Théorie des nombres

PARTIEL

Les exercices sont indépendants. Dans chaque exercice, vous pouvez indiquer que vous admettez la réponse à une question pour continuer. Documents, notes de cours ou de TD, téléphones portables, calculatrices sont interdits. Justifiez toutes vos réponses. Il est bon de relire sa copie...

Exercice 1

Introduire un anneau A et une fonction norme $N : A \to \mathbf{Z}$ dont on décrira les propriétés principales pour montrer que pour tout $(a, b, c, d) \in \mathbf{Z}^4$, on a une identité de la forme

$$(a^2 + 5b^2)(c^2 + 5d^2) = (???)^2 + ???(???)^2.$$

Exercice 2

Soit p un nombre premier et $k = \mathbf{F}_p$ le corps à p éléments.

1.– Quel est le nombre de polynômes de $k[X]$ de degré strictement inférieur à m ?

2.– Pour tout polynôme unitaire f de $k[X]$ de degré m, on pose $\| f \| := p^m$. Calculer $\| fg \|$ pour tout couple (f, g) de polynômes unitaires de $k[X]$.

3.– Montrer que la somme $\displaystyle\sum_{\substack{f \in k[X] \\ \text{unitaire}}} \frac{1}{\| f \|}$ diverge alors que la somme $\displaystyle\sum_{\substack{f \in k[X] \\ \text{unitaire}}} \frac{1}{\| f \|^2}$ converge.

4.– On considère l'ensemble $\mathcal{P} := \{f \in k[X], \text{unitaire irréductible}\}$ et pour tout $n \in \mathbf{N}^\star$ l'ensemble $\mathcal{P}_n := \{f \in k[X], \text{unitaire irréductible de degré inférieur à } n\}$. On s'intéresse à la convergence de la somme $\displaystyle\sum_{f \in \mathcal{P}} \frac{1}{\| f \|}$. On pose $\zeta_n := \displaystyle\prod_{f \in \mathcal{P}_n} \frac{1}{1 - \frac{1}{\|f\|}}$. Montrer que $\lim \zeta_n = +\infty$.

5.– Montrer que, pour tout $n \in \mathbf{N}^\star$, on a $\ln \zeta_n = \displaystyle\sum_{f \in \mathcal{P}_n} \frac{1}{\| f \|} + \sum_{f \in \mathcal{P}_n} \sum_{k=2}^{+\infty} \frac{1}{k \| f \|^k}$.

6.– Que peut-on en déduire sur la somme $\displaystyle\sum_{f \in \mathcal{P}} \frac{1}{\| f \|}$? et sur l'ensemble $\mathcal{P}$?

Exercice 3

1.– Soit p un nombre premier différent de 2 et de 3. Montrer que si p s'écrit sous la forme $p = a^2 + 3b^2$, avec $(a, b) \in \mathbf{Z}^2$, alors p est congru à 1 modulo 3.

On suppose désormais que p est congru à 1 modulo 3.

2.– Montrer que le groupe $(\mathbf{F}_p)^\times$ des inversibles du corps $\mathbf{F}_p$ admet un élément d'ordre 3.

3.– Montrer que le polynôme $X^2 + X + 1$ admet une racine α dans $\mathbf{F}_p$.

On notera A l'anneau $A = \mathbf{Z}[\sqrt{-3}]$ et B l'anneau $B = \mathbf{Z}[j]$ où j est la racine cubique complexe primitive de l'unité $j = \frac{-1+\sqrt{-3}}{2}$.

4.– Montrer que $A \subset B$. Montrer qu'un élément $\alpha = x+jy$ de B est dans A si et seulement si y est pair.

5.– Montrer que si α est dans B alors soit α soit $j\alpha$ soit $j^2\alpha$ est dans A.

6.– Montrer que p est une norme dans A si et seulement si c'est une norme dans B.

7.– Montrer que A n'est pas factoriel en écrivant deux factorisations de 4.

8.– Montrer que B est intègre et euclidien.

9.– Montrer que les anneaux quotients $\mathbf{F}_p[X]/(X^2+X+1)$ et $B/(p)$ sont isomorphes.

10.–En déduire que p est réductible dans B.

11.–Montrer que p est de la forme $p = N(x)$, avec $x \in B$.

12.–Montrer que p s'écrit donc sous la forme $p = a^2 + 3b^2$ avec $(a, b) \in \mathbf{Z}^2$.