Des anneaux et des oiseaux

1. (a) L'existence de l'écriture est garantie par la définition de $\mathbb{Z}[\sqrt{2}]$. Il reste à démontrer l'unicité, pour cela supposons que $x \in \mathbb{Z}[\sqrt{2}]$ ait deux écritures : $x = a + b\sqrt{2} = c + d\sqrt{2}$ où $(a, b, c, d) \in \mathbb{Z}^4$. Par soustraction, cela implique que $(a - c) + (b - d)\sqrt{2} = 0$, il y a deux cas à considérer :
   - ▶ Si $b = d$, on obtient immédiatement $a = c$.
   - ▶ Si $b \neq d$, on a $\sqrt{2} = \dfrac{c - a}{b - d}$. Ceci est absurde car $\sqrt{2}$ est irrationnel.

   On est toujours dans le premier cas et l'écriture est unique.

$$\boxed{\forall x \in \mathbb{Z}[\sqrt{2}],\ \exists!(a, b) \in \mathbb{Z}^2,\ x = a + b\sqrt{2}}$$

   (b) Nous allons démontrer que $\mathbb{Z}[\sqrt{2}]$ est un sous-anneau de l'anneau $(\mathbb{R}, +, \times)$.
   - ▶ Déjà $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ par définition.
   - ▶ Montrons que $(\mathbb{Z}[\sqrt{2}], +)$ est un sous-groupe de $(\mathbb{R}, +)$:
     - $0 = 0 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$
     - Soient $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$ avec $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ où $(a, b, c, d) \in \mathbb{Z}^4$. On a :

$$x + y = (a + c) + (b + d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \text{ car } a + c \in \mathbb{Z} \text{ et } b + d \in \mathbb{Z}$$

     - Soit $x \in \mathbb{Z}[\sqrt{2}]$ avec $x = a + b\sqrt{2}$ où $(a, b) \in \mathbb{Z}^2$. On a :

$$-x = -a - b\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \text{ car } -a \in \mathbb{Z} \text{ et } -b \in \mathbb{Z}$$

   - ▶ $1 = 1 + 0\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
   - ▶ Soient $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$ avec $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ où $(a, b, c, d) \in \mathbb{Z}^4$. On a :

$$xy = (ac + 2bd) + (ad + bc)\sqrt{2} \in \mathbb{Z}[\sqrt{2}] \text{ car } ac + 2bd \in \mathbb{Z} \text{ et } ad + bc \in \mathbb{Z}$$

$$\boxed{\mathbb{Z}[\sqrt{2}] \text{ est un sous-anneau de } \mathbb{R}}$$

   L'anneau $\mathbb{Z}[\sqrt{2}]$ est commutatif et intègre car c'est un sous-anneau de $\mathbb{R}$ qui est commutatif et intègre.

   (c) Vérifions les trois propriétés requises pour avoir un morphisme d'anneaux. Dans cette question, on se donne deux éléments de $\mathbb{Z}[\sqrt{2}]$ que l'on note $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ avec $(a, b, c, d) \in \mathbb{Z}^4$.
   - ▶ On a :

$$\varphi(x + y) = \varphi((a + c) + (b + d)\sqrt{2}) = (a + c) - (b + d)\sqrt{2} = (a - b\sqrt{2}) + (c - d\sqrt{2}) = \varphi(x) + \varphi(y)$$

   - ▶ D'autre part :

$$\varphi(xy) = \varphi((ac + 2bd) + (ad + bc)\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}) = \varphi(x)\varphi(y)$$

   - ▶ Enfin, il est clair que $\varphi(1) = 1$.

   L'application φ est bijective car $\varphi \circ \varphi = \mathrm{id}_{\mathbb{Z}[\sqrt{2}]}$.

$$\boxed{\varphi \text{ est un automorphisme de } \mathbb{Z}[\sqrt{2}]}$$

(d) Soient $(x, y) \in \mathbb{Z}[\sqrt{2}]^2$ avec $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ où $(a, b, c, d) \in \mathbb{Z}^4$. On a :

$$N(xy) = N((ac + 2bd) + (ad + bc)\sqrt{2}) = (ac + 2bd)^2 - 2(ad + bc)^2 = (ac)^2 + 4(bd)^2 - 2(ad)^2 - 2(bc)^2$$

