Université de Lille — FACULTÉ DES SCIENCES ET TECHNOLOGIES — Département de Mathématiques

M22 : Mathématiques fondamentales 2 L1 SESI 2019–2020

Corrigé du devoir surveillé n° 3 – Partie Algèbre

Exercice 1.

1. (a) On calcule les carrés et les cubes des entiers n modulo 4 :
   - si $n \equiv 0 \pmod 4$ alors $n^2 \equiv 0 \pmod 4$ et $n^3 \equiv 0 \pmod 4$,
   - si $n \equiv 1 \pmod 4$ alors $n^2 \equiv 1 \pmod 4$ et $n^3 \equiv 1 \pmod 4$,
   - si $n \equiv 2 \pmod 4$ alors $n^2 \equiv 0 \pmod 4$ et $n^3 \equiv 0 \pmod 4$,
   - si $n \equiv 3 \pmod 4$ alors $n^2 \equiv 1 \pmod 4$ et $n^3 \equiv 3 \pmod 4$.

   (b)
   - Si $x \equiv 0 \pmod 4$ ou $x \equiv 2 \pmod 4$, alors on a $x^3 \equiv 0 \pmod 4$ d'après la question précédente, et donc $y^2 = x^3 + 7 \equiv 7 \equiv 3 \pmod 4$, ce qui est impossible encore d'après la question précédente. De même, si $x \equiv 3 \pmod 4$, alors $x^3 \equiv 3 \pmod 4$ et donc $y^2 = x^3 + 7 \equiv 10 \equiv 2 \pmod 4$, ce qui est également impossible. On a donc bien $x \equiv 1 \pmod 4$.
   - Comme $x \equiv 1 \pmod 4$ d'après le point précédent, alors il existe $k \in \mathbb{Z}$ tel que $x = 4k + 1$. Si on suppose que $k \leq -1$, alors on obtient $x \leq -3$, puis $x^3 \leq -27$, et donc $y^2 = x^3 + 7 \leq -20$, ce qui est absurde. On a donc en fait $k \geq 0$, et donc $x = 4k + 1 \geq 1$.

2. (a) Le polynôme $X^3 + 8$ admet -2 comme racine, donc on peut le factoriser par $X + 2$ dans $\mathbb{Z}[X]$. En effectuant la division euclidienne de $X^3 + 8$ par $X + 2$, on obtient
$$X^3 + 8 = (X + 2)(X^2 - 2X + 4).$$
Comme de plus le discriminant du polynôme $X^2 - 2X + 4$ vaut $-12 < 0$, alors ce polynôme est irréductible dans $\mathbb{R}[X]$ et donc dans $\mathbb{Z}[X]$. Ainsi, la factorisation écrite ci-dessus est bien celle de $X^3 + 8$ dans $\mathbb{Z}[X]$.

   (b) Les entiers x et y vérifiant $y^2 = x^3 + 7$ par hypothèse, on a d'après la question précédente
$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4).$$
Comme $x \geq 1$ et $x \equiv 1 \pmod 4$ d'après le point (b) de la question 1, on en déduit que l'entier $n = x + 2$ divise $y^2 + 1$ et vérifie $n \geq 3$ et $n \equiv 3 \pmod 4$.

   (c) Si n n'admet que des facteurs premiers congrus à 0, 1 ou 2 modulo 4 alors, d'après le point (a) de la question 1, leurs puissances sont aussi congrues à 0, 1 ou 2 modulo 4, et il en est donc de même pour leur produit donnant n, ce qui est impossible puisque $n \equiv 3 \pmod 4$. Par conséquent, il existe un nombre premier p divisant n et vérifiant $p \equiv 3 \pmod 4$.

(d) Comme p divise n d'après le point (c) et comme n divise y^2+1 d'après le point (b), alors p divise y^2+1 par transitivité. Ainsi, on a $y^2+1 \equiv 0 \pmod{p}$, soit encore $y^2 \equiv -1 \pmod{p}$.

3. Par l'absurde, si p divise y, alors $y \equiv 0 \pmod{p}$ et donc $y^2 \equiv 0 \pmod{p}$, et on en déduit d'après la question précédente que $1 \equiv 0 \pmod{p}$. Cela signifie que p divise 1, ce qui est impossible puisque p est un nombre premier. Ainsi, p ne divise pas y et donc, d'après le petit théorème de Fermat, on a $y^{p-1} \equiv 1 \pmod{p}$.

4. D'après le point (c) de la question 2, on a $p \equiv 3 \pmod{4}$. Ainsi, il existe $k \in \mathbb{Z}$ tel que $p = 4k+3$, et donc $\frac{p-1}{2} = 2k+1$ est bien impair. Puisque de plus $y^2 \equiv -1 \pmod{p}$ d'après le point (d) de la question 2, on en déduit en élevant cette congruence à la puissance impaire $\frac{p-1}{2}$ que

$$y^{p-1} = (y^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

5. D'après les deux questions précédentes, on a obtenu respectivement $y^{p-1} \equiv 1 \pmod{p}$ et $y^{p-1} \equiv -1 \pmod{p}$. Par transitivité, on en déduit que $1 \equiv -1 \pmod{p}$, soit encore $2 \equiv 0 \pmod{p}$, ce qui signifie que p divise 2. Comme 2 est un nombre premier et comme $p \geq 2$ puisque p est aussi un nombre premier, on en déduit que $p = 2$, ce qui est contradictoire avec le fait que $p \equiv 3 \pmod{4}$. On a donc bien obtenu la contradiction attendue en supposant l'existence de $(x, y) \in \mathbb{Z}^2$ vérifiant $y^2 = x^3 + 7$.

Exercice 2.

1. — Montrons que $(A, +)$ est un sous-groupe du groupe $(\mathcal{M}_2(\mathbb{R}), +)$:
   - la matrice nulle s'écrit $M_{0,0} \in A$,
   - si $M_{a,b}, M_{c,d} \in A$ alors $M_{a,b} + M_{c,d} = M_{a+c,b+d} \in A$,
   - si $M_{a,b} \in A$ alors $-M_{a,b} = M_{-a,-b} \in A$.
   - La matrice identité s'écrit $M_{1,0} \in A$.
   - Si $M_{a,b}, M_{c,d} \in A$, alors $M_{a,b} \cdot M_{c,d} = M_{c,d} \cdot M_{a,b} = M_{ac,bc+ad} \in A$.

   Ainsi, $(A, +, \cdot)$ est bien un sous-anneau commutatif de l'anneau $(\mathcal{M}_2(\mathbb{R}), +, \cdot)$.

2. Montrons que $(H, +)$ est un sous-groupe du groupe $(A, +)$:
   - la matrice nulle s'écrit $M_{0,0} \in H$,
   - si $M_{0,b}, M_{0,d} \in H$ alors $M_{0,b} + M_{0,d} = M_{0,b+d} \in H$,
   - si $M_{0,b} \in H$ alors $-M_{0,b} = M_{0,-b} \in H$.

3. Soient $M_{a,b}, M_{c,d} \in A$. Alors $M_{a,b} \cdot M_{c,d} = M_{c,d} \cdot M_{a,b} = M_{ac,bc+ad}$, et donc

$$M_{a,b} \cdot M_{c,d} \in H \iff ac = 0 \iff a = 0 \text{ ou } c = 0 \iff M_{a,b} \in H \text{ ou } M_{c,d} \in H.$$