Banque exos 5/2

Exercice 1 ⋆⋆ - Nilpotents *(1)*

On suppose que A est commutatif, et on fixe x, y deux éléments nilpotents.

1. *Montrer que xy est nilpotent.*
2. *Montrer que $x+y$ est nilpotent.*
3. *Montrer que $1_A - x$ est inversible.*
4. *Dans cette question, on ne suppose plus que A est commutatif. Soit $u, v \in A$ tels que uv est nilpotent. Montrer que vu est nilpotent.*

Exercice 2 ⋆⋆⋆ - Un anneau d'entiers *(2)*

On considère $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2};\ a, b \in \mathbb{Z}\}$.

1. *Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un anneau.*
2. *On note $N(a + b\sqrt{2}) = a^2 - 2b^2$. Montrer que, pour tous x, y de $\mathbb{Z}[\sqrt{2}]$, on a $N(xy) = N(x)N(y)$.*
3. *En déduire que les éléments inversibles de $\mathbb{Z}[\sqrt{2}]$ sont ceux s'écrivant $a + b\sqrt{2}$ avec $a^2 - 2b^2 = \pm 1$.*

Exercice 3 ⋆ - Équations linéaires *(3)*

Résoudre, dans $\mathbb{Z}/37\mathbb{Z}$, les équations ou systèmes d'équations suivants :

1. $\bar{7}y = \bar{2}$.
2. $\begin{cases} \bar{3}x + \bar{7}y &= \bar{3} \\ \bar{6}x - \bar{7}y &= \bar{0} \end{cases}$

Exercice 4 ⋆⋆⋆⋆ - Théorème de Wilson *(4)*

Le but de cet exercice est de démontrer le théorème de Wilson : un entier $n \geqslant 2$ est premier si et seulement si $(n-1)! \equiv -1\ [n]$.

1. *Soit $p \geqslant 2$ premier. Combien de solutions l'équation $x^2 = 1$ admet-elle de solutions dans $\mathbb{Z}/p\mathbb{Z}$?*
2. *Soit $p \geqslant 2$ premier. Montrer que $(p-1)! = -1\ [p]$.*
3. *Soit $n \geqslant 2$ un entier tel que n divise $(n-1)!+1$. Montrer que pour tout $a \in \{1, \ldots, n-1\}$, a est inversible dans $(\mathbb{Z}/n\mathbb{Z}, \times)$. En déduire que n est premier.*

Indications 1 Soient n, m tels que $x^n = 0$ et $y^m = 0$.

1. Calculer $(xy)^p$ avec $p \geqslant \min(n, m)$.
2. Calculer $(x+y)^{n+m}$.
3. Calculer $(1-x)(1+x+\cdots+x^p)$.
4. Si $(uv)^n = 0$, montrer que $(vu)^{n+1} = 0$.

Indications 2

1. Montrer que c'est un sous-anneau de $(\mathbb{R}, +, \times)$.
2. Il suffit simplement de vérifier l'égalité.
3. Si x est inversible d'inverse y, on a $N(xy) = 1 = N(x)N(y)$. Réciproquement, simplifier $\frac{1}{a+b\sqrt{2}}$ en utilisant la quantité conjuguée.

Indications 3

1. Chercher l'inverse de $\bar{7}$ dans $\mathbb{Z}/37\mathbb{Z}$, en résolvant une équation de Bezout.
2. Résoudre comme s'il s'agissait d'un système ordinaire (substitution...)

Indications 4

1. Factoriser $x^2 - 1$.
2. On pourra regrouper chaque élément de $\{\bar{1}, \ldots, \overline{p-1}\}$ avec son inverse dans $\mathbb{Z}/p\mathbb{Z}$.
3. Appliquer le théorème de Bezout.

Corrige 1 Soient n, m tels que $x^n = 0$ et $y^m = 0$.

1. Puisque x et y commutent, on a $(xy)^n = x^n y^n = 0 \times y^n = 0$.
2. Remarquons d'abord que pour $p \geqslant n$, on a $x^p = x^{p-n}x^n = 0$.
   D'après la formule du binôme, $(x+y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k y^{n+m-k}$. Mais, pour $k \geqslant n$, $x^k = 0 \implies x^k y^{n+m-k} = 0$. D'autre part, pour $k \leqslant n$, on a $n+m-k \geqslant m$ et donc $y^{n+m-k} = 0 \implies x^k y^{n+m-k} = 0$. Ainsi, $(x+y)^{n+m} = 0$. On pourrait même se contenter de prendre la puissance $n+m-1$.
3. D'après l'identité remarquable (toujours valable dans un anneau)
$$1 - x^n = (1-x)(1 + x + \cdots + x^{n-1}).$$
   ce qui implique que $1-x$ est inversible d'inverse $1 + x + \cdots + x^{n-1}$.
4. Soit $n \geqslant 1$ tel que $(uv)^n = 0$. Alors
$$(vu)^{n+1} = v(uv)^n u = v \times 0 \times u = 0.$$
   Ainsi, vu est nilpotent.