D'autre part :

$$N(x)N(y) = (a^2 - 2b^2)(c^2 - 2d^2) = (ac)^2 - 2(ad)^2 - 2(bc)^2 + 4(bd)^2$$

Ce qui démontre le résultat voulu.

$$\boxed{N \text{ est multiplicative}}$$

(e) Démontrons le résultat par double implication, on a :

($\Rightarrow$) Soit $x \in \mathbb{Z}[\sqrt{2}]^\times$, il existe $y \in \mathbb{Z}[\sqrt{2}]$ tel que $xy = 1$. En prenant la norme, il vient $N(xy) = N(1) = 1$, c'est-à-dire $N(x)N(y) = 1$. Or, par définition, $N(x)$ et $N(y)$ sont des entiers relatifs, on a nécessairement $N(x) = \pm 1$.

($\Leftarrow$) Réciproquement soit $x \in \mathbb{Z}[\sqrt{2}]$ avec $x = a + b\sqrt{2}$ où $(a, b) \in \mathbb{Z}^2$ tel que $N(x) = \pm 1$. On pose $y = (a - b\sqrt{2})N(x)$, on a :

$$xy = (a + b\sqrt{2})(a - b\sqrt{2})N(x) = (a^2 - 2b^2)N(x) = N(x)^2 = 1$$

Ainsi x est un élément inversible de $\mathbb{Z}[\sqrt{2}]$ et l'on a même trouvé l'expression de son inverse.
On vient de démontrer le critère qui va nous servir dans toute la suite de l'exercice :

$$\boxed{x \in \mathbb{Z}[\sqrt{2}]^\times \Leftrightarrow N(x) = \pm 1}$$

(f) Par une récurrence immédiate, on démontre que pour tout entier naturel n, $N(x^n) = N(x)^n$ en utilisant la propriété de multiplicativité de N. Ainsi pour tout entier naturel n, on a :

$$N(\pm(1 \pm \sqrt{2})^n) = N(\pm 1)N(1 \pm \sqrt{2})^n = 1 \times (-1)^n = (-1)^n$$

D'après le critère démontré à la question précédente, cela suffit pour affirmer que :

$$\boxed{\forall n \in \mathbb{N},\ \pm(1 \pm \sqrt{2})^n \in \mathbb{Z}[\sqrt{2}]^\times}$$

2. (a) Les quatre éléments en question ont la même norme : $a^2 - 2b^2$. Si l'un d'entre eux est inversible sa norme vaut ± 1 et par suite la norme des trois autres éléments vaut également ± 1 d'où leur inversibilité.

(b) i. Si $a = 0$ alors $N(x) = -2b^2$ ne peut être égal à ± 1 et par suite x ne peut pas être inversible. Ce qui est contraire à l'hypothèse de départ.

$$\boxed{\text{Si } a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times \text{ alors } a \neq 0}$$

ii. Si $b = 0$, on a $N(x) = a^2 = \pm 1$ puisque x est supposé inversible. Ainsi $a = 1$ puisque le cas $a = -1$ est à exclure comme l'on a supposé que $a \in \mathbb{N}$.

$$\boxed{\text{Si } b = 0 \text{ alors } x = 1}$$

iii. On suppose $b \neq 0$, comme x est inversible on a $N(x) = a^2 - 2b^2 = \pm 1$. D'une part :

$$a^2 \leq 2b^2 + 1 < 2b^2 + 2b^2 = 4b^2 \text{ en utilisant } 1 < 2b^2 \text{ puisque } b \text{ est un entier strictement positif}$$

Par croissance de la fonction racine carrée, étant donné que a et b sont positifs, l'inégalité précédente implique $a < 2b$.
D'autre part :

$$a^2 - 2b^2 = \pm 1 \geq -1 \text{ ce qui implique que } 2b^2 \leq a^2 + 1 \leq 2a^2 \text{ car } 1 \leq a^2$$

Ce qui démontre que $b \leq a$

$$\boxed{\text{Si } b \neq 0 \text{ alors } b \leq a < 2b}$$

iv. On a :

$$\frac{x}{1+\sqrt{2}} = \frac{x(1-\sqrt{2})}{(1+\sqrt{2})(1-\sqrt{2})} = -x(1-\sqrt{2}) = (2b-a) + (a-b)\sqrt{2}$$

$$\boxed{\frac{x}{1+\sqrt{2}} = (2b-a) + (a-b)\sqrt{2}}$$

v. Pour $r \in \mathbb{N}^*$, on considère l'hypothèse de récurrence :

$$\mathcal{H}_r \ : \ \text{ si } x = a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times \text{ avec } (a,b) \in \mathbb{N}^2 \text{ et } a+b=r \text{ alors il existe } n \in \mathbb{N} \text{ tel que } x = (1+\sqrt{2})^n$$

