à 14h, Halles Grémeaux**
Durée de l'épreuve: **3 heures**

Chacune des deux parties devra être rédigée sur une copie différente.
Ni calculatrice ni documents.
Le barême est donné à titre indicatif.
Une attention particulière sera portée à la rédaction.

PARTIE I (copie blanche)

Exercice 1 [6 pts]: On définit l'ensemble $\mathbb{Z}[i\sqrt{11}]$ et l'application $N : \mathbb{Z}[i\sqrt{11}] \to \mathbb{Z}$ par:

$$\mathbb{Z}[i\sqrt{11}] = \{a + ib\sqrt{11} \in \mathbb{C} \mid a, b \in \mathbb{Z}\} \quad \text{et} \quad N(a + ib\sqrt{11}) = a^2 + 11b^2.$$

(a) Montrer que $(\mathbb{Z}[i\sqrt{11}], +, \times)$ est un anneau commutatif unitaire,
et que pour tous $z, z' \in \mathbb{Z}[i\sqrt{11}]$, on a $N(zz') = N(z)N(z')$.

(b) Montrer que les seuls éléments inversibles de l'anneau $\mathbb{Z}[i\sqrt{11}]$ sont 1 et -1.

(c) Montrer que 2, 3, 5, 7 sont des irréductibles de l'anneau $\mathbb{Z}[i\sqrt{11}]$.

(d) Montrer que ni 9 ni 11 ni 47 ne sont des irréductibles de l'anneau $\mathbb{Z}[i\sqrt{11}]$.

(e) Vérifier que $(1 + i\sqrt{11})(1 - i\sqrt{11}) = 12$ et en déduire que $\mathbb{Z}[i\sqrt{11}]$ n'est pas principal.

Exercice 2 [4 pts]: Soient G un groupe fini et p un nombre premier divisant l'ordre de G. Soit X l'ensemble des p-uplets $(g_1, \ldots, g_p) \in G^p$ tels que le produit $g_1 \cdots g_p$ vaut 1 (l'élément neutre de G). On note σ le p-cycle $(1\,2\,\ldots\,p)$ et $\rho : \langle\sigma\rangle \to \mathrm{Bij}(X)$ l'action du groupe engendré par σ (dans le groupe symétrique S_p) sur l'ensemble X définie par

$$\rho(\sigma)(g_1, \ldots, g_p) = (g_{\sigma(1)}, \ldots, g_{\sigma(p)}) \text{ pour } \sigma \in S_p \text{ et } (g_1, \ldots, g_p) \in X.$$

(a) Montrer que l'application $f : X \to G^{p-1}$ définie par $f(g_1, \ldots, g_p) = (g_1, \ldots, g_{p-1})$ est une bijection et en déduire $\mathrm{card}(X)$.

(b) Montrer que les points fixes de l'action ρ sont exactement les p-uplets de la forme $(g, \ldots, g)$ avec $g \in G$ tel que $g^p = 1$.

(c) Ecrire la formule des classes pour l'action ρ.

(d) Montrer que G possède un élément d'ordre p.

T.S.V.P.

PARTIE II (copie bleue)

Dans les exercices 3 et 4, on note $(\mathbb{Z}/p\mathbb{Z})^*$ l'ensemble $(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}$.

Exercice 3 [6 pts]: Soit p un nombre premier. On note $\mathcal{C}_5(p)$ l'ensemble des puissances 5-èmes des éléments de $\mathbb{Z}/p\mathbb{Z}$, c'est-à-dire:

$$\mathcal{C}_5(p) = \{x^5 \mid x \in \mathbb{Z}/p\mathbb{Z}\}, \text{ et } \mathcal{C}_5(p)^* = \mathcal{C}_5(p) \setminus \{0\}.$$

(a) Montrer que l'application $\varphi : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ définie par $\varphi(x) = x^5$ est un morphisme du groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$, que son groupe image est $\mathcal{C}_5(p)^*$ et que son noyau $\ker(\varphi)$ est d'ordre ≤ 5.

(b) Montrer que si $p \not\equiv 1$ [mod 5] alors $|\ker(\varphi)| = 1$.

(c) Montrer que si $p \equiv 1$ [mod 5] alors $|\ker(\varphi)| = 5$. (<u>Indication</u>: on pourra utiliser la question (d) de l'exercice 2).

(d) Montrer que si $p \equiv 1$ [mod 5], alors $\mathcal{C}_5(p)^*$ est l'ensemble des éléments $x \in \mathbb{Z}/p\mathbb{Z}$ tels que $x^{(p-1)/5} = 1$.

(e) Quel est l'ensemble $\mathcal{C}_5(p)^*$ si $p \not\equiv 1$ [mod 5]?

Exercice 4 [4 pts]: Soient p un nombre premier et $\mu \in \mathbb{Z}$ un entier tel que p divise $\mu^4 + 1$. On note $\overline{\mu}$ la classe de μ modulo p.

(a) Montrer que $\overline{\mu}$ est d'ordre au plus 8 dans le groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$.

(b) Montrer que si $p \neq 2$, alors $\overline{\mu}$ est d'ordre égal à 8 dans le groupe $((\mathbb{Z}/p\mathbb{Z})^*, \times)$.

(c) Montrer que pour tout entier pair m, si p est un diviseur premier de $m^4 + 1$, alors on a $p \equiv 1$ [mod 8].