Corrigé Contrôle continu Arithmétique et algèbre commutative mercredi 21 février 2013
10h00–12h00

1. Dans cet exercice on étudiera quelques propriétés de l'anneau $A = \mathbf{Z}[\sqrt{7}] = \{\, a + b\sqrt{7} \mid a, b \in \mathbf{Z} \,\}$.

a. Montrer que A est un sous-anneau de $\mathbf{R}$, et que c'est le plus petit tel sous-anneaux qui contient $\sqrt{7}$ (c'est-à-dire tout sous-anneau de $\mathbf{R}$ aussi contient $\sqrt{7}$ contient aussi tous les éléments de A). Vous pouvez utiliser sans preuve que tout sous-anneaux de $\mathbf{R}$ contient $\mathbf{Z}$.

√ *Il est clair que* $0, 1 \in A$ *et facile à voir que* A *est fermé pour l'addition. Quant à la multiplication, on a* $(a_0+b_0\sqrt{7})(a_1+b_1\sqrt{7}) = a_0a_1+7b_0b_1+(a_0b_1+a_1b_0)\sqrt{7}$*, ce qui montre que* A *est fermé pour la multiplication ; il s'agit donc bien d'un sous-anneau de* $\mathbf{R}$*. Or tout sous-anneau de* $\mathbf{R}$ *contenant* $\sqrt{7}$ *contient aussi, étant fermé pour addition et multiplication, tout* $a + b\sqrt{7} \in A$ *(avec* $a, b \in \mathbf{Z}$*).*

b. Montrer que pour $r \in A$ fixé, le couple $(a, b) \in \mathbf{Z}^2$ tel que $r = a + b\sqrt{7}$ (qui existe d'après la définition de A) est *unique*. Vous pouvez utiliser sans preuve que $\sqrt{7}$ est un nombre irrationnel.

√ *Si on suppose* $a_0 + b_0\sqrt{7} = a_1 + b_1\sqrt{7}$ *alors* $(a_0 - a_1) = (b_1 - b_0)\sqrt{7}$*, et si* $b_1 \neq b_0$ *on aurait* $\sqrt{7} = \frac{a_0-a_1}{b_1-b_0} \in \mathbf{Q}$*, ce qui est faux. Donc* $b_1 = b_0$*, et aussi* $a_1 = a_0$*, ce qui établit l'unicité.*

c. On définit l'application $n : A \to \mathbf{Z}$ par $n(a + b\sqrt{7}) = a^2 - 7b^2$ (une valeur qu'on pourra aussi écrire comme le produit $(a+b\sqrt{7})(a-b\sqrt{7})$ dans A). Montrer que n (qui n'est pas un morphisme d'anneaux) vérifie l'équation $n(xy) = n(x)n(y)$ pour tout $x, y \in A$.

√
$$\begin{aligned} n\big((a_0 + b_0\sqrt{7})(a_1 + b_1\sqrt{7})\big) &= (a_0 + b_0\sqrt{7})(a_1 + b_1\sqrt{7})(a_0 - b_0\sqrt{7})(a_1 - b_1\sqrt{7}) \\ &= n(a_0 + b_0\sqrt{7})n(a_1 + b_1\sqrt{7}) \end{aligned}$$

d. En déduire que, pour que $r \in A$ soit inversible dans A, il est nécessaire que $n(r) \in \{-1, +1\}$.

√ *Si* $rs = 1$ *alors* $n(r)n(s) = n(rs) = n(1) = 1$*, et* $n(r), n(s) \in \mathbf{Z}$*, donc* $n(r) \in \mathbf{Z}^\times = \{-1, +1\}$*.*

e. Montrer que cette condition est aussi suffisante : si $n(r) \in \{-1, +1\}$, alors r est inversible dans A. [Indication : utilisez l'égalité $n(a + b\sqrt{7}) = (a + b\sqrt{7})(a - b\sqrt{7})$ dans A.]

√ *Si* $n(a+b\sqrt{7}) = (a+b\sqrt{7})(a-b\sqrt{7}) = 1$ *dans* A *alors* $a-b\sqrt{7}$ *est inverse de* $a+b\sqrt{7}$*, et pareillement si* $n(a + b\sqrt{7}) = -1$ *alors* $-a + b\sqrt{7}$ *est inverse de* $a + b\sqrt{7}$*.*

f. Trouver un élément inversible de A de la forme $r = a + b\sqrt{7}$ avec $a, b \in \mathbf{Z}$, $b \neq 0$, et $1 \leq b \leq 5$, et donner son inverse r^{-1} dans A.

√ *En essayant les valeurs possibles de* b *on trouve facilement que* $n(a + 3\sqrt{7}) \in \{-1, +1\}$ *possède un solution* $a = 8$*, car* $8^2 - 7 \times 3^2 = 1$*, donc* $r = 8+3\sqrt{7}$ *est inversible. Son inverse est* $r^{-1} = 8 - 3\sqrt{7}$*.*

g. En utilisant cet élément r, montrer que le nombre d'éléments inversibles de A est infini.

