Université Claude Bernard Lyon 1

MASTER M1-G

Algèbre

EXAMEN

10 Janvier 2014

Durée : 3 heures

Toute preuve devra être axée sur un raisonnement clair, s'appuyant éventuellement sur des résultats du cours, énoncés avec précision. Tout argument d'autorité, comme "on a vu en TD que" ou "j'ai croisé Serre dans l'ascenseur et il m'a confirmé que" ne sera pas pris en compte.

Problème 1

On propose de montrer que si les entiers x, y vérifient

$$y^2 + 1 = x^3,$$

alors $(x, y) = (1, 0)$.

On veut donc résoudre sur l'anneau $\mathbb{Z}[i]$ l'équation

$$x^3 = (y + i)(y - i).$$

On rappelle que $\mathbb{Z}[i]$ est muni de la norme multiplicative N donnée par $N(a + ib) = a^2 + b^2$, $a, b \in \mathbb{R}$.

A. Préliminaires.

Nous allons commencer par montrer (rappeler ?) quelques propriétés de $\mathbb{Z}[i]$

1. *Question de cours.* Montrer que $\mathbb{Z}[i]$ est un anneau euclidien.
2. Montrer qu'un élément de $a + ib \in \mathbb{Z}[i]$ est inversible si et seulement si $a^2 + b^2 = 1$.
3. En déduire que les inversibles de $\mathbb{Z}[i]$ sont des cubes de $\mathbb{Z}[i]$.
4. On se donne z, $z' \in \mathbb{Z}[i]$, premiers entre eux. Montrer que si zz' est un cube de $\mathbb{Z}[i]$, alors, z et z' sont également des cubes de $\mathbb{Z}[i]$.
   On pourra citer, avec précision, un lemme du cours.

B. Réduction du problème.

On va voir ici qu'il suffit de prouver que $(y + i)$ est un cube de $\mathbb{Z}[i]$ pour obtenir la solution demandée.

1. On suppose $y + i = (m + ni)^3$, avec m, $n \in \mathbb{Z}$. Montrer que $n = -1$.
2. En déduire que l'ensemble de solutions est bien égal à $\{(1, 0)\}$.

A partir de là, on suppose que x et y sont deux entiers vérifiant $y^2 + 1 = x^3$.

C. Cas où y est pair.

Le but de cette section est de montrer que si y est pair, alors $(y + i)$ est bien un cube. On suppose donc que y est pair et que $d \in \mathbb{Z}[i]$ divise $(y + i)$ et $(y - i)$.

1. Montrer que $N(d)$ divise 4 et $y^2 + 1$ dans $\mathbb{N}$.

2. En déduire que d est inversible.
3. Conclure alors que $(y+i)$ est un cube.

D. Cas où y est impair.

Le but de cette section est de montrer que si y est impair, alors $(y+i)$ est un cube. On suppose donc que y est impair et que $d \in \mathbb{Z}[i]$ divise $(y+i)$ et $(y-i)$.

1. Montrer que $N(d)$ divise 2 et en déduire que $d = 1$ ou $1+i$ modulo les inversibles de $\mathbb{Z}[i]$.
2. On suppose ici que $(1+i)$ divise $y+i$ dans $\mathbb{Z}[i]$ et on pose $Z := \frac{y+i}{1+i} \in \mathbb{Z}[i]$.
   (a) Montrer que Z et $\overline{Z}$ sont premiers entre eux.
   (b) Montrer que $X := \frac{x}{2}$ est entier et que $Z\overline{Z} = 4X^3$.
   (c) Déduire une contradiction.
3. Conclure que si y est impair, alors $(y+i)$ est un cube.

Problème 2

Soit q une puissance d'un nombre premier. Pour tout entier positif n, on note $\mathcal{P}_n$ l'ensemble des polynômes irréductibles unitaires de degré n sur $\mathbb{F}_q$ et p_n le cardinal de $\mathcal{P}_n$. Le but du problème est de calculer p_n pour tout n et de fournir quelques applications de ce calcul.

