Université Claude Bernard Lyon 1

MASTER M1-G

Algèbre

CORRECTION DE L'EXAMEN

Problème 1

A. Préliminaires.

1. Voir le cours.
2. Voir le cours.
3. Les inversibles de $\mathbb{Z}[i]$ sont les éléments $a+bi$ tels que $a^2+b^2=1$. On trouve donc, $1=1^3$, $i=(-i)^3$, $-1=(-1)^3$, $-i=i^3$.
4. Le lemme du cours dit que, dans un anneau factoriel, si z et z' sont premiers entre eux, et zz' est un cube, alors z et z' sont des cubes modulo un élément inversible. Comme $\mathbb{Z}[i]$ est euclidien, il est factoriel, et comme tous ses inversibles sont des cubes, z et z' sont des cubes.

B. Réduction du problème.

1. On a $y+i=(m+ni)^3=m^3-3mn^2+i(3m^2n-n^3)$. Donc, par identification, $y=m(m^2-3n^2)$ et $1=n(3m^2-n^2)$. La seconde égalité dit que n divise 1, donc $n=\pm 1$.
2. Si $n=1$, alors $3m^2-1^2=1$, et donc m n'est pas entier. Si $n=-1$, alors $m=0$, et on obtient bien $y=0$ et $x=1$.

C. Cas où y est impair.

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

1. Si d divise $(y+i)$ et $(y-i)$, alors d divise $2i$ et $(y+i)$. Comme N est multiplicative, à valeur dans $\mathbb{N}$, il vient que $N(d)$ divise $N(2i)=4$ et $N(y+i)=y^2+1$ dans $\mathbb{N}$.
2. Comme $N(d)$ divise une puissance de 2, $N(d)$ vaut 1 ou est pair. Or, $N(d)$ divisey^2+1, qui est impair. Donc, $N(d)=1$ et d est inversible.
3. On a montré que $(y+i)$ et $(y-i)$ étaient premiers entre eux et donc $(y+i)$ est un cube, par la partie A.

D. Cas où y est impair.

1. On a comme ci-dessus $N(d)$ divise $N(2i)=4$ et $N(y+i)=y^2+1$. Or, y étant impair, y est congru à ± 1 modulo 4, donc, y^2+1 est congru à 2 modulo 4. Conclusion, $N(d)$ divise 2. Si $N(d)=2$, avec $d=a^2+b^2$, alors $a^2+b^2=2$ implique que $a,b=\pm 1$, donc $d=1+i$ modulo les inversibles. Si $N(d)=1$, alors d est inversible.
2. (a) Soit e dans $\mathbb{Z}[i]$ divisant Z et $\overline{Z}$. On note que $-i\overline{Z}(1+i)=\overline{Z}(1-i)=y-i$. Alors, $e(1+i)$ divise $y+i$ et $y-i$. Donc, $N(e(1+i))$ divise 2 par ce qui précède. Donc $N(e)=1$ et e est inversible.

   (b) Comme y est impair et $y^2+1=x^3$, il vient que x^3 est pair, donc, x est pair. De plus, $Z\overline{Z}=\frac{(y+i)(y-i)}{(1+i)(1-i)}=x^3/2=4X^3$.

(c) On a donc que $1+i$ divise le membre de droite et donc le membre de gauche. Or, $1+i$ est irréductible (et non inversible) puisque sa norme l'est dans $\mathbb{Z}$. Dans l'anneau factoriel (puisque euclidien) $\mathbb{Z}[i]$, cela veut dire que $1+i$ est premier. Il divise donc, soit Z, soit $\overline{Z}$. Supposons qu'il divise Z, alors $1-i$ divise $\overline{Z}$, et donc $1+i$ divise $\overline{Z}$. En contradiction avec le fait que Z et $\overline{Z}$ sont premiers entre eux.

3. Si y est impair, alors c'est impossible.

Problème 2

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

1. Si α est une racine de P alors α est aussi une racine de $X^{q^n}-X$ et donc, $\alpha \in \mathbb{F}_{q^n}$.
   Or, comme P est irréductible de degré d, on sait que $\mathbb{F}_q[alpha]$, le corps de rupture de P sur $\mathbb{F}_q$ est de degré d sur $\mathbb{F}_q$. Par unicité, on sait que $\mathbb{F}_q[alpha] = \mathbb{F}_{q^d}$. Donc, d'après ce qui précède, $\mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$, ce qui implique que d divise n.
2. (a) Comme P annule α, il est multiple du polynôme minimal de α et comme P est irréductible, on a égalité.
   (b) Comme α est dans $\mathbb{F}_{q^d}$ et que d divise n, il vient que $\alpha \in \mathbb{F}_{q^n}$. Donc, $X^{q^n}-X$ annule α et ainsi, P, le polynôme minimal de α, divise $X^{q^n}-X$.
3. Posons $Q = X^{q^n}-X$. Si β est une racine multiple de Q, alors β annule Q et $Q' = -1$. Absurde car $-1 \neq 0$. Donc, Q n'a que des racines simples.
   Comme $\mathbb{F}_q[X]$ est factoriel, Q se décompose en $a\prod P_i^{n_i}$, avec P_i irréductibles distincts et a dans $\mathbb{F}_q^*$. Comme Q n'a que des racines simples, on a $n_i = 1$. D'après les questions précédante, les P_i sont exactement les polynômes de $\mathcal{P}_d$, avec d divise n. Et comme tous les polynômes en présence sont unitaires, on a $a = 1$. D'où la factorisation demandée.

