Corrigé Examen Arithmétique et algèbre commutative mercredi 16 avril 2014
9h00–12h00

1. Pour les anneaux commutatifs mentionnés ci-dessous, indiquer la *première* classe dans la liste suivante à laquelle appartient l'anneau: (1) corps, (2) anneau principal, (3) anneau factoriel, (4) anneau intègre, (5) anneau commutatif. [Une seule réponse par anneau ; une justification n'est pas requise.]

a. $\mathbf{Z}/17\mathbf{Z}$

$\surd$ *(1), c'est un corps, car* 17 *est un nombre premier*

b. $\mathbf{Z}/18\mathbf{Z}$

$\surd$ *(5), ce n'est pas un anneau intègre, car* 18 *est composé (*$3 \times 6 = 0$*)*

c. $(\mathbf{Z}/5\mathbf{Z})[X]$

$\surd$ *(2), c'est un anneau (euclidien donc) principal, car de la forme* $K[X]$ *avec* K *un corps.*

d. $\mathbf{Z}[\mathbf{i}\sqrt{5}]$

$\surd$ *(4), c'est un anneau intègre, mais pas factoriel (vu en cours/TD).*

e. $\mathbf{Q}[X, Y, Z]$

$\surd$ *(3), c'est un anneau factoriel, par hérédité, car* $\mathbf{Q}[X]$ *euclidien.*

f. $\mathbf{R}[X]/(X^2 + X + 1)$

$\surd$ *(1), c'est un corps, quotient de l'anneau principal* $\mathbf{R}[X]$ *par l'idéal engendré par l'élément* X^2+X+1*, irréductible (le discriminant est négatif), et un tel idéal est maximal (en fait ce corps est* $\cong \mathbf{C}$*).*

2. Soit $n > 1$ entier, et $A = \mathbf{Z}[\mathbf{i}\sqrt{n}] \subseteq \mathbf{C}$. On veut montrer que A est un anneau avec factorisations : il est intègre et tout élément non nul et non inversible s'écrit comme produit d'éléments irréductibles.

a. Montrer rapidement que A est un anneau commutatif intègre.

$\surd$ *Tout sous-anneau du corps commutatif* $\mathbf{C}$ *est commutatif et intègre, et* A *est un tel sous-anneau (par définition de la notation).*

b. Vérifier que la norme algébrique N définie par $z \in A \mapsto N(z) = z\overline{z}$ est à valeurs dans $\mathbf{N}$.

$\surd$ *On a* $N(a + b\mathbf{i}\sqrt{n}) = (a + b\mathbf{i}\sqrt{n})(a - b\mathbf{i}\sqrt{n}) = a^2 + nb^2$*, qui est visiblement entier et positif si* $a, b \in \mathbf{Z}$ *et* $n > 1$ *est entier.*

c. Déterminer $A^\times$ et montrer que tout élément de $T = A \setminus (A^\times \cup \{0\})$ est de norme > 1.

$\surd$ *La norme est multiplicative car* $N(xy) = xy\overline{xy} = x\overline{x}y\overline{y} = N(x)N(y)$*. En particulier si* $x \in A^\times$*, disons* $xy = 1$*, on a* $N(x)N(y) = N(1) = 1$*, et en vue de la question précédente cela nécessite* $N(x) = 1$*. Or* $N(x) = 1$ *implique* $x \in \{1, -1\}$ *car* $a^2 + nb^2$ *n'est possible que si* $a \in \{1, -1\}$ *et* $b = 0$ *(car* $n > 1$*) ; comme* 1 *et* -1 *sont bien évidemment inversibles, on a* $A^\times = \{1, -1\}$*. Aussi* $N(x) = 0$ *entraîne* $x = 0$ *(car* $N(x) = x\overline{x}$*, et* A *est intègre), donc si* $x \in A \setminus (A^\times \cup \{0\})$*, on a nécessairement* $N(x) \notin \{0, 1\}$*, et donc* $N(x) > 1$*.*

d. Posons $W = \{\, x \in T \mid x \text{ ne s'écrit pas comme produit d'irréductibles} \,\}$. Supposons pour une contradiction $W \neq \emptyset$; soit $x \in W$. Justifier qu'il existe $a, b \in A$ tels que $x = ab$, avec $a \notin A^\times$ et $b \notin A^\times$. En déduire que a ou b est élément de W. En utilisant N, aboutir à une contradiction.

