Université d'Évry Val d'Essonne Licence 3 Mathematiques

M54 algèbre et arithmetique 2

Examen (16 Décembre 2015)

Exercice 1.

1. [**1 point**] Donner la définition de la caractéristique d'un anneau unitaire.
2. [**1 point**] Quelle est la caractéristique des anneaux $\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}$, $\mathbb{R}$, $\mathbb{R}[X]$.
3. [**1 point**] Quelle est la caractéristique d'un anneau intègre ? d'un corps ?
4. [**1 point**] Donner les définitions : Stathme, Anneau euclidien.

Exercice 2. Soit K un corps fini de cardinal q.

1. [**1 point**] On suppose dans cette question que K est de caractéritique 2. Montrer que tout élément de K est un carré.
   Dans la suite de cet exercice on suppose que la caractéritique p de K est différente de 2.
2. [**1 point**] Justifier pour quoi q doit-être de la forme : $q = p^d$.
3. [**1 point**] Déterminer les solutions de l'équation $x^2 = 1$ dans K.
4. [**1 point**] Montrer que , dans K, il y a exactement $(q+1)/2$ carrés.
   Indication : Étudier le morphisme de groupes $x \in K^\times \to x^2 \in K^\times$.
5. [**1 point**] Montrer que $x^{(q-1)/2} \in \{\pm 1\}$ pour tout $x \in K^\times$.
6. [**1 point**] Montrer que : $x \in K^\times$ est un carré $\iff x^{(q-1)/2} = 1$.
7. [**1 point**] Montrer que : -1 est un carré $\iff q = 1 \pmod 4$.
8. [**1 point**] En déduire que -1 est un carré modulo p si et seulement si $p = 1 \pmod 4$.

Exercice 3. Soit p un nombre premier ≥ 5, on pose : $\dfrac{A}{B} = \displaystyle\sum_{k=1}^{p-1} \frac{1}{k}$ avec $A, B \in \mathbb{N}^*$ tel que $pgcd(A, B) = 1$.
Le but de cet exercice est montrer que $p^2 | A$.

1. [**1 point**] Démontrer le théorème de Wilson : un entier $p > 2$ est un entier premier si et seulement si :

$$(p-1)! = -1 \pmod p.$$

2. [**1 point**] On pose, pour $1 \leq k \leq p-1$, $p_k = \frac{(p-1)!}{k(p-k)}$.
   Montrer l'identité : $pB \times \sum_{k=1}^{p-1} p_k = 2 \times (p-1)! \times A$.

3. [**1 point**] Montrer qu'un nombre $p \in \mathbf{N}$ est premier si et seulement s'il divise $\binom{p}{k}$ pour tout $k \in [\![1; p-1]\!]$.
4. [**1 point**] En travaillant dans $\mathbf{Z}/p\mathbf{Z}$, montrer que p divise $\sum_{k=1}^{p-1} p_k$.
5. [**1 point**] En déduire le théorème.

Exercice 4. On considère $\mathbb{Z}[i\sqrt{2}] = \{a + bi\sqrt{2};\ a, b \in \mathbb{Z}\}$, sur lequel on définit l'application définie de $\mathbb{Z}$ ver $\mathbb{N}$ par

$$N(a + bi\sqrt{2}) = a^2 + 2b^2.$$

1. [**1 point**] Montrer que $\mathbb{Z}[i\sqrt{2}]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.
2. [**1 point**] Déterminer les éléments inversibles de l'anneau $\mathbb{Z}[i\sqrt{2}]$.
3. [**1 point**] Soit $A, B \in \mathbb{Z}[i\sqrt{2}]$ avec $B \neq 0$. Montrer qu'il existe $q \in \mathbb{Z}[i\sqrt{2}]$ tel que
$$\left|\frac{A}{B} - q\right| < 1.$$
4. [**1 point**] Montrer que pour tout $A, B \in \mathbb{Z}[i\sqrt{2}]$ avec $B \neq 0$, il existe $q, r \in \mathbb{Z}[i\sqrt{2}]$ tel que $A = Bq + r$ avec $N(r) < N(B)$.
5. [**1 point**] En déduire que l'anneau $\mathbb{Z}[i\sqrt{2}]$ est euclidien pour la norme N.
6. [**1 point**] Montrer que , dans l'anneau $\mathbb{Z}[i\sqrt{2}]$, l'élément $i\sqrt{2}$ est irréductible.
7. Soit (x, y) dans $\mathbb{Z}^2$ une solution de l'équation
$$X^2 + 2 = Y^3.$$
Le but de la suite de cet exercice est de trouver toutes les solutions de cette équation diophantienne.
Soit I l'idéal de $\mathbb{Z}[i\sqrt{2}]$ engendré par les éléments $x + i\sqrt{2}$ et $x - i\sqrt{2}$.
   (a) [**1 point**] Montrer que l'idéal I contient $2i\sqrt{2}$.
   (b) [**1 point**] En déduire qu'il existe un entier m, $0 \leq m \leq 3$, tel que l'idéal I est engendré par $\left(i\sqrt{2}\right)^m$.
   (c) [**1 point**] Montrer que le cas $m \neq 0$ est impossible.
   (d) [**1 point**] En déduire que les éléments $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$.
   (e) [**1 point**] En consiérant la factorisation de y^3 dans l'anneau $\mathbb{Z}[i\sqrt{2}]$, montrer alors que $x + i\sqrt{2}$ est un cube dans cet anneau.
   (f) [**1 point**] Montrer qu'il existe $a, b \in \mathbb{Z}$ tel que :
$$x + i\sqrt{2} = \left(a + bi\sqrt{2}\right)^3.$$
En déduire que
$$x = a^3 - 6ab^2, \qquad \text{et} \quad 1 = (3a^2 - 2b^2)b.$$
   (g) [**1 point**] En déduire que : $x = \pm 5, y = 3$.
