Corrigé Examen 6L23 : Arithmétique dans les anneaux mercredi 4 mai 2011
9h00–12h00

1. On note $\mathbf{Q}(\sqrt{3})$ l'ensemble $\{\, a + b\sqrt{3} \mid a, b \in \mathbf{Q} \,\}$.

a. Montrer que $\mathbf{Q}(\sqrt{3})$ est un sous-corps de $\mathbf{C}$, et aussi un $\mathbf{Q}$-espace vectoriel de dimension 2.

√ *On a* $(a+b\sqrt{3})+(a'+b'\sqrt{3}) = (a+a')+(b+b')\sqrt{3}$ *et* $\lambda(a+b\sqrt{3}) = \lambda a+\lambda b\sqrt{3}$, *donc* $\mathbf{Q}(\sqrt{3})$ *est fermé pour l'addition et pour la multiplication scalaire par les nombres rationnels ; comme il contient aussi* 0 *c'est un* $\mathbf{Q}$*-espace vectoriel, dont* $\{1, \sqrt{3}\}$ *est visiblement une famille génératrice, qui est aussi libre par l'irrationalité de* $\sqrt{3}$, *donc c'est bien un* $\mathbf{Q}$*-espace vectoriel de dimension* 2. *Pour que ce soit un sous-anneau il suffit de vérifier ensuite qu'il contient* 1 *(évident), et qu'il est fermé pour la multiplication :* $(a+b\sqrt{3}) \times (a'+b'\sqrt{3}) = (aa'+3bb')+(ab'+ba')\sqrt{3}$. *Finalement pour que ce soit un corps, il suffit de trouver un inverse pour* $a+b\sqrt{3} \neq 0$, *et c'est* $\frac{a}{a^2-3b^2} - \frac{b}{a^2-3b^2}\sqrt{3}$, *où le dénominateur est un nombre rationnel non nul (par l'irrationalité de* $\sqrt{3}$*). Ce dernier point aurait aussi pu être établi en utilisant la question suivante (!), en remarquant que* X^2-3 *est irréductible (à cause encore de l'irrationalité de* $\sqrt{3}$ *: son degré étant* 2, *une décomposition nécessite une racine), et en invoquant proposition 2.3.9 du cours (et le paragraphe qui suit cette proposition).*

b. Montrer que le corps $\mathbf{Q}(\sqrt{3})$ est isomorphe à l'anneau quotient $\mathbf{Q}[X]/(X^2-3)$.

√ *Comme* $\mathbf{Q}(\sqrt{3})$ *est un anneau qui contient* $\mathbf{Q}$, *il existe un morphisme d'anneaux unique* $f : \mathbf{Q}[X] \to \mathbf{Q}(\sqrt{3})$ *qui fixe les éléments de* $\mathbf{Q}$ *et qui envoie* $X \mapsto \sqrt{3}$; *il est surjectif car* $\{1, \sqrt{3}\}$ *est contenu dans l'image qui est un* $\mathbf{Q}$*-espace vectoriel, et* $\ker(f)$ *est engendré par* X^2-3 *(car aucun polynôme de degré* 0 *ou* 1 *est dans le noyau, toujours par l'irrationalité de* $\sqrt{3}$*). L'énoncé est alors une instance du théorème d'isomorphisme 1.3.4.*
Beaucoup ont choisi d'argumenter que X^2-3 *engendre* $\ker(f)$ *en considérant uniquement des racines. Ceci n'est pas facile, car* X^2-3 *n'a pas de racines dans* $\mathbf{Q}$, *pendant que si on le considère comme polynôme dans* $\mathbf{Q}(\sqrt{3})[X]$ *(ou* $\mathbf{R}[X]$ *ou* $\mathbf{C}[X]$*), alors le fait d'avoir une racine* $\sqrt{3}$ *n'implique pas que* $-\sqrt{3}$ *est aussi une racine. Un raisonnement correct (mais que personne n'a donné) est le suivant. Le corps* $\mathbf{Q}(\sqrt{3})$ *possède un automorphisme* ϕ *avec* $\phi(\sqrt{3}) = -\sqrt{3}$ *et qui fixe* $\mathbf{Q}$ *; alors en désignant aussi par* ϕ *l'automorphisme de* $\mathbf{Q}(\sqrt{3})[X]$ *qui agit par* ϕ *sur les coefficients et qui fixe* X, *on a que si* $r \in \mathbf{Q}(\sqrt{3})$ *est racine de* $P \in \mathbf{Q}(\sqrt{3})[X]$, *alors* $\phi(r)$ *est racine de* $\phi(P)$, *et comme* $\phi(Q) = Q$ *pour* $Q \in \ker(f) \subseteq \mathbf{Q}[X]$, *le fait que* Q *a* $\sqrt{3}$ *comme racine entraîne qu'il a aussi* $-\sqrt{3}$ *comme racine, et est donc divisible par* $(X-\sqrt{3})(X+\sqrt{3}) = X^2-3$. *Mais prouver que l'automorphisme* ϕ *de* $\mathbf{Q}(\sqrt{3})$ *existe n'est pas plus simple que l'argument direct que* X^2-3 *engendre* $\ker(f)$.

