M1-Algèbre Correction Examen 2013

EXERCICE.

1) On sait que si P est irréductible sur $\mathbb{Z}[X]$ alors, il l'est sur $\mathbb{Q}[X]$ car $\mathbb{Z}$ est factoriel.
2) Pour montrer que l'application $Q \mapsto \overline{Q}_p$ définit un morphisme d'anneaux entre $\mathbb{Z}[X]$ et $\mathbb{F}_p[X]$, il suffit de voir qu'elle est compatible : $\overline{a_k + b_k} = \overline{a}_k + \overline{b}_k$, et compatible avec la multiplication $\overline{\sum_i a_i b_{k-i}} = \sum_i \overline{a}_i \overline{b}_{k-i}$. Ces deux égalités sont clairement vérifiées.

On en déduit la seconde assertion par la contraposée. Supposons que Q se réduise sur $\mathbb{Z}$, on a donc $Q = ST$, où S et T sont deux polynômes de degré non nul. Comme Q est unitaire, on peut supposer que S et T le sont. Il vient donc $\overline{Q}_p = \overline{ST}_p = \overline{S}_p \overline{T}_p$. Et comme S et T sont non constants et unitaires, il en est de même de $\overline{S}_p$ et de $\overline{T}_p$. Donc, $\overline{Q}_p$ se réduit.

3) Comme $X^3 - X - 1$ est de degré 3, pour montrer qu'il est irréductible sur $\mathbb{F}_3[X]$, il suffit de montrer qu'il n'a pas de racines dans $\mathbb{F}_3$. C'est clair !
4) Soit K le corps de décomposition du polynôme $X^4 + X + 1 \in \mathbb{F}_2[X]$ et $\alpha \in K$ une racine de ce polynôme.
a) Le polynôme X^4+X+1 n'a pas de racines dans $\mathbb{F}_2$. Il est donc soit irréductible, soit il se décompose en deux facteurs de degré 2. Dans le premier cas $\alpha \in \mathbb{F}_{16}$ puisque $\mathbb{F}_{16}$ est l'unique extension de degré 4 de $\mathbb{F}_2$, soit il est dans $\mathbb{F}_4$. Dans les deux cas, il se trouve dans $\mathbb{F}_{16}$.

Supposons que α soit dans $\mathbb{F}_4$, alors il vérifierait $\alpha^4 = \alpha$ et comme il annule déjà $X^4 + X + 1$, cela donnerait $2\alpha + 1 = 0$ donc $1 = 0$, absurde ! Donc $\alpha \notin \mathbb{F}_4$.
b) D'après l'étude faite dans le a), $X^4 + X + 1$ est irréductible dans $\mathbb{F}_2[X]$.
5) $\overline{P}_3 = (X^3 - X - 1)^3$ grâce au Frobenius. De plus, comme 1 est racine de $\overline{P}_2$, on peut factoriser $(X + 1)$ (on est en caractéristique 2 donc $+ = -$) et on trouve $\overline{P}_2 = (X + 1)(X^8 + X^2 + 1) = (X + 1)(X^4 + X + 1)^2$ encore grâce au Frobenius. Comme l'ensemble des degrés des polynômes irréductibles dans la décomposition P forme une partition de 9, cherchons cette partition. Si on note $P = \prod_i P_i$ la décomposition en irréductibles on a $\overline{P} = \prod_i \overline{P}_i$, mais les $\overline{P}_i$ (qui ne sont pas nécessairement irréductibles se décomposent en facteurs irréductibles sur l'anneau factoriel $\mathbb{F}_p[X]$. Donc, la partition associée est un raffinement de la partition des degrés des P_i. Comme $\overline{P}_3 = (X^3 - X - 1)^3$, on en déduit que la partition de P est raffinée par $3+3+3$, donc il s'agit forcément de 9 ou de $6+3$ ou de $3+3+3$. Mais de deux dernières ne peuvent se raffiner en $1 + 4 + 4$ qui est prévue par la réduction modulo 2. Donc la partition est 9, ce qui donne que P est irréductible sur $\mathbb{Z}$ donc sur $\mathbb{Q}$.

PROBLEME.

