Université Claude Bernard Lyon 1

MASTER M1 Recherche

M1-Algèbre

EXAMEN Du 5/01/12-Correction

EXERCICE.

On se propose de montrer que la seule solution entière de l'équation $y^2 = x^3 - 1$ est $(x, y) = (1, 0)$.
1) Voir le cours.
2) Si x était pair alors modulo 4 on aurait $y^2 = -1$. Or, -1 n'est pas un carré de $\mathbb{Z}/4\mathbb{Z}$. Donc x est impair et modulo 2, on a $y^2 = 1$, donc $y = 1$ modulo 2 et ainsi, y est impair.
3) On a dans $\mathbb{Z}[i]$ que $(y+i)(y-i) = x^3$. Or $\mathbb{Z}[i]$ est factoriel car euclidien, donc on peut parler de pgcd de $y+i$ et $y-i$. Montrons que celui ci vaut 1. Supposons par l'absurde d premier divisant $y+i$ et $y-i$, alors il diviserait leur différence $2i$. Donc, sa norme $N(d)$ diviserait $N(2i) = 4$ dans $\mathbb{Z}$. Donc $N(d) = 2$ ou 4 puisque $N(d)$ ne peut être égal à 1, sinon, d'après le cours d serait inversible dans $\mathbb{Z}[i]$, ce qui contredirait le fait qu'il soit premier. De plus, $N(d) = 2$ a pour solutions entière $\pm 1 + \pm i$ qui sont irréductible car de norme première et $N(d) = 4$ a pour solutions 2, $2i$, -2, $-2i$ qui sont réductible car $2 = (1+i)(1-i)$. Donc $d = 1+i$ à inversible près. Ceci implique que $y + i = (1+i)(a+bi)$ avec a, b dans $\mathbb{Z}$ donc $y = a - b$ et $1 = a + b$ et donc $y + 1 = 2a$ ce qui implique y impair, contradiction. Ainsi, la factorialité de $\mathbb{Z}[i]$ implique que $y + i$ est un cube modulo les inversibles qui sont eux-mêmes des cubes. D'où l'assertion.
4) On a donc $y + i = (a + bi)^3$. Donc $y = a^3 - 3ab^2$ et $1 = 3a^2b - b^3 = b(3a^2 - b^2)$. La seconde égalité montre que b divise 1 dans $\mathbb{Z}$ et donc que $b = \pm 1$. Cela donne aussi que $3a^2 - b^2 = \pm 1$. Finalement, on obtient successivement que $a = 0$, $y = 0$ puis que $x = 1$.

PROBLEME.

Soit k un corps et $P_n = X^n - 1$ pour $n \in \mathbb{N}^*$. On suppose que k est de caractéristique nulle ou de caractéristique p ne divisant pas n.

Préliminaires.

1) le produit de racines n-ièmes est clairement une racine n-ième car $(ab)^n = a^n b^n$.
2) Soit α une racine double de P_n. Alors, $P_n(\alpha) = P_n'(\alpha) = 0$, un petit calcul montre que c'est impossible. On a donc n racines de l'unités bien distinctes. Ainsi, U_n est un groupe abélien à n éléments. Soit k son exposant, alors k divise n et $x^k - 1$ possède au moins n solutions sur le corps K_n. On en déduit que $k \geq n$ et donc $k = n$. Donc, U_n possède un élément d'ordre n. C'est alors un générateur de U_n. D'où l'assertion.

Tout sous-groupe d'un groupe cyclique est lui-même cyclique. Donc, $U_n(k) \simeq \mathbb{Z}/d\mathbb{Z}$ avec d divise n.
3) Par définition, ζ est racine primitive n-ième de l'unité si et seulement si ζ est d'ordre n et donc si et seulement si ζ engendre le groupe $U_n(K_n)$, puisque celui-ci est d'ordre n.
4) Le degré de $\phi_n(X)$ est égal au nombre de générateurs de $\mathbb{Z}/n\mathbb{Z}$ et donc, c'est $\varphi(n)$. La formule $n = \sum_{d|n} \varphi(d)$ est juste l'égalité des degrés dans la formule (*).

A.
1) $\phi_8\phi_4\phi_2\phi_1 = X^8-1$ et $\phi_4\phi_2\phi_1 = X^4-1$ d'après (*). Il en résulte que $\phi_8 = X^4+1$.
2) Par récurrence, on montre que ϕ_n est entier et unitaire. Cela provient de (*) et du fait que si B divise A dans $\mathbb{C}[X]$ avec B, A unitaires dans $\mathbb{Z}[X]$, alors B divise A dans $\mathbb{Z}[X]$ (ce qui résulte directement de la division euclidienne des polynômes). En réduisant (*) modulo p (ce que l'on est en droit de faire puisque tous les polynômes sont entiers), on obtient

