Exercice 1 - Groupe de Heisenberg

1. Soit $(x,y,z,x',y',z') \in \mathbb{K}^6$. Comme les matrices considérées sont triangulaires supérieures, on sait que leur produit est triangulaire supérieur et que la diagonale du produit est constituée des produits des coefficients des diagonales de chaque matrice. Dans notre cas, la diagonale du produit est uniquement constituée de 1. Il ne nous reste qu'à déterminer les coefficients de places $(1,2),(1,3)$ et $(2,3)$.

$$\begin{pmatrix}1 & x & z\\ 0 & 1 & y\\ 0 & 0 & 1\end{pmatrix}\begin{pmatrix}1 & x' & z'\\ 0 & 1 & y'\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & 1\times x' + x\times 1 & 1\times z' + x\times y' + z\times 1\\ 0 & 1 & 0\times z' + 1\times y' + y\times 1\\ 0 & 0 & 1\end{pmatrix} = \begin{pmatrix}1 & x+x' & z+z'+xy'\\ 0 & 1 & y+y'\\ 0 & 0 & 1\end{pmatrix}$$

   On identifie bien alors

$$h(x,y,z)h(x',y',z') = h(x+x', y+y', z+z'+xy')$$

2. Soit $(x,y,z) \in \mathbb{K}^3$. Grâce au résultat précédent, on a les produits matriciels suivants :

$$h(x,y,z)h(-x,-y,-z+xy) = h(x-x, y-y, z+(-z+xy)+x(-y)) = h(0,0,0) = I_3$$

$$h(-x,-y,-z+xy)h(x,y,z) = h(-x+x, -y+y, -z+xy+z+(-x)y) = h(0,0,0) = I_3$$

   Comme I_3 est le neutre de la multiplication dans l'anneau $\mathcal{M}_3(\mathbb{K})$, on a trouvé un symétrique de $h(x,y,z)$ pour cette loi. Ainsi, $h(x,y,z)$ est inversible et son inverse vaut $h(-x,-y,-z+xy)$.

3. La question précédente assure que $\mathcal{H}_3(\mathbb{K})$ est inclus dans $GL_3(\mathbb{K})$. De plus, d'après la question 1, cette partie est stable par multiplication. La question 2 a également montré qu'elle est stable par inverse. Enfin, $I_3 = h(0,0,0)$ appartient à $\mathcal{H}_3(\mathbb{K})$. On a ainsi vérifié tous les critères suffisants pour établir que $\mathcal{H}_3(\mathbb{K})$ est un sous-groupe de $GL_3(\mathbb{K})$.

4. Pour tout entier naturel n, on note H_n l'assertion :

$$\forall (x,y,z) \in \mathbb{K}^3, \quad h(x,y,z)^n = h\left(nx, ny, nz + \frac{n(n-1)}{2}xy\right)$$

   et on la démontre par récurrence sur n. Pour $n=0$, on retrouve la convention $h(x,y,z)^0 = I_3$. Pour $n=1$, il s'agit d'une trivialité. Soit n un entier naturel tel que H_n est vraie. Démontrons l'assertion H_{n+1}. Soit $(x,y,z) \in \mathbb{K}^3$.

$$\begin{aligned}
h(x,y,z)^{n+1} &= h(x,y,z)^n h(x,y,z)\\
&= h\left(nx, ny, nz + \frac{n(n-1)}{2}xy\right)h(x,y,z) \quad \text{d'après l'hypothèse de récurrence}\\
&= h\left(nx+x, ny+y, nz + \frac{n(n-1)}{2}xy + z + nxy\right) \quad \text{d'après la question 1}\\
&= h\left((n+1)x, (n+1)y, (n+1)z + nxy\left(\frac{n-1}{2}+1\right)\right)\\
&= h\left((n+1)x, (n+1)y, (n+1)z + n\frac{n+1}{2}xy\right)
\end{aligned}$$

   En conclusion, l'assertion est démontrée par récurrence.