$\surd$ *Le fait que* $x \in T$ *dit que* x *est tel que* x *est ni nul ni inversible, et il n'est pas irréductible non plus, donc* x *est réducible ; cela veut dire qu'il existe* $a, b \in A$ *tels que* $x = ab$*, avec* $a \notin A^\times$ *et* $b \notin A^\times$*, et bien sur* $a, b \neq 0$*. Si* a, b *s'écrivaient tous deux comme produit d'irréductibles, ce serait aussi le cas de* $x = ab$ *(il suffit de concaténer les écritures de* a, b*), contrairement à l'hypothése* $x \in W$*. Par conséquent l'un au moins de* a, b *ne s'ecrit pas comme produit d'irréductibles ; par symétrie supposons que c'est* a*. On a* $N(a) = N(x)/N(b) < N(x)$ *(car* $N(b) > 1$*), et en prenant pour* x *un élément de* W *tel que* $N(x)$ *est minimal, on arrive à une contradiction. [En fait ici la preuve par contradiction n'apporte que des complications, car une preuve "positive" du fait que tout élément de* T *s'écrit comme produit d'irréductibles est possible, par récurrence sur la norme de l'élément.]*

3. On note $Q = (X+2)^2(X^2+1) \in \mathbf{R}[X]$.

a. L'anneau quotient $A = \mathbf{R}[X]/(Q)$ est-il intègre?

$\surd$ *Non, car l'idéal (Q) n'est pas premier : les facteurs $(X+2)^2$ et (X^2+1) de Q ne sont pas dans l'idéal, mais leur produit Q est dans l'idéal.*

b. À l'aide de la division euclidienne dans $\mathbf{R}[X]$, montrer que tout élément de A est la classe d'un polynome de degré au plus 3 de $\mathbf{R}[X]$.

$\surd$ *Si $P \in \mathbf{R}[X]$, la classe de P est la même que celle de son reste R après division par Q, qui vérifie par définition $\deg(R) < \deg(Q) = 4$.*

c. Déterminer tous les éléments P de A tels que $P^2 = 0$.

$\surd$ *Comme $(X+2)^2$ et (X^2+1) sont premiers entre eux, on a par le lemme chinois un isomorphisme $A \cong (\mathbf{R}[X]/(X+2)^2)) \times (\mathbf{R}[X]/(X^2+1))$, avec la projections sur les deux facteurs données par réduction modulo $(X+2)^2$ respectivement modulo (X^2+1). On aura $P^2 = 0$ dans A si et seulement is ses deux projections vérifient une même équation. Dans le second facteur, qui est une corps car X^2+1 est irréductible sur $\mathbf{R}$, l'équation $x^2 = 0$ a pour seule solution $x = 0$. Par contre dans le premier facteur $\mathbf{R}[X]/(X+2)^2)$ cette équation a des solution non nulles, à savoir tous les multiples de (l'image de) $X+2$. Par conséquent $P^2 = 0$ dans A si et seulement si P est la classe d'un polynôme qui est multiple de $(X+2)(X^2+1)$.*

d. Montrer que si $P \in A$ vérifie $P^3 = 0$, alors il vérifie aussi $P^2 = 0$.

$\surd$ *Par le même raisonnement, on a $P^3 = 0$ dès lors que ses projections sur les deux facteurs sont un multiple de $X+2$ respectivelemt nulle, et c'est la même condition qui donnait $P^2 = 0$.*

e. Déterminer l'idéal I de $\mathbf{R}[X]$ engendré par les deux polynômes Q et $X^4 - 1$. En déduire une description de l'anneau quotient $\mathbf{R}[X]/I$.

$\surd$ *On a la factorisation en irréductibles $X^4 - 1 = (X^2+1)(X+1)(X-1)$, et on en déduit que $\mathrm{pgcd}(Q, X^4-1) = X^2+1$. Par ce qu'on sait sur les anneaux principaux comme $\mathbf{R}[X]$ (relation de Bezout), ce* pgcd *est le générateur de l'idéal I engendré par le couple Q, X^4-1. Or X^2+1 est irréductible dans $R[X]$, donc R/I est un corps. En fait ce corps est isomorphe à $\mathbf{C}$ (il s'agit même de la présentation standard $\mathbf{C} \cong \mathbf{R}[X]/(X^2+1)$).*

4. Soit $A = \mathbf{Z}[\sqrt{10}]$, sous-anneau de $\mathbf{R}$. On note $N(z)$ la norme d'un élément $z \in A$, donnée par $N(z) = a^2 - 10b^2$ si $z = a + \sqrt{10}b$, et qui vérifie $N(xy) = N(x)N(y)$ pour tout $x, y \in A$ (admis).

a. Montrer qu'un élément $z \in A$ est inversible si et seulement si $N(z) \in \{1, -1\}$.

