Université Grenoble Alpes
Master1, mathématiques

Algèbre 1, examen
le 8 janvier 2019, de 9h à 12h

Documents et appareils électroniques interdits. **Chaque réponse doit être justifiée***; la qualité de la rédaction sera un élément d'appréciation des copies.*

I

On considère l'anneau $A = \mathbb{Z}[j]$, sous-anneau de $\mathbb{C}$, où on note $j = \frac{-1+i\sqrt{3}}{2}$. On admet que A est euclidien et on rappelle que $j^2 + j + 1 = 0$.

1. Montrer que A est isomorphe au quotient de $\mathbb{Z}[X]$ par l'idéal (X^2+X+1) et justifier que tout élément de A s'écrit de manière unique sous la forme $z = a+jb$, où a et $b \in \mathbb{Z}$.

On définit l'application *norme* d'un nombre complexe par $N(a + ib) = a^2 + b^2$, où $a, b \in \mathbb{R}$. On rappelle que N est multiplicative, c.a.d. que $N(zz') = N(z)N(z')$, pour tous $z, z' \in A$.

2. a) Calculer la norme d'un élément $z = a + jb$ de A. Vérifier que $N(z) \in \mathbb{N}$.

b) Montrer que $z \in A^\times$ si et seulement si $N(z) = 1$.

c) Soit $n \in \mathbb{N}$. Montrer que si $n \in N(A)$, alors n n'est pas irréductible dans A.

3. a) Soit $\mathbb{F}_q$ un corps fini. Quel est, suivant la classe de q modulo 3, l'ordre d'une racine de $P = X^2 + X + 1$ dans le groupe $\mathbb{F}_q^*$?

b) À quelle condition sur q le polynôme P est-il irréductible dans $\mathbb{F}_q$?

4. a) Dans la suite on désigne par p un nombre premier. À l'aide de **1**, montrer que les anneaux quotients $\mathbb{F}_p[X]/(X^2 + X + 1)$ et $A/(p)$ sont isomorphes.

b) En déduire que p est irréductible dans A si et seulement si $p \equiv 2 \bmod 3$.

c) Montrer si p n'est pas irréductible dans A, alors $p \in N(A)$.

On note B le sous-anneau $\mathbb{Z}[i\sqrt{3}]$ de $\mathbb{C}$. On a donc $B \subset A$.

5. a) Déterminer $B^\times$. L'élément 2 est-il irréductible dans B?

b) Montrer *soigneusement* que B n'est pas factoriel, en considérant $4 \in B$.

6. a) Soient $a, b \in \mathbb{Z}$. Montrer que $a + jb \in B$ si et seulement si b est pair.

b) Montrer que si $z \in A$, alors au moins un élément de l'ensemble $\{z, jz, j^2z\}$ appartient à B.

T.S.V.P.

c) Montrer que les images $N(A)$ et $N(B)$ sont égales.

d) En déduire l'équivalence: p est de la forme a^2+3b^2 où $a, b \in \mathbb{N}$ si et seulement si $p = 3$ ou $p \equiv 1 \bmod 3$.

II

VRAI ou FAUX? justifiez vos réponses.

1. Le corps $\mathbb{R}$ contient un sous-corps isomorphe à $\mathbb{Q}(T)$.

2. Le corps $\mathbb{Q}(T)$ est dénombrable.

3. Le corps $\mathbb{Q}(T)$ est algébriquement clos.

4. L'anneau $A = \mathbb{F}_2[X]/(X^{16} - X)$ est un corps.

5. L'anneau $A = \mathbb{F}_2[X]/(X^{16} - X)$ a un quotient qui est un corps à 16 éléments.

6. a) Le polynôme $X^4 + X^2 + X + 1$ est sans racine dans $\mathbb{F}_9$.

b) Le polynôme $2X^4 + 14X^2 + 8X + 2$ est irréductible dans $\mathbb{Q}[X]$.

7. L'anneau $\mathbb{D} = \mathbb{Z}[1/10]$ des nombres décimaux est un $\mathbb{Z}$-module de type fini.

III

On considère le polynôme $P = X^7 - 2$.

1. Quel est le degré d'un corps de décomposition de P sur $\mathbb{Q}$?

2. Dans la suite on considère P comme élément de $\mathbb{F}_{11}[X]$.

a) Montrer que le morphisme de groupes $x \mapsto x^7$ de $(\mathbb{F}_{11})^*$ dans lui-même est bijectif.

b) Déterminer les extensions finies de $\mathbb{F}_{11}$ dont le groupe multiplicatif contient un élément d'ordre 7.

c) Déterminer le corps de décomposition de P sur $\mathbb{F}_{11}$.

3. Décrire la décomposition du polynôme cyclotomique Φ_7 en polynômes irréductibles de $\mathbb{F}_{11}[X]$: degrés et multiplicités.

IV

On considère l'ensemble $M = \{(x, y, z) \in \mathbb{Z}^3 \mid x - 3y + 2z \equiv 0 \bmod 8\}$.

1. Montrer que M est un $\mathbb{Z}$-sous-module libre de $\mathbb{Z}^3$.

2. Donner la structure du groupe quotient $\mathbb{Z}^3/M$. Quel est le rang de M?

3. Donner une base de $\mathbb{Z}^3$ adaptée à M.

4. Décrire les classes d'isomorphisme de groupes abéliens du même ordre que $\mathbb{Z}^3/M$.