5. La réponse est négative. Pour cela, on assemble les produits matriciels suivants :

$$h(1,0,0)h(0,1,0) = h(1,1,1)$$

$$h(0,1,0)h(1,0,0) = h(1,1,0)$$

   Ces deux matrices sont distinctes puisque leurs coefficients de place $(1,3)$ sont distincts. Ainsi, le groupe $\mathcal{H}_3(\mathbb{K})$ n'est pas commutatif.

6. Soit $(x,y,z,x',y',z') \in \mathbb{K}^6$.

$$\begin{aligned} f(h(x,y,z)h(x',y,',z')) &= f(h(x+x',y+y',z+z'+xy')) \quad \text{d'après la question 1} \\ &= (x+x',y+y') \quad \text{d'après la définition de } f \\ &= (x,y)+(x',y') \quad \text{d'après la structure de groupe produit de } \mathbb{K}^2 \\ &= f(h(x,y,z))+f(h(x',y',z')) \quad \text{d'après la définition de } f \end{aligned}$$

Ainsi, f est un morphisme de groupes.

7. Soit $(x,y,z) \in \mathbb{K}^3$ tel que $f(h(x,y,z)) = 0_{\mathbb{K}^2} = (0,0)$. D'après la définition de f, cela implique $(x,y) = (0,0)$, donc $x = 0$ et $y = 0$. Ainsi,

$$\ker f \subset \{h(0,0,z) | z \in \mathbb{K}\}$$

Réciproquement, soit $z \in \mathbb{K}$, alors $f(h(0,0,z)) = (0,0)$, donc $h(0,0,z) \in \ker f$. En conclusion, $\ker f = \{h(0,0,z) | z \in \mathbb{K}\}$. En particulier, $h(0,0,1)$ appartient au noyau de f et est distinct de I_3, donc f n'est pas injective.

8. D'après la question 4, $h(1,1,0)^2 = h(2,2,1)$. Or, d'après la définition de g, $2g(h(1,1,0)) = 2(1,1,0) = (2,2,0)$ alors que $g(h(2,2,1)) = (2,2,1)$. On en déduit que

$$g\left(h(1,1,0)^2\right) \neq 2g(h(1,1,0))$$

donc que g n'est pas un morphisme de groupes.

Exercice 2 - Les entiers de Gauss

1. (a) On mène les vérifications d'usage. $1 = 1 + 0\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$. Soit $(a,b,a',b') \in \mathbb{Z}^4$. Alors, d'après la commutativité et la distributivité dans $\mathbb{C}$,

$$(a+b\mathrm{i})+(a'+b'\mathrm{i}) = (a+a')+(b+b')\mathrm{i}$$

Comme $\mathbb{Z}$ est un anneau, $a+a' \in \mathbb{Z}$ et $b+b' \in \mathbb{Z}$, donc $(a+b\mathrm{i})+(a'+b'\mathrm{i}) \in \mathbb{Z}[\mathrm{i}]$, ainsi cette partie de $\mathbb{C}$ est stable par addition. D'autre part,

$$(a+b\mathrm{i})(a'+b'\mathrm{i}) = (aa'-bb')+(ba'+ab')\mathrm{i}$$

Comme $\mathbb{Z}$ est un anneau, $(a+b\mathrm{i})(a'+b'\mathrm{i}) \in \mathbb{Z}[\mathrm{i}]$ et cette partie est stable par multiplication. Enfin, $-a-b\mathrm{i}$ est l'inverse pour l'addition de $a+b\mathrm{i}$ d'après la commutativité de $\mathbb{C}$. Tous les critères sont vérifiés et $\mathbb{Z}[\mathrm{i}]$ est un sous-anneau de $\mathbb{C}$.