$\surd$ *Si z possède un inverse $z^{-1} \in A$, alors $1 = N(1) = N(zz^{-1}) = N(z)N(z^{-1})$, une décomposition dans $\mathbf{Z}$ qui montre que $N(z) \in \mathbf{Z}^\times = \{1, -1\}$. Réciproquement, si $N(z) = z\overline{z} = \pm 1$, alors $z \times \pm\overline{z} = 1$, ce qui montre que z est inversible.*

b. Donner un exemple d'élément inversible $z \notin \{1, -1\}$.

$\surd$ *On peut prendre $z = 3 + \sqrt{10}$, pour lequel $N(z) = -1$, donc son inverse est $-\overline{z} = -3 + \sqrt{10}$. Il existe d'autres examples, tous de la form $\pm(3+\sqrt{10})^n$, par exemple $(3+\sqrt{10})^2 = 19 + 6\sqrt{10}$.*

c. Montrer que pour $a \in \mathbf{Z}/10\mathbf{Z}$ la condition $a^2 \in \{3, -3\}$ n'a pas de solutions.

$\surd$ *Comme $\mathbf{Z}/10\mathbf{Z}$ n'a que 10 éléments, il suffit de calculer leurs carrés et de constater que les seules valeurs obtenues sont les classes $0, 1, 4, 5, 6, 9$, donc ni 3 ni $-3 = 7$ sont des carrés dans $\mathbf{Z}/10\mathbf{Z}$. (Comme $(-a)^2 = a^2$, on pourrait se contenter de calculer les carrés juste des classes $0, 1, 2, 3, 4, 5$.)*

d. À l'aide de la question *c*, montrer que $4 + \sqrt{10}$ est irréductible dans A.

$\surd$ *On a $N(4+\sqrt{10}) = 6$, donc $4 + \sqrt{10}$ n'est ni nul ni (question b) inversible. Montrons qu'il ne peut pas être réducible, pour conclure qu'il est irréductible. Si on avait $4 + \sqrt{10} = xy$ avec x, y non inversibles, alors $N(x), N(y) \notin \{1, -1\}$ et leur produit doit être 6, ce qui laisse les deux possibilités $\{N(x), N(y)\} = \{2, 3\}$ et $\{N(x), N(y)\} = \{-2, -3\}$. Mais si $x = a + b\sqrt{10}$ on a $N(x) = a^2 - 10b^2 \equiv a^2 \pmod{10}$, et la question c montre que cela est impossible si $N(x) \in \{3, -3\}$ (d'ailleurs c'est également impossible si $N(x) \in \{2, -2\}$. Cela élimine les deux possibilités, donc on peut conclure que $4 + \sqrt{10}$ est irréductible dans A.*

e. Montrer que A n'est pas factoriel (indication : pensez à la norme de l'élément $4 + \sqrt{10}$).

$\surd$ *La norme $N(z) = 6 = z\overline{z}$ de $z = 4 + \sqrt{10}$ est divisible par z, et se décompose aussi en produit $6 = 2 \times 3$ de deux éléments non divisibles par z (leurs normes respectives $4, 9$ ne sont pas divisibles par la norme 6 de z). Cela montre que z, pourtant irréductible (question d) n'est pas premier. Dans un anneau factoriel tout élément irréductible est premier, donc A ne peut pas être factoriel.*

5. Soit $A = \mathbf{Z}[\sqrt{2}\,\mathbf{i}]$ le sous-anneau de $\mathbf{C}$ formé des nombres $s + \sqrt{2}\,\mathbf{i}\,t$ avec $s, t \in \mathbf{Z}$ (c'est un anneau commutatif intègre). On note $N : A \to \mathbf{N}$ la fonction $z \mapsto z\overline{z} = |z|^2$. Comme pour les entiers on veut montrer que A est un anneau euclidien, en l'occurrence avec N comme stathme. Cela veut dire que pour tout $a, b \in A$ avec $b \neq 0$ il existe $q, r \in A$ tels que $a = bq + r$ et $N(r) < N(b)$.

a. Montrer que dans ce cas il existe $s + \sqrt{2}\,\mathbf{i}\,t \in A$ tel qu'on ait, dans $\mathbf{C}$ (où la division $\frac{a}{b}$ est exacte) :

$$\left|\frac{a}{b} - (s + \sqrt{2}\,\mathbf{i}\,t)\right| \leq \frac{\sqrt{3}}{2}.$$