c. Soit

$$A = \begin{pmatrix} 0 & 0 & 3 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbf{Q})$$

Montrer que le polynôme minimal de A dans $\mathbf{Q}[X]$ est $X^3 - 3X = (X^2-3)X$. [Le polynôme minimal est par définition le polynôme unitaire $X^d + c_{d-1}X^{d-1} + \cdots + c_1X + c_0$ du plus petit degré d possible tel que $A^d + c_{d-1}A^{d-1} + \cdots + c_1A + c_0\,\mathrm{id} = 0$. Vous pouvez baser votre réponse directement sur cette définition, ou si vous préférez sur toute autre propriété connue du polynôme minimal, qu'il suffira de mentionner.]

√ *Les premières puissances de* A *sont respectivement*

$$A^0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \mathcal{M}_3(\mathbf{Q}), \qquad A^2 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 3 \end{pmatrix} \in \mathcal{M}_3(\mathbf{Q}),$$
$$A^1 = \begin{pmatrix} 0 & 0 & 3 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbf{Q}), \qquad A^3 = \begin{pmatrix} 0 & 0 & 9 \\ 0 & 0 & 0 \\ 3 & 0 & 0 \end{pmatrix} \in \mathcal{M}_3(\mathbf{Q}),$$

dont on voit facilement que A^0, A^1, A^2 *sont linéairement indépendants sur* $\mathbf{Q}$, *mais* $A^3 = 3A$, *donc le polynôme minimal* μ_A *est* $X^3-3X = (X^2-3)X$. *On pourrait aussi remarquer que* X^3-3X *est le polynôme caractéristique* χ_A *de* A *(par calcul direct), et comme il est à racines simples (dans* $\mathbf{C}$*) on a* $\mu_A = \chi_A$ *(car les racines de* μ_A *sont celles de* χ_A, *avec une multiplicité pas plus grande).*

d. En déduire que A n'est pas diagonalisable sur $\mathbf{Q}$, mais qu'elle est diagonalisable sur le corps $\mathbf{Q}(\sqrt{3})$.

√ *Le polynôme minimal $(X^2-3)X$ n'est pas scindé sur $\mathbf{Q}$, à cause du facteur irréductible X^2-3, donc A n'est pas diagonalisable sur $\mathbf{Q}$ (une condition nécessaire pour que A soit diagonalisable est que le polynôme minimal, ou de façon équivalente le polynôme caractéristique, soit scindé). Mais le polynôme minimal est scindé $X^3-3X=(X-\sqrt{3})(X+\sqrt{3})X$ sur le corps $\mathbf{Q}(\sqrt{3})$, et comme ses racines sont simples, A est diagonalisable sur $\mathbf{Q}(\sqrt{3})$. Que le polynôme minimal soit scindé à racines simples est nécessaire et suffisant pour que A soit diagonalisable ; la condition correspondante pour le polynôme caractéristique pouvait aussi être utilisée : elle est suffisante, même si elle n'est pas nécessaire. Une base de diagonalisation est $(\sqrt{3},0,1)$, $(-\sqrt{3},0,1)$, $\big(0,1,0\big)$.*

e. Donner un isomorphisme d'anneaux $\mathbf{Q}[X]/(X^3-3X)\to\mathbf{Q}[A]$, où $\mathbf{Q}[A]$ est le sous-anneau de $\mathcal{M}_3(\mathbf{Q})$ engendré par $\mathbf{Q}$ et A (c'est aussi le $\mathbf{Q}$-espace engendré par les puissances A^i, $i\in\mathbf{N}$).