► Si $r = a + b = 1$ alors comme $(a,b) \in \mathbb{N}^2$ et $a \neq 0$ d'après la question 2.(b)i., on a nécessairement $a = 1$ et $b = 0$. Dans ce cas, on a $1 + 0\sqrt{2} = (1+\sqrt{2})^0$ ce qui montre que $n = 0$ convient.
► Soit $r \in \mathbb{N}^*$, on procède par récurrence forte en supposant que H_k est vraie pour tout $k \in [\![1, r]\!]$. Il s'agit de démontrer que $\mathcal{H}_{r+1}$ est vraie. Soit $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ avec $(a,b) \in \mathbb{N}^2$ et $a + b = r + 1$. Si $b = 0$ alors $x = 1$ d'après la question 2.(b)ii. et l'on peut choisir $n = 0$. Si $b \neq 0$, on considère :

$$\frac{x}{1+\sqrt{2}} = (2b-a) + (a-b)\sqrt{2} = a' + b'\sqrt{2}$$

On a $\dfrac{x}{1+\sqrt{2}}$ qui appartient à $\mathbb{Z}[\sqrt{2}]^\times$ comme quotient d'éléments inversibles. De plus $a' = 2b - a$ et $b' = a - b$ sont des entiers positifs d'après la question 2.(b)iii. et $a' + b' = b < a + b = r + 1$. Ce qui permet d'appliquer l'hypothèse de récurrence à $a' + b'\sqrt{2}$, il existe $n \in \mathbb{N}$ tel que $a' + b'\sqrt{2} = (1+\sqrt{2})^n$ et par suite $x = (1+\sqrt{2})^{n+1}$. Ce qui démontre que $\mathcal{H}_{r+1}$ est vraie et achève la récurrence.

$$\boxed{\text{Si } x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times \text{ avec } (a,b) \in \mathbb{N}^2 \text{ alors il existe } n \in \mathbb{N} \text{ tel que } x = (1+\sqrt{2})^n}$$

(c) Soit $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ avec $(a,b) \in \mathbb{Z}^2$. Il y a 4 cas à considérer :
► Si $a \geq 0$ et $b \geq 0$ alors d'après la question précédente, il existe $n \in \mathbb{N}$ tel que $\underline{a + b\sqrt{2} = (1+\sqrt{2})^n}$
► Si $a \leq 0$ et $b \leq 0$ alors d'après la question précédente, il existe $n \in \mathbb{N}$ tel que $-a - b\sqrt{2} = (1+\sqrt{2})^n$ d'où $\underline{a + b\sqrt{2} = -(1+\sqrt{2})^n}$.
► Si $a \geq 0$ et $b \leq 0$ alors d'après la question précédente, il existe $n \in \mathbb{N}$ tel que $a - b\sqrt{2} = (1+\sqrt{2})^n$, on applique φ à cette égalité et on utilise la propriété de morphisme de φ :

$$\varphi(a - b\sqrt{2}) = \varphi\Big((1+\sqrt{2})^n\Big) = \varphi(1+\sqrt{2})^n \Leftrightarrow \underline{a + b\sqrt{2} = (1-\sqrt{2})^n}$$

► Enfin si $a \leq 0$ et $b \geq 0$, on a d'après l'alinéa précédent, l'existence de $n \in \mathbb{N}$ tel que $-a-b\sqrt{2} = (1-\sqrt{2})^n$ d'où $\underline{a+b\sqrt{2} = -(1-\sqrt{2})^n}$
Dans les quatre cas, on a :

$$\boxed{\exists n \in \mathbb{N},\ x = \pm(1 \pm \sqrt{2})^n}$$

En résumé, cette question ainsi que la question 1.(f) permettent d'aboutir à la caractérisation des inversibles de l'anneau $\mathbb{Z}[\sqrt{2}]$:

$$\boxed{x \in \mathbb{Z}[\sqrt{2}]^\times \Leftrightarrow \exists n \in \mathbb{N},\ x = \pm(1 \pm \sqrt{2})^n}$$