(b) Soit $(a,b,a',b') \in \mathbb{Z}^4$. Comme la multiplication dans $\mathbb{C}$ est commutative, on a

$$(a+b\mathrm{i})(a'+b'\mathrm{i}) = (a'+b'\mathrm{i})(a+b\mathrm{i})$$

Ainsi, l'anneau est commutatif. De plus, $\mathbb{C}$ est intégre, donc si $(a+b\mathrm{i})(a'+b'\mathrm{i}) = 0$, alors $a+b\mathrm{i} = 0$ ou $a'+b'\mathrm{i} = 0$. On en déduit que $\mathbb{Z}[\mathrm{i}]$ est intègre.

(c) On reconnaît la restriction à $\mathbb{Z}[\mathrm{i}]$ du carré du module complexe, dont on sait qu'il est multiplicatif. Plus pédestrement, soit $(a,b,a',b') \in \mathbb{Z}^4$.

$$\begin{aligned} \mathrm{N}((a+b\mathrm{i})(a'+b'\mathrm{i})) &= \mathrm{N}((aa'-bb')+(ba'+ab')\mathrm{i}) \\ &= (aa'-bb')^2+(ba'+ab')^2 \\ &= (aa')^2+(bb')^2+(ba')^2+(ab')^2 \\ &= (a^2+b^2)(a'^2+b'^2) \\ &= \mathrm{N}(a+b\mathrm{i})\mathrm{N}(a'+b'\mathrm{i}) \end{aligned}$$

(d) Procédons par double implication. Supposons tout d'abord z inversible et notons z' son inverse. D'après la question précédente, $N(z)N(z') = N(zz') = N(1) = 1$. Comme $z' \in \mathbb{Z}[i]$ et N est à valeurs dans $\mathbb{N}$, $N(z)$ divise 1, donc $N(z) = 1$. Réciproquement, supposons que $N(z) = 1$ et montrons que z est inversible. Pour cela, on note $z' = \overline{z}$ le conjugué de z dans $\mathbb{C}$. Alors $zz' = z\overline{z} = |z|^2 = N(z) = 1$. Comme l'anneau est commutatif, cela prouve que $\overline{z}$ est l'inverse de z. De plus, $\overline{z}$ appartient clairement à $\mathbb{Z}[i]$, puisque $-\mathrm{Im}(z) \in \mathbb{Z}$. Ainsi, l'inverse de z est bien dans $\mathbb{Z}[i]$.

(e) D'après la question précédente, il suffit de chercher les couples d'entiers relatifs $(a,b) \in \mathbb{Z}^2$ tels que $a^2 + b^2 = 1$. Soit (a,b) un tel couple. Alors $a^2 \leq a^2 + b^2 = 1$, donc $a \in \{-1,0,1\}$. De même, $b^2 \leq a^2 + b^2 = 1$, donc $b \in \{-1,0,1\}$. De plus, $a^2 = 1 \iff b = 0$ et $b^2 = 1 \iff a = 0$. Il ne nous reste ainsi que quatre possibilités $\{(1,0),(-1,0),(0,1),(0,-1)\}$. Ainsi, $\mathbb{Z}[i]^\times = \{1,-1,i,-i\}$.

2. (a) On note $v = z/w$. On note alors $(x,y) \in \mathbb{R}^2$ tel que $v = x + yi$. On pose alors $x' = \lfloor x \rfloor$ si $\{x\} \leq 1/2$ et $x' = \lfloor x \rfloor + 1$ si $\{x\} > 1/2$. De même, on pose $y' = \lfloor y \rfloor$ si $\{y\} \leq 1/2$ et $y' = \lfloor y \rfloor + 1$ si $\{y\} > 1/2$. Dans tous les cas, $(x',y') \in \mathbb{Z}^2$ et

$$|v - (x' + y'i)|^2 = (x-x')^2 + (y-y')^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1$$

On pose alors $q = x' + y'i$ et $r = z - qw$, ces deux éléments sont bien dans $\mathbb{Z}[i]$ et vérifient $z = qw + r$. De plus, comme w est non nul,

$$0 \leq N(r) = |w(v-q)|^2 = |w|^2|v-q|^2 < |w|^2 = N(w)$$

(b) On reprend la méthode précédente, $v = \frac{7+3i}{2+3i} = \frac{(7+2i)(2-3i)}{13} = \frac{20}{13} + \frac{-17}{13}i$. On pose alors $q = 2 - i$ et $r = z - qw = i$. On retrouve bien sûr $N(r) = 1 < 13 = N(w)$.