√ *Pour $s+\sqrt{2}\,\mathbf{i}\,t \in A$ donné, l'ensemble des $z \in \mathbf{C}$ qui sont plus proche de $s+\sqrt{2}\,\mathbf{i}\,t$ que de tout autre élément de A est $\{\, z \in \mathbf{C} \mid s - \frac{1}{2} < \operatorname{Re} z < s + \frac{1}{2}, \sqrt{2}(t - \frac{1}{2}) < \operatorname{Im} z < \sqrt{2}(t + \frac{1}{2}) \,\}$; pour les points sur le bord de ce rectangle cette distance est encore minimale, mais cette fois ex aequo avec un autre point de A. Les clôtures de ces rectangles recouvent le plan complexe, et leur diamètre est $\sqrt{1+2} = \sqrt{3}$; la distance maximale des points d'un tel rectangle des son centre en est la moitié. La distance d'un nombre complexe z à l'élément de A le plus proche est donc au plus $\frac{\sqrt{3}}{2}$. En prenant $z = \frac{a}{b}$ on obtient l'existence de s, t avec l'inégalité demandée.*

b. En prenant dans cette situation $q = s + \sqrt{2}\,\mathbf{i}\,t$, montrer que $r = a - bq$ vérifie $N(r) < N(b)$, et conclure que A est un anneau euclidien.

√ *On a $|r| = |a - bq| = |\frac{a}{b} - (s + \sqrt{2}\,\mathbf{i}\,t)|.|b| \leq \frac{\sqrt{3}}{2}|b|$ et donc $N(r) = |r|^2 \leq \frac{3}{4}|b|^2 < N(b)$. Cette inégalité, valable quels que soient a et $b \neq 0$ (pour les q, r indiqués), montre que N est un stathme dans A, qui est donc un anneau euclidien.*

c. Effectuer la division euclidienne dans A de $4 + 3\sqrt{2}\,\mathbf{i}$ par $2 - \sqrt{2}\,\mathbf{i}$, et calculer leur pgcd.

√ *La division dans $\mathbf{C}$ donne $\frac{4+3\sqrt{2}\,\mathbf{i}}{2-\sqrt{2}\,\mathbf{i}} = N(2-\sqrt{2}\,\mathbf{i})^{-1}(4+3\sqrt{2}\,\mathbf{i})(2+\sqrt{2}\,\mathbf{i}) = \frac{1}{6}(2+10\sqrt{2}\,\mathbf{i}) = \frac{1}{3}+\frac{5}{3}\sqrt{2}\,\mathbf{i}$. Le quotient dans A en est déduit par arrondi des deux coefficients entiers : $q = 0 + 2\sqrt{2}\,\mathbf{i}$; et le reste correspondant sera $r = 4 + 3\sqrt{2}\,\mathbf{i} - q(2 - \sqrt{2}\,\mathbf{i}) = 4 + 3\sqrt{2}\,\mathbf{i} - (4 + 4\sqrt{2}\,\mathbf{i}) = -\sqrt{2}\,\mathbf{i}$, qui vérifie $N(r) = 2 < N(2 - \sqrt{2}\,\mathbf{i}) = 4$. En continuant l'algorithme d'Euclide, la division de $2 - \sqrt{2}\,\mathbf{i}$ par le reste $r = -\sqrt{2}\,\mathbf{i}$ est exacte dans A (avec quotient $1 + \sqrt{2}\,\mathbf{i}$), donc $\operatorname{pgcd}(4+3\sqrt{2}\,\mathbf{i}, 2-\sqrt{2}\,\mathbf{i}) = -\sqrt{2}\,\mathbf{i}$ (qui est associé à $\sqrt{2}\,\mathbf{i}$).*

d. [bonus] On a vu en TD que l'anneau $B = \mathbf{Z}[\sqrt{3}\,\mathbf{i}]$ n'est pas un anneau principal, ce qui implique que B ne peut pas être un anneau euclidien non plus. Si l'on essaye néanmoins de faire le raisonnement ci-dessus pour B au lieu de A, avec $\sqrt{3}$ à la place de $\sqrt{2}$, qu'est-ce qui change pour empêcher qu'on arrive à la fausse conclusion que B serait un anneau euclidien ?

√ *Avec $\sqrt{3}$ à la place de $\sqrt{2}$, le diamètre des rectangles est $\sqrt{1+3} = 2$; la distance maximale vers un point de A donc 1. On n'aura plus forcément d'inégalité stricte $N(r) < N(b)$, et on ne saura conclure que N soit un stathme euclidien. Visiblement le cas où le quotient $\frac{a}{b}$ est à distance maximale $\sqrt{4}/2 = 1$ de l'élément le plus proche de B se produit réellement pour certains $a, b \in B$; en fait on peut voir que c'est le cas pour $a = 1 + \sqrt{3}\mathbf{i}$ et $b = 2$ (ou pour $a = 1 + \sqrt{3}\mathbf{i}$ et $b = 1 - \sqrt{3}\mathbf{i}$).*

Fin.