√ *Le polynôme minimal X^3-3X engendre le noyau du morphisme de substitution $\mathbf{Q}[X]\to\mathrm{End}(\mathbf{Q}^3)$ qui envoie $X\mapsto A$ et $\lambda\mapsto\lambda I_3$ pour $\lambda\in\mathbf{Q}$. L'image de ce morphisme est par définition $\mathbf{Q}[A]$, donc le morphisme induit un isomorphisme d'anneaux $\mathbf{Q}[X]/(X^3-3X)\to\mathbf{Q}[A]$ d'après le théorème d'isomorphisme 1.3.4.*

f. Trouver dans $\mathbf{Q}[X]$ une relation de Bézout $U(X^2-3)+VX=1$ avec $\deg(U)=0$ et $\deg(V)=1$.

√ *Par inspection $U=-\frac{1}{3}$ et $V=\frac{1}{3}X$ conviennent.*

g. Le morphisme d'anneaux $\mathbf{Q}[X]\to\mathbf{Q}[X]/(X^2-3)\times\mathbf{Q}[X]/(X)$, qui à $P\in\mathbf{Q}[X]$ associe le couple de ses classes modulo X^2-3 et modulo X, respectivement, est surjectif et a pour noyau l'idéal engendré par X^3-3X ; il induit donc un isomorphisme $\mathbf{Q}[X]/(X^3-3X)\to\mathbf{Q}[X]/(X^2-3)\times\mathbf{Q}[X]/(X)$. Utiliser la relation de Bezout pour trouver, pour $a,b,\lambda\in\mathbf{Q}$, l'image réciproque pour cet isomorphisme du couple $(\overline{a+bX},\overline{\lambda})\in\mathbf{Q}[X]/(X^2-3)\times\mathbf{Q}[X]/(X)$, sous forme de la classe modulo X^3-3X d'un polynôme de degré au plus 2.

√ *On a $1=-\frac{1}{3}(X^2-3)+\frac{1}{3}X\cdot X$, donc $\frac{1}{3}X^2\equiv 1 \pmod{X^2-3}$ et $-\frac{1}{3}(X^2-3)\equiv 1 \pmod{X}$. Cela fournit des solutions $\frac{1}{3}X^2$ pour le cas particulier $a=1,b=\lambda=0$, respectivement $-\frac{1}{3}(X^2-3)$ pour $a=b=0,\lambda=1$ (ces solutions sont à interpréter comme leurs classes modulo X^3-3X). Pour un troisième cas linéairement indépendant $a=\lambda=0,b=1$, il suffit de multiplier la première solution par X, ce qui donne $\frac{1}{3}X^3$, quelle solution est équivalente modulo X^3-3X à $\frac{3}{3}X=X$ (et effectivement $X\equiv X \pmod{X^2-3}$ et $X\equiv 0 \pmod{X}$). En formant une combinaison linéaire des trois solutions particulières, on trouve la solution $\frac{1}{3}aX^2+bX-\frac{1}{3}\lambda(X^2-3) \pmod{X^3-3X}$.*

h. Montrer qu'il existe un isomorphisme d'anneaux $\phi:\mathbf{Q}(\sqrt{3})\times\mathbf{Q}\to\mathbf{Q}[A]$ donné par

$$\phi(a+b\sqrt{3},\lambda)=\begin{pmatrix}a&0&3b\\0&\lambda&0\\b&0&a\end{pmatrix}.$$