3. (a) On a $2 = (1+i)(1-i)$ et d'après la liste des inversibles faite en question 1.e), ni $1+i$ ni $1-i$ ne sont inversibles, donc 2 n'est pas irréductible dans $\mathbb{Z}[i]$. Soit $3 = st$ une factorisation de 3 dans $\mathbb{Z}[i]$. Comme l'application N est multiplicative, on en déduit que $N(s)N(t) = N(3) = 9$. Comme $N(s)$ et $N(t)$ sont des entiers naturels, on en déduit d'après les diviseurs positifs de 9 dans $\mathbb{N}$, que $N(s) \in \{1,3,9\}$. Supposons un instant que $N(s) = 3$. On dispose de $(a,b) \in \mathbb{Z}^2$ tel que $s = a + bi$), donc $a^2 + b^2 = 3$. De même qu'en question 1.e), on a $a^2 \leq 3$, donc $a^2 = 0$ ou $a^2 = 1$. Si $a^2 = 0$, alors $b^2 = 3$, ce qui est impossible, puisque b est entier. Si $a^2 = 1$, alors $b^2 = 2$, ce qui est encore impossible. Conclusion, $N(s) \neq 3$, donc $N(s) = 1$ ou $N(s) = 9$. Dans le premier cas, s est inversible. Dans le second cas, $N(w) = 1$ et w est inversible. Ainsi, les seules factorisations de 3 dans $\mathbb{Z}[i]$ sont les factorisations triviales. Comme 3 est non inversible et non nul, 3 est irréductible dans $\mathbb{Z}[i]$.

(b) Notons $a + bi = st$ une factorisation de w dans $\mathbb{Z}[i]$. Alors $p = a^2 + b^2 = N(w) = N(s)N(t)$. Comme $N(s)$ et $N(t)$ sont des entiers, $N(s)$ et $N(t)$ divisent l'entier premier p. Par conséquent, $N(s) = 1$ ou $N(t) = 1$, donc s ou t est inversible. De plus, w n'est pas inversible car sa norme ne vaut pas 1, puisque 1 n'est pas premier dans $\mathbb{Z}$. Enfin, w est non nul, puisque sa norme est non nulle. Conclusion, w est irréductible dans $\mathbb{Z}[i]$. Comme $\overline{w}$ est de même norme, le même raisonnement se reproduit à l'identique et $\overline{w}$ est irréductible dans $\mathbb{Z}[i]$.

(c) Suivons l'indication, supposons qu'il existe un triplet (w,a,b) tel que w irréductible, w divise ab, mais w ne divise ni a ni b. Nécessairement, b est non nul, puisque tout le monde divise 0. On sélectionne parmi ceux-là un triplet tel que $N(b)$ est minimal, ceci est possible puisque N est à valeurs dans $\mathbb{N}$. D'après la question 2.a, on dispose d'entiers de Gauss q et r tels que $w = qb + r$ et $N(r) < N(b)$ puisque b est non nul. Mais alors $ar = aw - qab = aw - qvw = w(a - qv)$ est multiple de w. Ainsi, (w,a,r) est un triplet qui vérifie les mêmes conditions qu'au départ. Par minimalité de $N(b)$, on en déduit que $N(r) = 0$, donc que $r = 0$ et $w = qb$. Comme w est irréductible, cela entraîne que b est inversible ou associé à w. Si b est inversible, alors w divise a, mais ne divise pas a, ce qui est absurde. Dans le second cas, w divise b, mais ne divise pas b, ce qui est absurde.