A.
1) Les carrés de $\mathbb{Z}/4\mathbb{Z}$ sont 0 et 1.
2) Soit p premier impair, $p = a^2 + b^2$, alors modulo 4, on voit que p vaut $0+0$ ou $0+1$ ou $1+1$, mais comme p est impair, il ne peut pas être congru ni à 0, ni à 2 modulo 4. Il est donc congru à 1 (on ne s'est pas servi du fait qu'il était premier).
3) Question de cours : montrer que l'anneau $\mathbb{Z}[i]$ des entiers de Gauss est principal. Voir le cours.
4) Si p premier est congru à 3 modulo 4 et si p se factorise dans $\mathbb{Z}[i]$, alors on pourrait trouver une décomposition $p = (a+ib)(a'+ib')$ avec $a+ib$ et $a'+ib'$ non unitaires et donc de norme différente de 1. En prenant la norme, on obtiendrait dans $\mathbb{Z}$ que $N(a+ib)$ diviserait strictement $N(p) = p^2$, et serait différente de 1. On aurait donc $a^2 + b^2 = p$ par élimination puisque, p étant premier, les seuls diviseurs de p^2 sont 1, p, et p^2. Ceci contredit la question 2). Donc, p est premier dans $\mathbb{Z}[i]$.
B. 1) Les p_i sont donc soit congrus à 1 modulo 4, soit $p_i = 2$. Dans le premier, le symbole de Legendre donne $(-1)^{(p-1)/2} = 1$ donc 1 est un carré. Dans le second cas $-1 = 1$ est un carré modulo 2.
2) Si on appelle φ le morphisme du lemme chinois de $\mathbb{Z}/n\mathbb{Z}$ vers $\prod \mathbb{Z}/p_i\mathbb{Z}$, les composantes de $varphi(-1)$ sont les classes de -1 modulo p_i et sont donc des carrés de b_i. On a donc $\varphi^{-1}((b_i)_i)^2 = \varphi^{-1}((b_i^2)_i) = \varphi^{-1}((-1)_i) = -1$. Et donc -1 est un carré dans $\mathbb{Z}/n\mathbb{Z}$.

On voit donc que les racines carrées de -1 dans $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les $(b_i)_i$ où b_i est une racine de -1 dans $\mathbb{Z}/p_i\mathbb{Z}$. Or, comme $\mathbb{Z}/p_i\mathbb{Z}$ est un corps, il y a au plus 2 racines carrées. Une racine double si $p_i = 2$ et deux racines sinon (car si b_i est racine, alors $-b_i$ l'est aussi et est distincte). Donc -1 possède 2^k racines si n est impair et 2^{k-1} sinon.
3) On voit sans problème que $P.u = P(\omega)u$, $P \in \mathbb{Z}[X]$ vérifie les conditions de module... Distributivité à gauche, à droite, pseudo-associativité, et pseudo-neutralité.
4) Comme (X^2+1) annule le module $\mathbb{Z}/n\mathbb{Z}$, par construction de ω, on a un module sur l'anneau quotient $\mathbb{Z}[X]/(X^2+1) \simeq \mathbb{Z}[i]$.

Ce module est engendré par $\overline{1}$ puisqu'il l'est déjà comme groupe.
C. Soit m un entier positif et ϕ un morphisme *injectif* de $\mathbb{Z}$-module de $\mathbb{Z}^m$ dans lui-même.
1) Soit M l'image de $\mathbb{Z}^m$ par ϕ. On sait qu'il existe une base $(e_1, \ldots, e_m)$ de $\mathbb{Z}^m$ et une base de M de la forme $(a_1e_1, \ldots, a_ke_k)$ avec $k \leq m$. Soit e'_i tels que $\phi(e'_i) = a_ie_i$ pour i de 1 à k.

Montrons que (e'_i) est libre. Toute combinaison nulle des e'_i donne par ϕ une combinaison nulle des a_ie_i or celle-ci est libre, donc les constantes de la combinaison sont toutes nulles.

Montrons que (e'_i) est génératrice. Soit u dans $\mathbb{Z}^m$. On a $\phi(u) = \sum_i \lambda_i(a_ie_i)$ par construction, pour des λ_i entiers. Soit $u' = \sum_i \lambda_i e'_i$. Alors, $\phi(u') = \phi(u)$ et

par injectivité, $u = u'$. Conclusion u se décompose dans (e'_i).

Prenons pour la base de départ (e'_i) et la base d'arrivée (e_i). La matrice de ϕ dans ces bases est diagonale, c'est la diagonale des a_i.