√ *Toutes les puissances* r^k *avec* $k \in \mathbf{Z}$ *sont inversibles, car* $r^k(r^{-1})^k = 1$*. Aussi ces puissance sont distinctes, car* $r^k = r^l$ *entraîne* $r^{k-l} = 1$*, mais comme* $r \in \mathbf{R} \setminus \{-1, 1\}$ *ceci n'arrive que si* $k = l$*.*

2. Dans cet exercice A est un anneau commutatif. Un élément $a \in A$ est appelé nilpotent s'il existe $n \in \mathbf{N}$ tel que $a^n = 0$.

a. Décrire les éléments nilpotents de l'anneau $\mathbf{Z}/72\mathbf{Z}$. Combien en y a-t-il ?

√ *Si l'on écrit* $\bar{m}$ *pour la classe de* $m \in \mathbf{Z}$ *dans* $\mathbf{Z}/72\mathbf{Z}$*, alors* $\bar{m}$ *est nilpotent s'il existe* $n \in \mathbf{N}$ *tel que* $\bar{m}^n = \bar{0}$*, c'est-à-dire tel que* m^n *est divisible par* 72*. Pour cela il faut que* m *contient au moins un facteur* 2 *et un facteur* 3 *(car sinon aucune puissance* m^n *ne contient de tel facteurs), et cela suffit aussi, car* a^3 *sera divisible par* 2^3 *et par* 3^3*, et donc par* $2^3 3^2 = 72$*. Les éléments nilpotents de* $\mathbf{Z}/72\mathbf{Z}$ *sont donc les* $\bar{m}$ *avec* m *divisible par* 6*, et il y a* $72/6 = 12$ *différents tels éléments* $(\bar{0}, \bar{6}, \bar{12}, \bar{18}, \bar{24}, \bar{30}, \bar{36}, \bar{42}, \bar{48}, \bar{54}, \bar{60}, \bar{66})$*.*

b. Dans le cas où A est un anneau intègre, quels sont alors les éléments nilpotents de A ?

√ *Si* A *est intègre,* $a^n = 0$ *entraîne que l'un des facteurs* a *du produit* a^n *est nul ; bref* $a = 0$ *est le seul élément nilpotent.*

c. Montrer que l'ensemble des éléments nilpotents de A forme un idéal N de A.

√ *Si* a, b *sont nilpotents, disons* $a^n = 0 = b^m$*, alors tous les termes de* $(a + b)^k = \sum_{i=0}^{k} \binom{k}{i} a^i b^{k-i}$ *s'annulent dès que* $k \geq n + m - 1$*. Donc* $a + b$ *est nilpotent et l'ensemble d'éléments nilpotents est fermé pour l'addition. Aussi* $(xa)^n = x^n a^n = 0$ *pour tout* $x \in A$*, donc* xa *est nilpotent et l'ensemble d'éléments nilpotents est fermé pour la multiplication par un élément quelconque de* A*.*

d. Montrer que dans l'anneau quotient A/N, l'élément $0 \in A/N$ est le seul élément nilpotent.

$\surd$ *Soit $x \in A$ tel que son image $\bar{x} \in A/N$ soit nilpotent, disons $(\bar{x})^n = 0$. Cela veut dire que $a = x^n$ est dans N, donc nilpotent, disons $a^m = 0$. Alors $x^{nm} = (x^n)^m = a^m = 0$ et $x \in N$, donc $\bar{x} = 0$.*

e. [Hors barème] Montrer que si I est une idéal premier de A, alors $I \supseteq N$, c'est-à-dire I contient tous les éléments nilpotents de A. L'idéal N lui-même, est-il forcément un idéal premier ?

$\surd$ *Soit $x \in N$, disons $x^n = 0$, alors aussi $\bar{x}^n = 0 \in A/I$ pour son image $\bar{x} \in A/I$. Comme A/I est intègre quand I est un idéal premier, ceci entraîne $\bar{x} = 0$ (question b) et donc $x \in I$, ce qui prouve $N \subseteq I$. L'exemple de la question a montre que N lui-même n'est pas forcément premier : on a $N = 6\mathbf{Z}/72\mathbf{Z} \subseteq A = \mathbf{Z}/72\mathbf{Z}$, et $A/N \cong \mathbf{Z}/6\mathbf{Z}$ n'est pas un anneau intègre, donc N n'est pas un idéal premier. Aussi un anneau sans éléments nilpotents autre que 0 peut avoir des diviseurs de zéro, comme c'est le cas pour $A = R \times S$ quand R, S sont des anneaux intègres ; pour un tel A on aura $N = \{0\}$, qui n'est pas un idéal premier.*

Fin.