Conclusion, w divise a ou b.

(d) Soit z un entier de Gauss de norme p. Alors $z\overline{z} = N(z) = p = w\overline{w}$. Ainsi, w divise le produit $z\overline{z}$ dans $\mathbb{Z}[i]$. Comme w est irréductible, la question précédente assure que w divise z ou $\overline{z}$.

Dans le premier cas, il existe un entier de Gauss u tel que $wu = z$. Mais alors $N(w)N(u) = N(z)$, donc $N(u) = 1$ et u est inversible. Il appartient alors à $\{1, -1, i, -i\}$ d'après la question 1.e) et $z = u(a + ib)$. Dans le second cas, il existe un entier de Gauss u tel que $wu = \overline{z}$ et on conclut de la même manière que u est inversible et $z = u(a - ib)$.

(e) Comme q n'est pas somme de deux carrés d'entiers, il n'est pas la norme d'un élément de $\mathbb{Z}[i]$. Soit $q = st$ une factorisation de q dans $\mathbb{Z}[i]$. Alors $N(q) = q^2 = N(s)N(t)$. De même que précédemment, $N(s)$ et $N(t)$ sont des entiers naturels, donc on a une factorisation de q^2 dans $\mathbb{N}$. Par conséquent, $N(s) \in \{1, q, q^2\}$. On a vu que $N(s) \neq q$ car sinon q s'écrirait comme somme de carrés d'entiers. Idem pour $N(t)$. Ainsi, $N(s) = 1$ ou $N(t) = 1$ et s ou t est inversible. D'autre part, q est clairement non nul et non inversble dans $\mathbb{Z}[i]$, donc q est irréductible dans $\mathbb{Z}[i]$.

Exercice 3 - Une extension quadratique

1. (a) Comme $\mathbb{K}$ est un sous-corps de $\mathbb{Q}$, il contient 1. D'autre part, pour tout entier naturel n non nul, si n appartient à $\mathbb{K}$, alors par stabilité additive, $n + 1$ appartient à $\mathbb{K}$. Ainsi, $\mathbb{K}$ contient $\mathbb{N}^*$ par récurrence. D'autre part, il contient également 0, puisque c'est le neutre additif de $\mathbb{Q}$. Comme $\mathbb{K}$ est stable par passage à l'opposé, il contient $\mathbb{Z}$. Soit $q \in \mathbb{Q}$, on l'écrit sous la forme n/m avec $n \in \mathbb{Z}$ et $m \in \mathbb{N}^*$. Comme $\mathbb{K}$ est un sous-corps, il est stable par passage à l'inverse, donc $1/m \in \mathbb{K}$. On en déduit par stabilité multiplicative, que n/m appartient à $\mathbb{K}$, donc que $q \in \mathbb{K}$. En conclusion, $\mathbb{K}$ contient $\mathbb{Q}$.

   (b) L'intersection est non vide puisque $\mathbb{C}$ est un corps qui contient A. La partie $\mathbb{Q}(A)$ est une intersection de sous-corps de $\mathbb{C}$, donc un sous-corps de $\mathbb{C}$. D'autre part, c'est une intersection de parties qui contiennent toutes A, donc $\mathbb{Q}(A)$ contient A. Soit à présent L un sous-corps de $\mathbb{C}$ qui contient A, alors il fait partie de la liste des sous-corps de $\mathbb{C}$ qui contiennent A, par conséquent, $\mathbb{Q}(A) \subset L$. Ainsi, $\mathbb{Q}(A)$ est le plus petit (au sens de l'inclusion) sous-corps de $\mathbb{C}$ qui contient A.

