Université de Cergy-Pontoise
Décembre 2011

Structures algébriques

Licence de Mathématiques, troisième année

Corrigé

Premier exercice 4 points

Soit σ la permutation donnée par

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 6 & 7 & 8 & 1 & 2 \end{pmatrix}$$

1. En cherchant les images successives, on trouve que σ est composé de deux 4-cycles :

   $$\sigma = (1, 3, 5, 7)(2, 4, 6, 8)$$

   Les 4-cycles sont de signature -1, donc sigma est de signature $+1$.

2. $\tau(2) = \tau \circ \tau(1) = \sigma(1) = 3$. On peut maintenant calculer $\tau(3) = \tau \circ \tau(2) = \sigma(2) = 4$, et ainsi de suite. On trouve que τ est le 8-cycle

   $$\tau = (1, 2, 3, 4, 5, 6, 7, 8)$$

   et il est immédiat que τ vérifie bien (1).

3. La même démarche conduit à $\tau(5) = \tau \circ \tau(1) = \sigma(1) = 3$. On peut maintenant calculer $\tau(3) = \tau \circ \tau(5) = \sigma(5) = 7$, puis $\tau(7) = \tau \circ \tau(3) = \sigma(3) = 5$ et il y a une contradiction, car 5 ne peut être à la fois l'image de 1 et de 3.

Second Exercice - 5 points

On rappelle que $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$. Soit $P = X^2 + \overline{1}$ polynôme de $\mathbb{F}_3[X]$.

1. Le polynôme $X^2 + \overline{1}$, s'il était réductible, serait produit de deux polynômes du premier degré. Il aurait donc au moins une racine dans $\mathbb{F}_3$. Or $P(0) = 1$, $P(1) = 2$ et $P(2) = P(-1) = 2$. Le polynôme P est bien irréductible.

2. Tout polynôme est congru modulo P à son reste dans la division euclidienne par P. Les restes distincts sont incongrus et il y a $3 \times 3 = 9$ polynômes du premier degré dans $\mathbb{F}_3[X]$. A a donc 9 éléments. De plus, $\mathbb{F}_3[X]$ est principal, donc tout polynôme irréductible engnedre un idéal maximal, le quotien est donc un corps.

3. Dans A, on a $\alpha^2 + 1 = 0$, donc $\alpha^2 = -1$. On en déduit $\alpha^3 = -\alpha$ et $\alpha^4 = 1$. L'ordre est donc 4.

4. Si $\beta = 1+\alpha$, $\beta^2 = 1+2\alpha+\alpha^2 = 2\alpha$, $\beta^3 = 2\alpha(\alpha+1) = 1+2\alpha$, $\beta^4 = (1+2\alpha)(1+\alpha) = 2 = -1$, $\beta^5 = 2+2\alpha$, $\beta^6 = \alpha$, $\beta^7 = 2+\alpha$ et $\beta^8 = 1$. L'ordre de β est donc 8. Comme A est un corps, G est formé de tous les éléments non nuls, il a 8 éléments. C'est donc un groupe cyclique dont β est un générateur.

   Remarque : en utilisant que G est de cardinal 87, compte-tenu du théorème de Lagrange, on aurait pu se contenter de calculer les puissances 2, 4 et 8.

Troisième Exercice - 5 points

On note B l'ensemble

$$B = \{z \in \mathbb{R} \mid \exists (a,b) \in \mathbb{Z}^2,\ z = a + b\sqrt{2}\}$$

1.
$$(a+b\sqrt{2}) + (a'+b'\sqrt{2}) = (a+a') + (b+b')\sqrt{2}$$
$$(a+b\sqrt{2}) \times (a'+b'\sqrt{2}) = (aa'+2bb') + (ab'+a'b)\sqrt{2}$$

   prouve que B est stable pour les opérations. De plus, B contient 1, c'est donc un sous-anneau de $\mathbb{R}$. L'écriture est unique car si $a+b\sqrt{2} = a'+b'\sqrt{2}$, si $b = b'$ alors $a = a'$ et si $b \neq b'$, on obtiendrait que $\sqrt{2}$ est rationnel.

2.
$$\begin{aligned} N(zz') = (aa'+2bb')^2 - 2(ab'+a'b)^2 &= a^2a'^2 + 4b^2b'^2 - 2a^2b'^2 - 2a'^2b^2 \\ &= (a^2-2b^2)(a'^2-2b'^2 \\ &= N(z)N(z'). \end{aligned}$$

   Il s'agit bien d'un morphisme multiplicatif et $N(z)$ est évidemment un élément de $\mathbb{Z}$.

3. Si $zz' = 1$, avec $(z,z') \in B$, alors $N(z)N(z') = N(1) = 1$. Donc $N(z)$ est un élément inversible de $\mathbb{Z}$ donc $N(z) = \pm 1$. Réciproquement, si $N(z) = \pm 1 = (a+b\sqrt{2})(a-b\sqrt{2}$, on vérifie bien que l'inverse de $a+b\sqrt{2}$ est $\pm(a-b\sqrt{2}$ qui est dans B.

4. $\omega = 1+\sqrt{2}$ a pour inverse $-1+\sqrt{2} = \omega^{-1}$. Toutes les puissances positives ω^n de *omega* sont également inversibles (d'inverses ω^{-n} et elles sont distinctes cer elles forment une suite (géométrique) strictement croissante. Il y a donc une infinité d'éléments inversibles. N.B. On peut montrer que les inversibles sont exactement les $\pm\omega^n$ où $n \in \mathbb{Z}$.

5. I contient $\sqrt{2} \times \sqrt{2} = 2$, par seconde propriété des idéaux. Il contient également tous les $b\sqrt{2}$, toujours par cette propriété. Il ne peut coïncider avec B tout entier, sion il existerait $z \in B$ tel que $z\sqrt{2} = 1$, et $\sqrt{2}$ serait inversible, ce qui n'est pas le cas ($N(\sqrt{2}) = 4$. Montrons que c'est un idéal maximal. Supposons $I \subsetneq J \subset B$ et soit $a \in J \setminus I$. Alors a n'est pas de la forme $2n+m\sqrt{2}$ (sinon il serait dans I, il est donc de la forme $2n+1+m\sqrt{2}$ et donc $1 = a-(2n+m\sqrt{2}$ est dans J, c'est-à-dire que $J = B$.

Quatrième Exercice

1. Montrons
$$\forall x \in \mathcal{N}(A),\ \forall a \in A,\ ax \in \mathcal{N}(A)$$
   En effet, sinon ax serait inversible d'inverse y et $axy = 1$ prouve que x est inversible.

2. Les non inversibles de $\mathbb{Z}/8\mathbb{Z}$ sont $0, 2, 4, 6,$, ils forment un idéal (idéal principal engendré par 2). Les non inversibles de $\mathbb{Z}/15\mathbb{Z}$ sont 0, 3, 5, 6, 9, 10, 12. Ils ne forment pas un idéal car, par exemple $3 + 5 = 8$ qui est inversible.
3. Il suffit de rappeler que si un idéal contient un inversible, il coïncide avec l'anneau tout entier.
4. C'est immédiat : $\mathcal{N}(A)$ contient tous les idéaux stricts de A. Si donc $\mathcal{N}(A) \subsetneq J \subset A$, où J est un idéeal, nécessairement $J = A$. De plus, tout idéal maximal I doit être inclus dans $\mathcal{N}(A)$ qui est un idéal... La seule possibilité est qu'il coïncide avec $\mathcal{N}(A)$.