√ *Il suffit de composer les isomorphisme suivants: $\mathbf{Q}(\sqrt{3})\times\mathbf{Q}\to\mathbf{Q}[X]/(X^2-3)\times\mathbf{Q}[X]/(X)$ donné par $(a+b\sqrt{3},\lambda)\mapsto(\overline{a+bX},\overline{\lambda})$, l'isomorphisme $\mathbf{Q}[X]/(X^2-3)\times\mathbf{Q}[X]/(X)\to\mathbf{Q}[X]/(X^3-3X)$ réciproque à celui évoqué dans la question g, et l'isomorphisme $\mathbf{Q}[X]/(X^3-3X)\to\mathbf{Q}[A]$ de la question e. En utilisant les réponses précédentes on trouve la description*

$$(a+b\sqrt{3},\lambda)\mapsto(\overline{a+bX},\overline{\lambda})\mapsto\overline{\frac{1}{3}aX^2+bX-\frac{1}{3}\lambda(X^2-3)}\mapsto\frac{1}{3}aA^2+bA-\frac{1}{3}\lambda(A^2-3\,\mathrm{id})$$

de la composée, dont l'expression finale s'évalue à la matrice de l'énoncé.

2. Dans cette partie R désigne un anneau commutatif quelconque. On admet le résultat suivant (qui est mentionné dans le cours sans être démontré, connu comme le théorème de Krull) : tout anneau commutatif non trivial contient un idéal maximal.

√ *Cette partie a été largement boudée. Pourtant les réponses sont plus simples que dans les autres parties.*

a. En déduire la généralisation suivante : tout idéal propre I de R il existe un idéal maximal de R qui contient I. (Indication : penser aux anneaux quotient.)

√ *L'anneau R/I contient un idéal maximal, dont l'image réciproque par la projection canonique $R\to R/I$ est un idéal maximal de R contenant I (correspondance de la proposition 1.3.3). Autrement dit, il existe un morphisme surjectif $R/I\to K$ où K est un corps (dont le noyau est l'idéal de R/I produit par le théorème de Krull), et composition avec la projection canonique donne un morphisme surjectif $R\to K$, dont le noyau est un idéal maximal de R contenant I.*

b. Soit $a \in R$ un élément contenu dans *aucun* idéal maximal. Montrer que a est inversible dans R.

√ *Si aR était un idéal propre, il serait contenu dans un idéal maximal (question précédente), et donc en particulier a aussi, contradiction. Donc $aR = R \ni 1$, et a est inversible.*

c. Soit $x \in R$ un élément nilpotent, disons $x^n = 0$. Montrer que tout idéal premier de R contient x.

√ *Quand un idéal premier contient un produit de plusieurs facteurs, il contient au moins un de ces facteurs (par récurrence immédiate basée sur le produit de deux facteurs). Tout idéal premier contient $0 = x^n$, et donc l'un des n facteurs x du produit ; il contient donc x. Ou encore : dans l'anneau quotient par un idéal premier, donc intègre, l'image nilpotente de x est forcément nulle.*

d. Soit I un idéal premier de $R[X]$. Montrer que $I \cap R$ est un idéal premier de R.

√ *Le quotient $R[X]/I$ est un anneau intègre, et l'image du morphisme composé $R \to R[X] \to R[X]/I$, étant un sous-anneau de celui-ci, est aussi intègre. Le noyau du morphisme composé est $I \cap R$, et c'est un idéal premier dans R. On peut aussi raisonner directement si $a, b \in R$ avec $ab \in I \cap R$, alors en particulier $ab \in I$, donc $a \in I$ ou $b \in I$, et donc $a \in I \cap R$ ou $b \in I \cap R$, respectivement.*

On suppose désormais que $a \in R$ est contenu dans tout idéal premier de R. On cherche à démontrer la réciproque de l'énoncé de la question *c*, à savoir que a est nécessairement nilpotent.

e. Montrer que a est contenu dans tout idéal maximal de $R[X]$.

√ *Un idéal maximal M de $R[X]$ est en particulier un idéal premier de $R[X]$, donc d'après la question c, $M \cap R$ est un idéal premier de R, et par conséquent il contient a.*

f. En déduire que pour cet élément $a \in R$, le polynôme $1 - aX$ est inversible dans $R[X]$.

