Corrigé du DM 12

Problème. Étude de l'anneau $\mathbb{Z}[\sqrt{2}]$.

Partie I. Étude de l'anneau $(\mathbb{Z}[\sqrt{2}], +, \times)$.

1. Nous allons vérifier que $(A, +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$.
Considérons deux éléments de A : $a+b\sqrt{2}$ et $c+d\sqrt{2}$ (avec a, b, c, d dans $\mathbb{Z}$).
— On calcule
$$a-b = \underbrace{(a-c)}_{\in\mathbb{Z}} + \underbrace{(b-d)}_{\in\mathbb{Z}}\sqrt{2},$$
ce qui montre que $(a+b\sqrt{2}) - (c+d\sqrt{2}) \in A$.
— On a aussi
$$(a+b\sqrt{2})\cdot(c+d\sqrt{2}) = ac+bc\sqrt{2}+ad\sqrt{2}+bd\sqrt{2}^2 = \underbrace{(ac+2bd)}_{\in\mathbb{Z}} + \underbrace{(bc+ad)}_{\in\mathbb{Z}}\sqrt{2},$$
ce qui montre que $(a+b\sqrt{2}) \times (c+d\sqrt{2}) \in A$.
— Enfin, $1 = \underbrace{1}_{\in\mathbb{Z}} + \underbrace{0}_{\in\mathbb{Z}}\sqrt{2}$ donc $1 \in A$.
Sous-anneau de $\mathbb{R}$, anneau commutatif, $\boxed{A \text{ est bien un anneau commutatif}}$.

2. Pour prouver l'*unicité de l'écriture*, on considère un élément x de A et deux couples (a, b) et (c, d) de $\mathbb{Z}^2$ tels que
$$x = a+b\sqrt{2} = c+d\sqrt{2}.$$
Par différence, on obtient $a-c = (d-b)\sqrt{2}$.
Supposons que $a \neq c$. Alors, on obtient $\sqrt{2} = \frac{d-b}{a-c}$ (quotient d'entiers) ce qui est absurde par irrationalité de $\sqrt{2}$.
Ainsi $a-c = 0$. Comme $(d-b)\sqrt{2} = 0$ et $\sqrt{2} \neq 0$, on a $d-b = 0$.
Ceci achève de prouver que $\boxed{(a, b) = (c, d)}$.

3. Soit $x \in A$. On l'écrit $x = a+b\sqrt{2}$, avec $(a, b) \in \mathbb{Z}^2$. On calcule
$$N(x) = \bar{x}x = (a-b\sqrt{2})(a+b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Z}.$$
— Supposons que $x = 0$. L'écriture (unique) de 0 comme élément de A est $0 = 0+0\sqrt{2}$. On a donc $\bar{0} = 0-0\sqrt{2} = 0$. Ainsi, $N(x) = 0\cdot 0 = 0$.
— Supposons que $N(x) = 0$, soit $\bar{x}x = 0$. On a donc $x = 0$ ou $\bar{x} = 0$. Dans le second cas, on a $a-b\sqrt{2} = 0$, ce qui donne $a = b = 0$ par unicité. Dans les deux cas, $x = 0$.
$$x = 0 \iff N(x) = 0.$$

4. Soit $(x, x') \in A^2$.
Il existe deux couples d'entiers (a, b) et (c, d) tels que $x = a+b\sqrt{2}$ et $x' = c+2\sqrt{2}$.
On a développé xx' en question 1 ; on calcule donc
$$N(xx') = (ac+2bd)^2 - 2(bc+ad)^2 = a^2c^2 + \cancel{4abcd} + 4b^2d^2 - 2b^2c^2 - 2a^2d^2 - \cancel{4abcd}.$$
D'autre part, on a
$$N(x)N(x') = (a^2-2b^2)(c^2-2d^2) = (ac+2bd)^2 - 2(bc+ad)^2 = a^2c^2+4b^2d^2-2b^2c^2-2a^2d^2.$$
On a bien vérifié que $\boxed{N(xx') = N(x)N(x')}$.

5. On sait déjà que A est commutatif.
Considérons deux éléments x et x' tels que $xx' = 0$. Alors, $N(xx') = N(0)$, soit d'après la question 4, $N(x)N(x') = 0$. Or, $N(x)$ et $N(x')$ sont deux éléments de $\mathbb{Z}$, qui est intègre. On a donc $N(x) = 0$ ou $N(x') = 0$ et donc $x = 0$ ou $x' = 0$ d'après 3. $\boxed{\text{L'anneau } A \text{ est bien intègre}}$.