A. Factorisation de $X^{q^n} - X$ sur $\mathbb{F}_q$.

Le but de cette première section est de factoriser $X^{q^n} - X$ en facteurs irréductibles sur $\mathbb{F}_q$.

1. Soit $P \in \mathcal{P}_d$ un facteur irréductible de degré d de $X^{q^n} - X$. Montrer que si α est une racine de P, dans une extension de $\mathbb{F}_q$, alors $\alpha \in \mathbb{F}_{q^n}$. En déduire que d divise n.
2. Réciproquement, soit $P \in \mathcal{P}_d$, avec d divise n. On veut montrer que P divise $X^{q^n} - X$.
   (a) Soit α une racine de P, dans une extension de $\mathbb{F}_q$. Montrer que P est le polynôme minimal annulant α sur $\mathbb{F}_q$.
   (b) En déduire que P divise $X^{q^n} - X$.
3. Montrer que $X^{q^n} - X$ n'a que des racines simples, puis, en déduire la factorisation

$$X^{q^n} - X = \prod_{d|n} \prod_{P \in \mathcal{P}_d} P.$$

B. Etude de la suite p_n.

1. On pose $u_n = np_n$ pour tout n. Montrer les égalités

$$(*) \sum_{d|n} u_d = q^n,\ u_1 = q.$$

2. On fixe un entier naturel n. On note $\mathcal{S}$ l'ensemble des entiers positifs non nuls, possédant, pour tout p, une p-valuation égale à 0 ou 1 (donc l'ensemble des éléments de $\mathbb{N}^*$ n'ayant pas de multiplicité dans leur décomposition en facteurs premiers). On note $D_n := \{d \in \mathcal{S}, d \text{ divise } n\}$. On note également $D_{n,k}$ l'ensemble des éléments de D_n possédant k diviseurs premiers et soit $\nu(n)$ le nombre de diviseurs premiers de n.

   Montrer que le cardinal de $D_{n,k}$ est égal au nombre binomial $\binom{\nu(n)}{k}$.

3. On pose
$$v_n = \sum_{0\leq k\leq \nu(n)} \sum_{d\in D_{n,k}} (-1)^k q^{\frac{n}{d}}.$$
Montrer que $u_n = v_n$ pour tout n.
On pourra montrer que v_n vérifie (*), en calculant le terme en q^d dans $\sum_{d|n} u_d$. On pourra utiliser la formule $\sum_{0\leq k\leq \nu(n)}(-1)^k\binom{\nu(n)}{k} = 0$, pour $\nu(n) > 0$.

C. Propriétés de la suite (p_n).

1. Montrer l'inégalité $1 + q + \cdots + q^{n-1} < q^n$ et en déduire que pour tout n, $p_n \neq 0$.
2. Montrer que les suites p_n et $\frac{1}{n}q^n$ sont équivalentes quand n tend vers l'infini.

D. Applications.

1. Montrer qu'il existe α dans $\mathbb{F}_{q^n}$ tel que $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha]$.
2. Montrer que pour tout n, il existe une extension de $\mathbb{Q}$ de degré n.

E. Une famille d'exemples pour les survivors.

Soit p un nombre premier. On va construire une famille de polynômes irréductibles sur $\mathbb{Q}$, de degré p. On pose
$$Q_p := X^p - X - 1 \in \mathbb{Z}[X]$$

1. On considère la réduction $\overline{Q}_p \in \mathbb{F}_p[X]$ modulo p.
   (a) Soit $R \in \mathbb{F}_p[X]$ un facteur irréductible de $\overline{Q}_p$ et α une racine de R. Montrer, à l'aide du Frobenius, que $\alpha + 1$ est racine de R.
   (b) En déduire que $\overline{Q}_p$ est irréductible.
2. En déduire que Q_p est un polynôme irréductible sur $\mathbb{Q}$.