√ *D'après la question b, il suffit de montrer que $1 - aX$ n'est dans aucun idéal maximal de $R[X]$. Mais tout tel idéal maximal M contient a (question e), et s'il contiendrait aussi $1 - aX$ on aurait $1 = (1 - aX) + Xa \in M$, contredisant le fait que les idéaux maximaux sont des idéaux propres.*

g. Trouver explicitement un inverse de $1 - aX$ dans l'anneau de séries formelles $R[[X]]$.

√ *Si $S = \sum_{i \in \mathbf{N}} a^i X^i$ désigne la série formelle suite de coefficients $(1, a, a^2, \ldots)$, on calcule coefficient par coefficient que $S(1 - aX) = 1$. Donc S est l'inverse de $1 - aX$ dans $R[[X]]$.*

h. Conclure, en observant que $R[[X]]$ contient $R[X]$ comme sous-anneau.

√ *D'une part $R[[X]]$ ne peut contenir qu'un seul inverse de $1 - aX$, la série (géométrique) S de la question f, et d'autre part $1 - aX$ possède un inverse dans le sous-anneau $R[X]$. On doit donc avoir $S \in R[X]$, ce qui veut dire que la suite de coefficients $(1, a, a^2, \ldots)$ devient nulle à partir d'un certain indice, c'est-à-dire $a^i = 0$; autrement dit a est nilpotent.*

3. On considère le sous-anneau $A = \mathbf{Z}[\sqrt{2}\,\mathbf{i}] = \{\, a + b\sqrt{2}\,\mathbf{i} \mid a, b \in \mathbf{Z} \,\}$ de $\mathbf{C}$ (similaire à celui des entiers de Gauss), dont on étudiera quelques propriétés. On a

$$(a + b\sqrt{2}\,\mathbf{i})(c + d\sqrt{2}\,\mathbf{i}) = ac - 2bd + (ad + bc)\sqrt{2}\,\mathbf{i}.$$

a. On définit $N : A \to \mathbf{Z}$ par $N(a + b\sqrt{2}\,\mathbf{i}) = a^2 + 2b^2 = (a + b\sqrt{2}\,\mathbf{i})(a - b\sqrt{2}\,\mathbf{i})$ pour $a, b \in \mathbf{Z}$ (application appelée la norme de A). Montrer que N vérifie $N(x) = |x|^2$ (le carré du module de x comme nombre complexe) ainsi que $N(xy) = N(x)N(y)$ pour tout $x, y \in A$.

√ *Si $x = a + b\sqrt{2}\,\mathbf{i}$ avec $a, b \in \mathbf{Z}$ on a $|x|^2 = a^2 + (b\sqrt{2})^2 = a^2 + 2b^2 = N(x)$. Il en découle que $N(xy) = |xy|^2 = (|x|\,|y|)^2 = |x|^2|y|^2 = N(x)N(y)$. Cette dernière identité peut aussi être obtenue directement ainsi : $N(xy) = xy\,\overline{xy} = x\overline{x}\,y\overline{y} = N(x)N(y)$, ou avec $y = c + d\sqrt{2}\,\mathbf{i}$ pour les plus courageux : $N(xy) = N(ac - 2bd + (ad + bc)\sqrt{2}\,\mathbf{i}) = (ac - 2bd)^2 + 2(ad + bc)^2 = a^2c^2 + 4b^2d^2 + 2a^2d^2 + 2b^2c^2 = (a^2 + 2b^2)(c^2 + 2d^2) = N(x)N(y)$.*

b. Montrer que les seuls éléments inversibles de A sont 1 et -1.