$$\overline{X^n - 1} = \prod_{d|n} \bar{\phi}_d(X). \quad (*)$$

sur $\mathbb{F}_p$. Or, le polynôme $X^n - 1$ est sans multiplicité sur $\mathbb{F}_p$ d'après les préliminaires. Donc, les racines de $\bar{\phi}_n$ sont exactement les éléments d'ordre n (les racines n-ièmes qui ne sont pas racines d-ièmes pour d divise strictement n). Donc, c'est égal à $\phi_{n,\mathbb{F}_p}$.
3) Via l'isomorphisme entre U_n et $\mathbb{Z}/n\mathbb{Z}$, cela revient à dire que si a est un générateur de $\mathbb{Z}/n\mathbb{Z}$ alors pa est encore un générateur, ou encore dit autrement, si a et p sont premiers avec n alors ap est premier avec n. Ceci est clair.
4)a) Le polynôme ϕ_n annule ζ donc, le polynôme minimal P de ζ divise ϕ_n. P est donc un facteur irréductible de ϕ_n dans $\mathbb{Q}[X]$. Or, ϕ_n est dans $\mathbb{Z}[X]$ qui est factoriel, donc ϕ_n se décompose en $a\prod_i P_i$ avec P_i irréductible de $\mathbb{Z}[X]$, $a \in \mathbb{Z}$. Comme ϕ_n est unitaire, on a $a = 1$ (on peut utiliser le contenu pour s'en assurer). Par unicité de la décomposition en irréductibles dans $\mathbb{Q}[X]$, on a $P = P_i$ pour un i de P et donc P est dans $\mathbb{Z}[X]$. Idem pour Q.
b) On sait que ζ annule $Q(X^p)$, donc $P(X)$ divise $Q(X^p)$ dans $\mathbb{Q}[X]$. Comme ils sont tous deux unitaires dans $\mathbb{Z}[X]$, on a aussi la divisibilité dans $\mathbb{Z}[X]$.
c) On a $P(X) = R(X)Q(X^p)$ dans $\mathbb{Z}[X]$ donc modulo p, $\bar{P}(X) = \bar{R}(X)\bar{Q}(X^p) = \bar{R}(X)\bar{Q}(X)^p$.
d) $\bar{\phi}_n$ est divisible par $\bar{P}$ et possède donc des racines d'ordre p par ce qui précède. C'est impossible d'après les préliminaires car p ne divise pas n. D'où la contradiction. Il vient que $P = Q$.
5) On a $m = \prod_i p_i$ avec p_i premiers qui ne divisent pas n. Donc si ζ est racine de P, on a vu que ζ^{p_i} est racine de $Q = P$, donc par récurrence, on a que ζ^m est encore racine de P.
Supposons donc que $\phi_n = PR$ et ζ une racine de P. Soit ζ' une autre racine de ϕ_n. Il vient que ζ, ζ' sont des racines primitives $n$iemes de l'unité et donc $\zeta' = \zeta^m$

avec m premier avec n. On en déduit que ζ' est racine de P. Donc, P et ϕ_n sont unitaires et ont les mêmes racines. Ils sont égaux et ainsi, ϕ_n est irréductible dans $\mathbb{Z}[X]$.

B.

1) Soit m l'ordre de p dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$. On a donc n divise $p^m - 1$ et ainsi $\zeta^{p^m-1} - 1 = \zeta^{nk} - 1 = 1 - 1 = 0$. Or, $X^n - 1$ ne possède que des racines simples, donc se décompose en facteurs $(X - \zeta)$ tous premiers entre eux. Comme chaque $(X - \zeta)$ divise $X^{p^m-1} - 1$, leur produit $X^n - 1$ le divise aussi.

2) D'après ce qui précède, on a $\zeta^{p^m} - \zeta = 0$, donc $\zeta \in \mathbb{F}_{p^m}$.

Supposons maintenant par l'absurde $\zeta^{p^r} = \zeta^{p^{r'}}$, $0 \leq r < r' \leq m - 1$. Alors, on aurait $\zeta^{p^{r'}-p^r} = 1$, donc ζ étant d'ordre n, on a n divise $p^{r'} - p^r = p^r(p^{r'-r} - 1)$. Comme n est premier avec p, le lemme de Gauss implique que n divise $p^{r'-r} - 1$ et donc $p^{r'-r} = 1$ modulo n. Ce qui est impossible car m est l'ordre de p modulo n et $0 < r' - r < m$. Donc ils sont distincts.

3) Les coefficients de P sont au signe près de la forme $\alpha_r = \sum_{\{i_1,\ldots,i_r\}} a_{i_1} \ldots a_{i_r}$, avec $a_i = \zeta^{p^i}$. Etant donné que $a_i^p = a_{i+1}$ (où i est vu modulo m, on obtient bien en utilisant le morphisme de Frobenius que $\alpha_r^p = \alpha_r$ et donc que $\alpha_r \in \mathbb{F}_p$. Donc P est un polynôme de $\mathbb{F}_p[X]$.

4) Si ζ est racine de Q, alors $Q(\zeta) = 0$, donc, $Q(\zeta^p) = Q(\zeta)^p = 0$, car $Q \in \mathbb{F}_p[X]$. On montre alors comme dans A5) que P est irréductible.

5) Soit ζ une racine de $\phi_{n,\mathbb{F}_p}$ et soit P son polynôme minimal sur $\mathbb{F}_p$. Alors P est irréductible et donc $P := \prod_{r=0}^{m-1}(X - \zeta^{p^r})$ par unicité d'un polynôme irréductible annulant ζ sur $\mathbb{F}_p$. Donc, tout facteur irréductible de $\phi_{n,\mathbb{F}_p}$ est de degré m. Ainsi $\phi_{n,\mathbb{F}_p}$ se décompose en $\varphi(n)/m$ facteurs irréductibles distincts.

6) Le polynôme ϕ_8 se décompose en $\varphi(8)/m = 4/m$ facteurs est réductible modulo p pour tout p premier. Or, $(\mathbb{Z}/8\mathbb{Z})^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et donc l'ordre m de p est inférieur à 2. Ceci implique que ϕ_8, qui est irréductible sur $\mathbb{Z}$, ne l'est plus modulo p pour tout p.