B. Etude de la suite p_n.

1. Les polynômes unitaires de $\mathbb{F}_q[X]$ de degré 1 sont de la forme $X-a$, $a \in \mathbb{F}_q$ sont tous irréductibles. Donc,$p_1 = q$. L'égalité $\sum_{d|n} dp_d = q^n$ provient de l'égalité des degrés dans la factorisation précédente.
2. Si on pose p_i, $1 \leq i \leq \nu(n)$, les nombres premiers qui divisent n, on a $D_{n,k} = \{p_{i_1}\cdots p_{i_k},\ 1 \leq i_1 < \cdots < i_k \leq \nu(n)\}$. Par unicité de la décomposition en facteurs premiers, le cardinal de $D_{n,k}$ est égal à $\binom{\nu(n)}{k}$.
3. On pose $v_n = \sum_{0\leq k\leq \nu(n)} \sum_{d\in D_{n,k}} (-1)^k q^{\frac{n}{d}}$. Calculons $r_n := \sum_{d|n} v_d$. Notons que r_n est une somme de puissances de q divisant n. Le coefficient en q^n est 1. Pour tout d divisant n, le terme en q^d provient du développement des $v_{d'}$, avec d' divisant n, tels que $\frac{d'}{d} \in \mathcal{S}$. Si $\frac{d'}{d} \in \mathcal{S}_k$, le terme en q^d dans $v_{d'}$ est $(-1)^k$. Donc, le terme en q^d dans r^n vaut $\sum_{0\leq k\leq \nu(n/d)} (-1)^k \binom{\nu(n/d)}{k} = 0$, si $d \neq n$ et 1 si $d = n$. Conclusion, $r_n = q^n$. Comme $r_1 = v_1 = q$. On a bien que les suites v_n et u_n suivent les mêmes récurrences. Donc,

$$np_n = u_n = v_n = \sum_{0\leq k\leq m} \sum_{d\in D_{n,k}} (-1)^k q^{\frac{n}{d}}.$$

C. Propriétés de la suite (p_n).

1. La formule de la série géométrique donne $1+q+\cdots+q^{n-1} = \frac{q^n-1}{q-1} \leq q^n - 1 < q^n$. On a donc, pour tout n, $u_n \geq q^n - (q^{n-1}+\cdots+q+1) > 0$. Donc, $p_n = \frac{u_n}{n} > 0$.

2. On a $|q^{-n}u_n - 1| \leq |q^{-n}\sum_{0<k\leq m}\sum_{d\in D_{n,k}}(-1)^k q^{\frac{n}{d}}| \leq q^{-n} + \cdots + q^{-E(\frac{n}{2})}$. Par la formule de la série géométrique, celle-ci tend vers 0. Conclusion, p_n et $\frac{1}{n}q^n$ sont équivalentes quand n tend vers l'infini.

D. Applications.

1. D'après C, p_n est non nul, donc, il existe un polynôme irréductible P de degré n sur $\mathbb{F}_q$. Le corps de rupture $\mathbb{K}$ de P sur $\mathbb{F}_q$ est donc de degré n. On a donc un α tel que $\mathbb{F}_q[\alpha] = \mathbb{K} = \mathbb{F}_{q^n}$, puisque $\mathbb{K}$ est de degré n sur $\mathbb{F}_q$. Par construction, $\alpha \in \mathbb{F}_{q^n}$.
2. Soit $q = p$ un nombre premier. On sait donc qu'il existe un polynôme unitaire irréductible de degré n dans $\mathbb{F}_p[X]$. On peut le relever en un polynôme P unitaire de $\mathbb{Z}[X]$ de degré n. Comme P est irréductible modulo p, il est irréductible sur $\mathbb{Z}$. Comme P est irréductible sur $\mathbb{Z}$ factoriel, il est irréductible sur $\mathbb{Q}$. Le corps de rupture de P constitue donc une extension de $\mathbb{Q}$ de degré n.

   Ah ? On peut aussi faire ça avec le critère d'Eisenstein puisque $X^n - 2$ est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$. Ok...

D. Une famille d'exemples pour les survivors.

1. (a) Puisque α est une racine de R, c'est aussi une racine de $X^p - X - 1$. Donc, $Fr(\alpha) = \alpha^p = \alpha + 1$, où Fr désigne l'automorphisme de Frobenius.
   De plus, comme $R = \sum_i a_i X^i$ est à coefficients dans $\mathbb{F}^p$, on a $\sum_i a_i\alpha^i = 0$ implique

$$\sum_i a_i Fr(\alpha)^i = \sum_i Fr(a_i)Fr(\alpha^i) = Fr(\sum_i a_i\alpha^i) = 0.$$

   Ce qui prouve que $\alpha + 1$ est encore racine de R.

   (b) Donc, $\alpha + 1, \alpha + 2, \ldots, \alpha + p - 1$ sont encore des racines de R. De plus, ces racines sont distinctes, puisque les $1, 2, \ldots, p - 1$ sont distincts. Donc, R possède au moins p racines distinctes, il est de degré $\geq p$. Comme R divise $\overline{Q}_p$, il lui est égal et donc $\overline{Q}_p$ est irréductible.
2. Si Q_p se réduisait sur $\mathbb{Z}$, on aurait $Q_p = ST$ avec S et T dans $\mathbb{Z}$, donc unitaires de degré > 0. On aurait alors $\overline{Q}_p = \overline{ST}$. Avec $\overline{S}$ et $\overline{T}$ unitaires de même degré, respectivement que S et T, donc non inversibles. Ce qui est en contradiction avec le fait que $\overline{Q}_p$ est irréductible. Conclusion, Q_p est irréductible sur $\mathbb{Z}$, et comme $\mathbb{Z}$ est factoriel, il est irréductible sur $\mathbb{Q}$.