√ *Si $xy = 1$ on a $N(x)N(y) = N(1) = 1$, et comme $N(x), N(y) \in \mathbf{N}$ (l'expression pour $N(x)$ exclut toute valeur négative) cela n'est possible que si $N(x) = N(y) = 1$. Mais $a^2 + 2b^2 = 1$ avec $a, b \in \mathbf{Z}$ n'a que les solutions $a = \pm 1$, $b = 0$ correspondants à $x = \pm 1$.*

c. Montrer que si $\rho : \mathbf{Q} \to \mathbf{Z}$ est l'opération d'arrondir vers l'entier le plus proche (qui vérifie plus précisément $\rho(n + \alpha) = n$ pour tout $n \in \mathbf{Z}$ et $\alpha \in \mathbf{Q}$ avec $-\frac{1}{2} \leq \alpha < \frac{1}{2}$), alors pour tout $x = a + b\sqrt{2}\,\mathbf{i} \in A$ et $y = c + d\sqrt{2}\,\mathbf{i} \in A \setminus \{0\}$, l'élément $q = \rho(\frac{ac+2bd}{c^2+2d^2}) + \rho(\frac{bc-ad}{c^2+2d^2})\sqrt{2}\,\mathbf{i}$ de A vérifie $N(x - qy) < N(y)$, ce qui veut dire que A est un anneau euclidien avec N comme stathme. [Indication: on peut remarquer que dans $\mathbf{C}$ on a $x/y = \frac{ac+2bd}{c^2+2d^2} + \frac{bc-ad}{c^2+2d^2}\sqrt{2}\,\mathbf{i}$.]

√ *Si on pose $q_0 = x/y \in \mathbf{C}$, on a $-\frac{1}{2} \leq \mathrm{Re}(q_0 - q) < \frac{1}{2}$, et $-\frac{\sqrt{2}}{2} \leq \mathrm{Re}(q_0 - q) < \frac{\sqrt{2}}{2}$, et donc $|q_0 - q|^2 \leq \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1$. Or on a $x - qy = q_0 y - qy = y(q_0 - q)$, et avec l'inégalité précédente on obtient $N(x - qy) = |y|^2|q_0 - q|^2 < |y|^2 = N(y)$. Attention, éviter $N(q_0 - q)$, car $q_0 \notin A$.*

d. Soit π un élément irréductible de A. On décompose dans $\mathbf{Z}$ la norme $N(\pi)$ en nombres premiers: $N(\pi) = p_1 \cdots p_k$. Déduire du fait que π divise $N(\pi)$ dans A, que π divise (toujours dans A) l'un des nombres premiers p_i, et puis par la multiplicativité de N (question *a*) que $N(\pi)$ divise $N(p_i) = p_i^2$ dans $\mathbf{Z}$.

$\surd$ *Comme A est un anneau euclidien, il est factoriel, et l'élément irréductible π est aussi premier; alors comme π divise dans A le produit $N(\pi) = p_1 \cdots p_k$, il divise l'un des facteurs π_i. Si on pose $p_i = \pi y$ on a $N(\pi)N(y) = N(p_i) = p_i^2$, dans lequel chaque facteur appartient à $\mathbf{Z}$, donc et $N(\pi)$ divise p_i^2 dans $\mathbf{Z}$.*

e. Conclure que soit $k = 1$ (c'est-à-dire $N(\pi)$ est un nombre premier), soit $k = 2$ avec $p_1 = p_2$ (c'est-à-dire $N(\pi)$ est le carré d'un nombre premier), et que dans ce dernier cas $\pi \in \{p_1, -p_1\}$.

$\surd$ *Comme π n'est pas inversible dans A, on a $N(\pi) \neq 1$; les seuls autres diviseurs positifs de p_i^2 dans $\mathbf{Z}$ sont p_i et p_i^2. Or $N(\pi) = p_1 \cdots p_k$ est un de ces diviseurs, d'où les deux options indiquées. Dans le second cas $N(\pi) = p_1^2$, comme π divise $p_1 = p_2$ dans A (le point de départ de la question précédente), on a $N(p_1/\pi) = N(p_1)/N(\pi) = 1$, et (question b) $p_1/\pi = \pm 1$, c'est-à-dire $\pi = \pm p_1$.*

f. On se place dans le premier cas de figure : $\pi = a + b\sqrt{2}\,\mathbf{i}$ est irréductible dans A, et $N(\pi)$ est un nombre premier p ; on aura $b \neq 0$ (pourquoi?). Déduire du fait que p est réductible dans A (car $p = \pi\tilde{\pi}$ avec $\tilde{\pi} = a - b\sqrt{2}\,\mathbf{i}$) que le polynôme $X^2 + 2 \in (\mathbf{Z}/p\mathbf{Z})[X]$ est réductible dans $(\mathbf{Z}/p\mathbf{Z})[X]$. [Indication : considérer le morphisme $(\mathbf{Z}/p\mathbf{Z})[X] \to A/pA$ qui envoie $X \mapsto \sqrt{2}\,\mathbf{i}$.]