2) Le module quotient $\mathbb{Z}^m/\mathrm{Im}\phi$ est d'après le théorème de la base adaptée isomorphe à $\prod_i \mathbb{Z}/a_i\mathbb{Z}$. Il est donc de cardinal $|\prod_i a_i|$. Or un changement de base dans le module libre $\mathbb{Z}^m$ se fait à l'aide de matrices de passages de $\mathrm{GL}_m(\mathbb{Z})$, donc de determinant ± 1. Le determinant de ϕ ne dépend pas, en valeur absolue, des bases choisies donc $|\det(\phi)| = |\prod_i a_i| = \mathbb{Z}^m/\mathrm{Im}\phi$.

3) On considère le morphisme de $\mathbb{Z}[i]$-modules qui envoie $(s + it)$ dans $\mathbb{Z}[i]$ sur $(s + \omega t)$ dans $\mathbb{Z}/n\mathbb{Z}$. Il est bien sur surjectif et son noyau est un sous-module donc un idéal de $\mathbb{Z}[i]$. COmme cet anneau est principal, ce noyau est de la forme $(a + ib)\mathbb{Z}[i]$. On obtient donc une présentation de $\mathbb{Z}/n\mathbb{Z}$ comme $\mathbb{Z}[i]$-module.

4) Or $\mathbb{Z}[i]$ est un $\mathbb{Z}$-module de rang 2 (clairement isomorphe à $\mathbb{Z}^2$.

Donc, $\mathbb{Z}/n\mathbb{Z}$ est le quotient de $\mathbb{Z}^2$ par l'image de $\mathbb{Z}^2$ pour le morphisme ϕ correspondant à $\mathbb{Z}[i] \to \mathbb{Z}[i]$, $1 \mapsto a + ib$. dans la base canonique de $\mathbb{Z}^2$, ce morphisme a pour matrice

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Donc n qui est le cardinal de $\mathbb{Z}/n\mathbb{Z}$ est aussi le déterminant de cette matrice qui est égal à $a^2 + b^2$.

5) Si la p-valuation $\nu_p(n)$ est paire dès que p est un nombre premier congru à 3 modulo 4, alors n s'écrit $r^2.\prod p_i$, avec r entier et les p_i comme dans le B. Comme-1 est un carré modulo $\prod p_i$, il s'écrit comme somme de carrés d'entiers et donc n s'écrit également comme une somme de deux carrés d'entiers.

D.

1) On a vu qu'un nombre premier p reste premier dans $\mathbb{Z}[i]$ si p est congru à 3 modulo 4. On vient de voir que si p est soit 2 soit congru à 1 modulo 4, alors il s'écrit a^2+b^2, c'est à dire $(a+bi)(a-bi)$, avec bien sûr, $(a\pm bi)$ non unitaire puisque la norme vaut p. Donc p n'est pas premier et nous avons montré la réciproque par la contraposée.

2) Si p est premier, avec $p = a^2 + b^2$, alors $a + ib$ et $a - ib$ sont premiers dans $\mathbb{Z}[i]$: effectivement on a vu que dans ce cas $N(a \pm bi) = p$. Toute décomposition (stricte) de $(a + bi)$ dans $\mathbb{Z}[i]$ entrainerait une décomposition (stricte) de p dans $\mathbb{Z}$, ce qui est impossible.

3) Le nombre n se décompose sur $\mathbb{Z}$ en facteurs premiers, puis sur $\mathbb{Z}[i]$. D'après ce qui précède la décomposition en facteurs premiers de n dans $\mathbb{Z}[i]$ est de la forme $\prod_j p_j \prod_k (a_k + b_k i)$ avec les p_k congrus à 3 modulo 4. Or, $n = a^2 + b^2 = (a + bi)(a - bi)$. Si un p_k se trouve dans la factorisation précédente de n, alors comme p_k est premier, il divise $(a + bi)$ ou il $(a - bi)$. Mais, par conjugaison, s'il divise l'un, il divise l'autre. De même, on montre que si ν_k, resp. ν'_k, resp. ν''_k, est l'exposant de p_k dans la décomposition de n, resp. $(a + bi)$, resp. $(a - bi)$, alors $\nu'_k + \nu''_k = \nu_k$ et par conjugaison $\nu'_k = \nu''_k$. Ce qui prouve que ν_k est pair.