3. (a) Les oiseaux volent en formation triangulaire, c'est-à-dire qu'il existe $l \in \mathbb{N}$ tel que :

$$N = 1+2+3+\ldots+l = \frac{l(l+1)}{2}$$

D'autre part $\dfrac{N}{2}$ est également un entier qui peut s'écrire sous la forme $1+2+3+\ldots+m$ puisque les deux groupes de $\dfrac{N}{2}$ oiseaux volent également en formation triangulaire.

$$\boxed{\exists (l,m) \in \mathbb{N}^2,\ N = \frac{l(l+1)}{2} = m(m+1)}$$

(b) Utilisons l'équivalence démontrée à la question 1.(e) en vérifiant que $N(a+b\sqrt{2}) = \pm 1$. On a :

$$\begin{aligned} N(a+b\sqrt{2}) &= a^2 - 2b^2 \\ &= (2l+1)^2 - 2(2m+1)^2 \\ &= 4l^2 + 4l + 1 - 8m^2 - 8m - 2 \\ &= 8\Big(\frac{l(l+1)}{2} - m(m+1)\Big) - 1 \\ &= -1 \end{aligned}$$

$$\boxed{\text{Si } a = 2l+1 \text{ et } b = 2m+1 \text{ alors } a+b\sqrt{2} \text{ est inversible}}$$

(c) Comme a et b sont positifs, on est dans le cadre de la question 2.(b), ainsi :

$$\boxed{\exists n \in \mathbb{N},\ a+b\sqrt{2} = (1+\sqrt{2})^n}$$

(d) Si $n = 0$, on a $(1+\sqrt{2})^0 = 1 = 1 + 0 \times \sqrt{2}$ ainsi $a_0 = 1$ et $b_0 = 0$. Soit $n \in \mathbb{N}$, on a :

$$a_{n+1} + b_{n+1}\sqrt{2} = (1+\sqrt{2})^{n+1} = (1+\sqrt{2})(1+\sqrt{2})^n = (1+\sqrt{2})(a_n + b_n\sqrt{2}) = (a_n + 2b_n) + (a_n + b_n)\sqrt{2}$$

Ce qui démontre que $a_{n+1} = a_n + 2b_n$ et $b_{n+1} = a_n + b_n$, cette identification étant valable puisque tout élément de $\mathbb{Z}[\sqrt{2}]$ s'écrit de façon unique sous la forme $a + b\sqrt{2}$.

$$\boxed{\begin{cases} a_0 = 1,\ b_0 = 0 \\ \forall n \in \mathbb{N},\ a_{n+1} = a_n + 2b_n \\ \forall n \in \mathbb{N},\ b_{n+1} = a_n + b_n \end{cases}}$$

(e) Les formules précédentes permettent de calculer de proche en proche les coefficients du développement de $(1+\sqrt{2})^n$. Une fois que l'on connaît ces coefficients, on trouve $a = a_n$ puisque $a + b\sqrt{2} = (1+\sqrt{2})^n$ et on en déduit l car $l = \dfrac{a-1}{2}$. Si l'on connaît l, on trouve le nombre d'oiseaux N puisque $N = \dfrac{l(l+1)}{2}$.

n	a_n	b_n	a	l	N
0	1	0	1	0	0
1	1	1	1	0	0
2	3	2	3	1	1
3	7	5	7	3	6
4	17	12	17	8	36
5	41	29	41	20	210
6	99	70	99	49	1225

Le seul résultat étant compris entre 100 et 1000 est $N = 210$.

On remarque d'ailleurs que si n est pair alors b_n est pair ce qui ne peut pas convenir à notre problème où b est impair.

$\boxed{\text{Ce jour-là il y avait 210 vanneaux huppés}}$

(f) C'est bien sûr 42 (qui n'est pas ma pointure de chaussures).

Un autre problème assez similaire est celui de la pile d'oranges. On considère une pyramide à base carrée d'oranges, c'est-à-dire qu'il y n^2 oranges à la base (un carré de n par n), $(n-1)^2$ oranges au dessus ainsi de suite jusqu'à l'orange qui se trouve au sommet. Le nombre, N, d'oranges est de la forme :

$$N = 1 + 2 + ... + (n-1)^2 + n^2 \text{ pour un certain } n \in \mathbb{N}$$

La pile s'effrondre et l'on remarque que l'on peut réorganiser les oranges en un carré parfait. C'est-à-dire que $N = l^2$ où $l \in \mathbb{N}$. Hormis $N = 1$, la seule solution est $N = 4900$.