Corrige 2

1. Il suffit de prouver que c'est un sous-anneau de $(\mathbb{R}, +, \times)$. En effet, $\mathbb{Z}[\sqrt{2}]$ est :
   — stable par la loi $+$: $(a + b\sqrt{2}) + (a' + b'\sqrt{2}) = (a+a') + (b+b')\sqrt{2}$.
   — stable par la loi $\times$:
$$(a + b\sqrt{2}) \times (a' + b'\sqrt{2}) = (aa' + 2bb') + (ab' + a'b)\sqrt{2}.$$
   — stable par passage l'opposé $-(a + b\sqrt{2}) = -a + (-b)\sqrt{2}$.
   — Enfin, $1 \in \mathbb{Z}[\sqrt{2}]$,
   ce qui achève la preuve du fait que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$.
2. Posons $x = a + b\sqrt{2}$ et $y = a' + b'\sqrt{2}$. En tenant compte de la formule pour le produit obtenue la question précédente, on a
$$\begin{aligned} N(xy) &= (aa' + 2bb')^2 - 2(ab' + a'b)^2 \\ &= (aa')^2 - 2(ab')^2 - 2(a'b)^2 + 4(bb')^2. \end{aligned}$$
   D'autre part,
$$\begin{aligned} N(x) \times N(y) &= (a^2 - 2b^2)(a'^2 - 2b'^2) \\ &= (aa')^2 - 2(ab')^2 - 2(a'b)^2 + 4(bb')^2. \end{aligned}$$
3. Soit $x = a + b\sqrt{2}$. Supposons d'abord que x est inversible, d'inverse y. Alors $N(xy) = N(1) = 1$, et donc $N(x)N(y) = 1$. Puisque $N(x)$ et $N(y)$ sont tous les deux des entiers, on a nécessairement $N(x) = \pm 1$. Réciproquement, si $N(x) = \pm 1$, alors, en utilisant la quantité conjuguée :
$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \pm(a - b\sqrt{2})$$
   ce qui montre que $a + b\sqrt{2}$ est inversible, d'inverse $\pm(a - b\sqrt{2})$.

Corrige 3

1. On cherche d'abord l'inverse de $\overline{7}$ dans $\mathbb{Z}/37\mathbb{Z}$. Cela revient a résoudre l'équation de Bezout $7u + 37v = 1$. En appliquant l'algorithme d'Euclide, on trouve qu'une solution particulière est donnée par $16 \times 7 - 3 \times 37 = 1$. Ainsi, $\overline{16}$ est inverse de $\overline{7}$ dans $\mathbb{Z}/37\mathbb{Z}$. Il vient
$$\overline{7}y = \overline{2} \iff \overline{16} \times \overline{7}y = \overline{16} \times \overline{2} \iff y = \overline{32}.$$
2. On additionne la première et la deuxième ligne pour trouver $\overline{9}x = \overline{3}$. Or, $1 = 37 - 4 \times 9$ et donc $-\overline{4}$ est un inverse de $\overline{9}$ dans $\mathbb{Z}/37\mathbb{Z}$. On trouve donc
$$\overline{9}x = \overline{3} \iff x = -\overline{4} \times \overline{3} = -\overline{12} = \overline{25}.$$
   Si on reporte dans la première équation, on obtient
$$\overline{3} \times (-\overline{12}) + \overline{7}y = \overline{3} \iff \overline{7}y = \overline{39} = \overline{2}.$$
   Le résultat de la question précédente nous donne $y = 32$. La solution unique est donc le couple $(\overline{25}, \overline{32})$.

Corrige 4

1. L'équation $x^2 = 1$ est équivalente $(x-1)(x+1) = 0$, ce qui est équivalent dire, puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, $x = 1$ ou $x = -1$. L'équation admet donc deux solutions.

2. Travaillons dans $\mathbb{Z}/p\mathbb{Z}$. Tout élément de $\{\bar{1}, \ldots, \overline{p-1}\}$ est inversible et son inverse est différent de lui-même, sauf pour $\bar{1}$ et $\overline{-1}$ d'après la question précédente. Dans le produit $\bar{2} \times \cdots \times \overline{p-2}$, on peut donc regrouper chaque élément avec son inverse, et on trouve que

$$\bar{1} \times \cdots \times \overline{p-1} = \bar{1} \times \overline{p-1} = \overline{-1}$$

ce qui est le resultat attendu.

3. Soit $a \in \{1, \ldots, n-1\}$. Alors a est un facteur de $(n-1)!$ et donc il existe k tel que $(n-1)! = ak$. On en déduit $a \times (-k) \equiv 1\ [n]$, et donc a est inversible dans $\mathbb{Z}/n\mathbb{Z}$. Par le théorème de Bézout, ceci signifie que a est premier avec n, et ceci est vrai pour tout a de $\{1, \ldots, n-1\}$. Autrement dit, n est premier.