Université Claude Bernard Lyon 1

CORRECTION DE L'EXAMEN PARTIEL

M1-Algèbre 2016

Exercice 1. 1. Comme N est distingué, G agit par conjugaison sur N. Les orbites de cette action sont en bijection avec des ensembles de classes de la forme G/G_x où G_x est un sous-groupe de G. En conséquence, par Lagrange, le cardinal des orbites est une puissance de p, éventuellement $p^0 = 1$.

2. Un élément n de N est dans le centre de G si et seulement si $gn = ng$ pour tout g de G, c'est-à-dire, si et seulement si $gng^{-1} = n$, ce qui revient à dire que l'orbite de n est singletone. Dans la formule des classes, on regroupe donc toute ces orbites à un élément pour constituer le centre $Z(G) \cap N$. Il vient

$$|N| = |Z(G) \cap N| + \sum_n |\mathcal{O}_n|,$$

où n décrit un ensemble de représentants d'éléments d'orbites qui ne sont pas dans $Z(G)$. Il en résulte par ce qui précède que p divise $|Z(G) \cap N|$, puisque p divise $|N|$ (on rappelle que N est non trivial) et que p divise chaque $|\mathcal{O}_n|$. Donc, $Z(G) \cap N$ ne peut être réduit à l'élément neutre.

Exercice 2.

1. A est l'ensemble des $P(\alpha)$ quand P décrit $\mathbb{Z}[X]$. Or, $X^2 + 7$ étant unitaire, la division euclidienne de P par $X^2 + 7$ (dans l'anneau euclidien $\mathbb{Q}[X]$), reste dans $\mathbb{Z}[X]$. Il en résulte que l'on peut trouver des polynômes Q et R dans $\mathbb{Z}[X]$ tels que $P = (X^2 + 7)Q + R$, avec $R = bX + a$.

   Au final, $P(\alpha) = a + b\alpha$.

   Soit $z = a + b\alpha$, avec a, b entiers. Alors, $N(z) = a^2 + 7b^2$.

2. Soit u un inversible de A, et soit $u' = a' + b'\alpha$ son inverse. Alors $uu' = 1$ implique $N(u)N(u') = N(uu') = 1$. Comme $N(u)$ et $N(u')$ sont des entiers naturels, il vient alors que $N(u) = 1$.

   Ceci implique $a^2 + 7b^2 = 1$, et donc $b = 0$, ce qui implique $u = a = \pm 1$. Réciproquement, on vérifie que ± 1 sont inversibles.

3. On se ramène à trouver a et b entiers tels que $a^2 + 7b^2 = 4$. Il vient encore une fois $b = 0$ et donc $-2 \leq a \leq 2$. On trouve au final $\{-2, -1, 0, 1, 2\}$.

   On suppose que 2 s'écrit $2 = xy$, avec x, y non inversibles dans A. Alors, $N(x)$ et $N(y)$ sont distincts de 1 et $N(x)N(y) = N(2) = 4$. Ceci implique que $N(x) = 2$, ce qui est impossible dans A, d'après ce qui précède.

   De même, avec $N(1 \pm i\sqrt{7}) = 8$, on montre qu'une décomposition $1 \pm i\sqrt{7} = xy$ avec x, y non inversibles dans A impliquerait $N(x)$ ou $N(y)$ égal à 2, impossible. Ils sont donc tous irréductibles.

4. On a $2^3 = (1 - i\sqrt{7})(1 + i\sqrt{7})$. Or, $1 \pm i\sqrt{7}$ et 2 ne sont pas associés dans A, puisqu'ils n'ont pas même norme. On a donc deux décompositions distinctes en irréductible. Ainsi, A n'est pas factoriel.
5. On a A isomorphe à $\mathbb{Z}[X]/(X^2 + 7)$. Par les isomorphismes canoniques d'anneaux, on a d'une part
$$\mathbb{Z}[X]/(2, X^2 + 7) \simeq A/(2),$$
et d'autre part
$$\mathbb{Z}[X]/(2, X^2 + 7) \simeq \mathbb{F}_2[X]/(X^2 + 7) = \mathbb{F}_2[X]/(X^2 + 1).$$
Ceci nous donne l'isomorphisme demandé.
Si A était factoriel, alors 2, qui est irréductible, serait premier. Or, $A/(2)$ n'est pas intègre, puisque $\mathbb{F}_2[X]/(X^2+1)$ ne l'est pas. Effectivement, $X+1$ n'est pas nul dans $\mathbb{F}_2[X]/(X^2+1)$, alors que son carré $(X + 1)^2 = X^2 + 1 = 0$.
6. On pose $\beta = \frac{1+\alpha}{2}$. On a, en utilisant le polynôme annulateur unitaire $X^2 - X + 2$, que $\mathbb{Z}[\beta]$ est l'ensemble d'éléments de la forme $a + b\beta$. De plus, $N(a + b\beta) = a^2 + ab - 2b^2$.
Il en résulte que $z := x + y\beta$ dans $\mathbb{C}$ peut être approché par $a + b\beta$, avec $|x - a| \leq \frac{1}{2}$, $|y - b| \leq \frac{1}{2}$. Ceci donne
$$N(z - (a + b\beta)) = (x - a)^2 + (x - a)(y - b) + 2(y - b)^2.$$
Si $|x - a| < \frac{1}{2}$ ou $|y - b| < \frac{1}{2}$, alors $N(z) < 1$ et on sait construire alors un stathme euclidien avec la norme.
Sinon, on peut se ramener à $x - a = \frac{1}{2}$ et $y - b = -\frac{1}{2}$, et dans ce cas, quitte à remplacer a, resp. b, par $a + 1$ ou $a - 1$, resp. par $b + 1$ ou $b - 1$.
$$N(z - (a + b\beta)) = \frac{1}{4} - \frac{1}{4} + 2 \cdot \frac{1}{4} = \frac{1}{2} < 1.$$
On a donc bien un stathme.
7. L'anneau $\mathbb{Z}[\frac{1+\alpha}{2}]$ euclidien, donc principal, donc factoriel.