$\surd$ *Si on avait $b = 0$, on aurait $N(\pi) = a^2$ qui n'est pas un nombre premier, donc $b \neq 0$. On a $pA = \{\, pA + pb\sqrt{2}\,\mathbf{i} \mid a, b \in \mathbf{Z} \,\}$ et le noyau du morphisme $\mathbf{Z} \to A/pA$ est $p\mathbf{Z}$, on a donc bien un morphisme $\mathbf{Z}/p\mathbf{Z} \to A/pA$, qui est injectif, et un morphisme $\phi : \mathbf{Z}/p\mathbf{Z}[X] \to A/pA$ qui l'étend en envoyant $X \mapsto \sqrt{2}\,\mathbf{i}$, et qui est surjectif. Comme $\phi(\overline{a} + \overline{b}X) = \overline{a + b\sqrt{2}\,\mathbf{i}}$ pour $\overline{a}, \overline{b} \in \mathbf{Z}/p\mathbf{Z}$, le noyau de ϕ ne contient pas de polynômes de degré 0 ou 1, mais on a clairement $X^2 + 2 \in \ker(\phi)$; par conséquent $X^2 + 2 \in (\mathbf{Z}/p\mathbf{Z})[X]$ engendre l'idéal $\ker(\phi)$ de $(\mathbf{Z}/p\mathbf{Z})[X]$, et on a un isomorphisme $\hat{\phi} : (\mathbf{Z}/p\mathbf{Z})[X]/(X^2+2) \to A/pA$. Comme p est réductible dans A, l'anneau A/pA n'est pas intègre, et comme $(\mathbf{Z}/p\mathbf{Z})[X]/(X^2+2)$ n'est donc pas non plus intègre, l'élément X^2+2 de l'anneau factoriel (car $\mathbf{Z}/p\mathbf{Z}$ est une corps) $(\mathbf{Z}/p\mathbf{Z})[X]$ n'est pas premier, et donc réductible (théorème 2.2.10 du cours, partie (ii)). En fait, mais cela demande un raisonnement supplémentaire, on peut déduire d'une factorisation de p dans A une factorisation de $X^2 + 2$ dans $(\mathbf{Z}/p\mathbf{Z})[X]$: l'égalité $\pi\tilde{\pi} = p$ dans A donne une paire de diviseurs de zéro $\overline{\pi}, \overline{\tilde{\pi}}$ dans A/pA, et leurs images par $\hat{\phi}^{-1}$ forment une paire de diviseurs de zéro dans $(\mathbf{Z}/p\mathbf{Z})[X]/(X^2 + 2)$, dont les représentants dans $(\mathbf{Z}/p\mathbf{Z})[X]$ ont donc un produit qui est un multiple de $X^2 + 2$. Mais on peut choisir ces représentants de degré 1, auquel cas ce multiple ne peut être que par un polynôme constant, et donc inversible. Par exemple $(3 + 2\sqrt{2}\,\mathbf{i})(3 - 2\sqrt{2}\,\mathbf{i}) = 17$ donne $(3 + 2X)(3 - 2X) = 9 - 4X^2 = 13(X^2 + 2)$ dans $(\mathbf{Z}/17\mathbf{Z})[X]$, et donc $2 + X^2 = (3 + 2X)((3 - 2X)/13) = (3 + 2X)(12 - 8X)$ dans $(\mathbf{Z}/17\mathbf{Z})[X]$. Mais dans le sens opposé le multiple pose plus de problèmes, car par exemple $(6 + X)(-6 + X) = 2 + X^2$ dans $(\mathbf{Z}/19\mathbf{Z})[X]$ donne $(6+\sqrt{2}\,\mathbf{i})(-6+\sqrt{2}\,\mathbf{i}) = -38$ dans A, qui est bien un multiple de 19, mais comme $-38/19 = -2$ n'est pas inversible dans A, on n'obtient pas ainsi une factorisation de 19 dans A.*

g. Conclure que dans ce cas la congruence $a^2 \equiv -2 \pmod{p}$ pour $a \in \mathbf{Z}$ possède des solutions.