   (c) Suivons l'indication, notons $L = \left\{a + b\sqrt{2} \mid (a, b) \in \mathbb{Q}^2\right\}$ et montrons que L est un sous-corps de $\mathbb{C}$. La stabilité par addition et stabilité par passage à l'opposé est laissée à votre sagacité. D'autre part $1 = 1 + 0 \times \sqrt{2}$ appartient à L. Soit $(a, b, a', b') \in \mathbb{Q}^4$, alors

$$(a + b\sqrt{2})(a' + b'\sqrt{2}) = aa' + 2bb' + (a'b + ab')\sqrt{2}$$

   appartient clairement à L puisque $\mathbb{Q}$ est un corps. Soit x un élément non nul de L. On note $(a, b) \in \mathbb{Q}^2$ tel que $x = a + b\sqrt{2}$. Alors $a - b\sqrt{2}$ est non nul, car $\sqrt{2}$ est irrationnel. De plus, $a^2 - 2b^2$ est non nul car sinon $x(a - b\sqrt{2}) = a^2 - 2b^2 = 0$ et x serait nul par intégrité de $\mathbb{R}$, ce qui est faux. On pose alors

$$y = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}$$

   C'est clairement un élément de L et $xy = yx = 1$. Ainsi, L est un sous-corps de $\mathbb{C}$. De plus, $\sqrt{2} = 0 + 1 \times \sqrt{2}$ appartient à L, donc L contient $Q(\sqrt{2})$. D'autre part, $\mathbb{Q}(\sqrt{2})$ contient $\mathbb{Q}$ car c'est un sous-corps de $\mathbb{C}$, il contient alors tout élément de la forme $a + b\sqrt{2}$, $(a, b) \in \mathbb{Q}^2$, donc $Q(\sqrt{2}) \supset L$ et l'égalité est prouvée par double inclusion.

2. (a) On procède comme en 1.a). Comme f est un morphisme de corps, $f(1) = 1$. Pour tout entier naturel non nul n, si $f(n) = n$, alors $f(n + 1) = f(n) + f(1) = n + 1$. Il s'ensuit par récurrence que $\forall n \in \mathbb{N}, f(n) = n$. De plus, $f(0) = 0$ par absorption de 0. Par passage à l'opposé, $\forall n \in \mathbb{Z}, f(n) = n$. Soit $q \in \mathbb{Q}$, on l'écrit sous la forme n/m avec $n \in \mathbb{Z}$ et $m \in \mathbb{N}^*$. Alors $f(q) = f\left(\frac{n}{m}\right) = \frac{f(n)}{f(m)} = \frac{n}{m} = q$.

   (b) Comme $\sqrt{2}^2 = 2$ et $2 \in \mathbb{Q}$, on en déduit, d'après ce qui précède, que

$$f\left(\sqrt{2}\right)^2 = f\left(\sqrt{2}^2\right) = f(2) = 2$$

   Par conséquent, les seules valeurs possibles pour $f\left(\sqrt{2}\right)$ sont $\sqrt{2}$ et $-\sqrt{2}$.

(c) Procédons par analyse-synthèse. Phase d'analyse : soit f un automorphisme de corps de $\mathbb{Q}(\sqrt{2})$. En particulier, c'est un morphisme de corps. D'après les questions précédentes, nous n'avons que deux possibilités :

$$\forall (a,b) \in \mathbb{Q}^2, f(a+b\sqrt{2}) = f(a) + f(b)f(\sqrt{2}) = a + b\sqrt{2}$$

ou alors

$$\forall (a,b) \in \mathbb{Q}^2, f(a+b\sqrt{2}) = f(a) + f(b)f(\sqrt{2}) = a - b\sqrt{2}$$

Phase de synthèse : L'application identité de $\mathbb{Q}(\sqrt{2})$ est clairement un automorphisme de corps de $\mathbb{Q}(\sqrt{2})$. Notons d'autre part, $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2}), a + b\sqrt{2} \mapsto a - b\sqrt{2}$. Alors, $\sigma(1) = \sigma(1 + 0\sqrt{2}) = 1 - 0\sqrt{2} = 1$. L'addivité de σ est laissée à votre bon soin. Soit $(a, b, a', b') \in \mathbb{Q}^4$.