Exercice 3.

1. Comme $\mathbb{Z}$ est factoriel, tout polynôme irréductible sur $\mathbb{Z}$ l'est sur $\mathbb{Q}$.
2. (a) On note a_i, resp. b_i, les coefficients de P, resp. de Q. Alors , les coefficients de $P + Q$ sont $a_i + b_i$, et les coefficients de PQ sont les coefficients de $P + Q$ sont $\sum_{j+k=i} a_j b_k$. Comme $\overline{a_i + b_i} = \overline{a_i} + \overline{b_i}$, et $\overline{\sum_{j+k=i} a_j b_k} = \sum_{j+k=i} \overline{a_j}\overline{b_k}$, on a bien le morphisme annoncé.
   (b) Supposons par l'absurde, que Q ne soit pas irréductible sur $\mathbb{Z}[X]$. Alors, on peut trouver deux polynômes non constants S et T de $\mathbb{Z}[X]$, tels que $Q = ST$. Les polynôme S et T sont alors unitaires, et donc $\overline{S}_p$ et $\overline{T}_p$ sont non constants, donc non inversibles dans $\mathbb{F}_p[X]$. Donc, $\overline{Q}_p = \overline{S}_p\overline{T}_p$ (donné par le morphisme d'anneaux précédent) contredit l'irréductibilité de $\overline{Q}_p$.
3. Comme ce polynôme est de degré 3, il est irréductible sur $\mathbb{F}_3$ si et seulement s'il n'a pas de racine dans $\mathbb{F}_3$. Ce que l'on vérifie avec grâce et élégance sur les trois éléments de $\mathbb{F}_3$.

4. (a) On rappelle que toute extension de $\mathbb{F}_2$ est de caractéristique 2, et donc $-1 = 1$ dans toutes ces extensions.
   On a $\alpha^4 + \alpha + 1 = 0$. Il en résulte
   $$\alpha^{16} = (\alpha + 1)^4 = \alpha^4 + 1 = \alpha.$$
   Donc, $\alpha \in \mathbb{F}_{16}$.
   Supposons $\alpha \in \mathbb{F}_4$. Alors, $\alpha + 1 = \alpha^4 = \alpha$ et donc $1 = 0$, absurde. Donc, $\alpha \notin \mathbb{F}_4$.

   (b) Le polynôme $X^4 + X + 1$ n'a pas de racine dans $\mathbb{F}_2[X]$. De plus, si $X^4 + X + 1$ se décomposait en produit de polynômes irréductibles de degré 2, alors α serait dans une extension de degré 2 de $\mathbb{F}_2$, c'est-à-dire $\mathbb{F}_4$, par unicité des corps de cardinal donné, ce qui est impossible. Donc, il est irréductible.

5. On trouve facilement $\overline{P}_3 = (X^3 - X - 1)^3$, et $\overline{P}_2 = (X + 1)(X^4 + X + 1)^2$.
   Si P se décompose en polynômes irréducibles sur $\mathbb{Z}$, alors le degré 9 de P se décompose en une partition des degrés des polynômes irréductibles en présence. Ces polynômes irréductibles, unitaires, ont des degrés qui se scindent alors eux même en partitions des degrés de leur décomposition sur $\mathbb{F}_p$.
   Par exemple, la partition associée à $\overline{P}_3$ est $9 = 3 + 3 + 3$, et la partition associée à $\overline{P}_2$ est $9 = 4 + 4 + 1$. Ce sont donc deux raffinements de la partition associée à P. Or, au dessus de la partition $3 \geq 3 \geq 3$, il y a $6 \geq 3$ et 9. Au dessus de la partition $4 \geq 4 \geq 1$, il y a $8 \geq 1$, $5 \geq 4$, et 9. Le seul en commun possible est 9. Donc, P est irréductible sur $\mathbb{Z}$, et donc sur $\mathbb{Q}$.