$\surd$ *Si $X^2 + 2$ est réductible dans $(\mathbf{Z}/p\mathbf{Z})[X]$, il possède au moins une racine r dans $\mathbf{Z}/p\mathbf{Z}$, et les représentants $a \in \mathbf{Z}$ de r seront des solutions de la congruence $a^2 \equiv -2 \pmod{p}$.*

h. Prenons maintenant réciproquement un entier $a \in \mathbf{Z}$ et un nombre premier p qui divise $a^2 + 2$. Montrer qu'en calculant $\pi = \mathrm{pgcd}(a+\sqrt{2}\,\mathbf{i}, p)$ dans l'anneau euclidien A, on trouvera un élément irréductible π de A avec $N(\pi) = p$.

$\surd$ *On aura $(a+\sqrt{2}\,\mathbf{i})(a-\sqrt{2}\,\mathbf{i}) = a^2+2 \in p\mathbf{Z}$, et comme p ne divise aucun des facteurs $a+\sqrt{2}\,\mathbf{i}, a-\sqrt{2}\,\mathbf{i}$ de ce produit dans A, il n'est par irréductible dans A. Si π est un diviseur irréductible de p dans A, sa norme divise $N(p) = p^2$, mais $N(\pi) \neq p^2$, car sinon $\pi = \pm p$ (question d) contredisant p réductible dans A. Donc $N(\pi) = p = \pi\tilde{\pi}$. Comme π est premier dans A et divise $(a + \sqrt{2}\,\mathbf{i})(a - \sqrt{2}\,\mathbf{i})$, il divise l'un des deux facteurs, et alors $\tilde{\pi}$ divisera l'autre facteur ; quitte à intervertir π et $\tilde{\pi}$ on peut supposer que $\pi \mid a + \sqrt{2}\,\mathbf{i}$ et alors $\pi = \mathrm{pgcd}(a + \sqrt{2}\,\mathbf{i}, p)$ est un élément irréductible avec $N(\pi) = p$.*

i. Trouver concrètement $k, l \in \mathbf{N}$ avec $k^2 + 2l^2 = 1667$ (qui est un facteur premier de 10002).

$\surd$ *Pour $x = 1667$ et $y = 100 + \sqrt{2}\,\mathbf{i}$ dans la question c, donc $a = 1667$ $b = 0$, $c = 100$, $d = 1$, on trouve $q = \rho(\frac{ac+2bd}{c^2+2d^2}) + \rho(\frac{bc-ad}{c^2+2d^2})\sqrt{2}\,\mathbf{i} = 17 + 0\sqrt{2}\,\mathbf{i}$ et $x - qy = -33 - 17\sqrt{2}\,\mathbf{i}$, dont la norme $N(-33 - 17\sqrt{2}\,\mathbf{i}) = 33^2 + 2 \times 17^2 = 1089 + 2 \times 289 = 1667$ est effectivement plus petit que $N(y) = 100^2 + 2 = 10002$. En fait on a déjà trouvé un élément de A dont la norme est 1667, et en fait le prochain quotient $y/(x - qy) = (100 + \sqrt{2}\,\mathbf{i})/-(33 + 17\sqrt{2}\,\mathbf{i}) = -(2 - \sqrt{2}\,\mathbf{i})$ est exact dans A, ce qui établit $33 + 17\sqrt{2}\,\mathbf{i} = \mathrm{pgcd}(100 + \sqrt{2}\,\mathbf{i}, 1667)$ dans A. La solution est donc $k = 33$, $l = 17$.*

Fin.