$$\begin{aligned}
\sigma((a+b\sqrt{2})(a'+b'\sqrt{2})) &= \sigma(aa' + 2bb' + (a'b + ab')\sqrt{2}) \\
&= aa' + 2bb' - (a'b + ab')\sqrt{2} \\
&= aa' + 2(-b)(-b') + (a'(-b) + a(-b'))\sqrt{2} \\
&= (a - b\sqrt{2})(a' - b'\sqrt{2}) \\
&= \sigma(a+b\sqrt{2})\sigma(a'+b'\sqrt{2})
\end{aligned}$$

Ainsi, σ est un morphisme de corps. D'autre part, on a clairement $\sigma^2 = \mathrm{Id}_{\mathbb{Q}(\sqrt{2})}$, donc σ est bijective, donc un automorphisme de corps.
En conclusion, $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \{\mathrm{Id}_{\mathbb{Q}(\sqrt{2})}, \sigma\}$.

3. (a) Le plus efficace est d'isoler $\sqrt{2}$ puis d'élever au carré. On a $(z-a)^2 = 2b^2$, soit $z^2 - 2az + (a^2 - 2b^2) = 0$. On pose alors $P = X^2 - 2aX + (a^2 - 2b^2)$. Comme a et b sont rationnels, ce polynôme est de degré 2, unitaire et à coefficients dans $\mathbb{Q}$. Si on dispose d'un polynôme unitaire de degré 1 à coefficients dans $\mathbb{Q}$ tel que $P(z) = 0$, alors P est de la forme $X - \alpha$ avec α un rationnel. Mais alors $P(z) = a - \alpha + b\sqrt{2} = 0$. Comme $\sqrt{2}$ est irrationnel, on en déduit que $b = 0$ et $a = \alpha$. En conclusion, si $z \in \mathbb{Q}$, le plus petit polynôme satisfaisant est $X - a$, sinon il s'agit du polynôme $X^2 - 2aX + (a^2 - 2b^2)$.

   (b) Supposons que a n'est pas entier. On écrit alors $2a = a'$ avec a' un entier relatif impair. D'autre part, $a^2 - 2b^2 = \frac{a'^2}{4} - 2\frac{r^2}{s^2}$ appartient à $\mathbb{Z}$, notons-le n. On écrit plus harmonieusement, $4s^2n = a'^2s^2 - 8r^2$. Alors 4 divise a'^2s^2 tandis que a' est impair, on en déduit que s est pair. On écrit alors $s = 2s'$ et l'égalité précédente devient $4s'^2n = a'^2s'^2 - 2r^2$. Mais alors s'^2 divise $2r^2$ et s' est premier avec r comme r/s est l'écriture irréductible de b. D'après le lemme de Gauss, on tire que s'^2 divise 2. Comme 2 est sans facteurs carrés, cela impose $s' = 1$. On en déduit que $4n = a'^2 - 2r^2$. D'autre part, $s = 2$, donc r est impair. Par conséquent, en raisonnant modulo 4, on constate que tout les carrés d'entiers impairs sont congrus à 1 modulo 4. Cela amène $2 \equiv 1[4]$, ce qui est absurde. Ainsi, a appartient à $\mathbb{Z}$.
   Mais alors, $2b^2$ est entier et avec les mêmes notations que précédemment, s^2 divise $2r^2$ et s est premier avec r. D'après le lemme de Gauss, s^2 divise 2. Comme 2 est sans facteurs carrés, cela impose $s = 1$. Cela entraîne que b est entier.

   ☞ **Remarque**
   Cette dernière conclusion fonctionne encore avec $\sqrt{3}$, mais pas avec $\sqrt{5}$.