6. Soit $x \in A$.
• Supposons que x est inversible. L'inverse de x, noté x^{-1}, existe et $xx^{-1} = 1$.
Appliquons N, qui est compatible avec le produit d'après 4 :
$$N(x)N(x^{-1}) = 1.$$
Puisque $N(x)$ et $N(x^{-1})$ sont des entiers, et que les seuls inversibles de $\mathbb{Z}$ sont 1 et -1, on a $N(x) = 1$ ou $N(x) = -1$.
• Supposons que $N(x) = \pm 1$. Alors $\frac{\bar{x}}{N(x)}$ est encore un élément de A et
$$\frac{\bar{x}}{N(x)} \cdot x = 1.$$
Ceci démontre que x est inversible d'inverse $x^{-1} = \frac{\bar{x}}{N(x)}$.
On a établi que $\boxed{x \text{ est inversible ssi } N(x) \in \{-1, 1\}.}$

Partie II. Étude des inversibles de $\mathbb{Z}[\sqrt{2}]$.

7. On a fixé un élément $x \in U$ et $(a,b) \in \mathbb{Z}^2$ tel que $x = a + b\sqrt{2}$.
   (a) Supposons que a et b sont de même signe.
   Alors $|x| = |a| + |b|\sqrt{2}$ (facile en examinant les deux cas).
   Les entiers a et b ne sont pas tous les deux nuls car sinon $x = 0$, qui n'est pas inversible dans A.
   Si $a \neq 0$, alors $|a| \geq 1$ et $|x| \geq 1 + 0$.
   Si $b \neq 0$, alors $|b| \geq 1$ et $|x| \geq 0 + \sqrt{2}$.
   Puisque $\sqrt{2} \geq 1$, on a dans les deux cas $\boxed{|x| \geq 1}$.

   (b) Supposons que $ab \leq 0$. Rappelons que x est inversible, ce qui est équivalent à $N(x) = \pm 1$, soit $\bar{x}x = 1$. Passons aux valeurs absolues :
   $$|\bar{x}| \cdot |x| = 1.$$
   Le nombre $|x|$ est non nul et on a $|x| = |\bar{x}|^{-1}$. Or, puisque $\bar{x} = a - b\sqrt{2}$ et que $ab \leq 0$, les nombres a et $-b$ sont de même signe. D'après la question (a), $\bar{x}| \leq 1$, ce qui donne $\boxed{|x| \leq 1}$.

8. On note $U^+ = U \cap]1, +\infty[$.
   (a) Soit $x \in U^+$. On l'écrit $x = a + b\sqrt{2}$ avec $(a,b) \in \mathbb{Z}^2$. Puisque $|x| > 1$, la question 7(b) nous assure par contraposée que a et b sont de même signe, positif en l'occurrence puisque x est positif. De plus,
   — $(a,b) = (0,0)$ et $(a,b) = (1,0)$ sont exclus car on aurait $x < 1$.
   — $(a,b) = (0,1)$ aussi car on aurait $x = \sqrt{2} \notin U$ (puisque $N(\sqrt{2}) = -2 \neq \pm 1$).
   On a donc $a \geq 1$ et $b \geq 1$, ce qui donne que $1 + \sqrt{2}$ minore U^+.
   Reste à vérifier que $1 + \sqrt{2}$ appartient à U^+. On a $N(1 + \sqrt{2}) = 1 - 2 = -1$ donc il est bien dans U, et il est clairement strictement supérieur à 1.
   On a bien montré que $\boxed{1 + \sqrt{2} \text{ est le minimum de } U^+.}$ Ce nombre sera noté α.

   (b) La suite $(\alpha^n)_{n\in\mathbb{N}}$ est strictement croissante et la famille $\left([\alpha^n, \alpha^{n+1}[\right)_{n\in\mathbb{N}}$ est une partition de $[1, +\infty[$. Pour $x \in U^+$, x appartient en particulier à $[1, +\infty[$ donc $\boxed{x \text{ appartient à un (unique) intervalle } [\alpha^n, \alpha^{n+1}[\text{ pour } n \in \mathbb{N}}$.
   Remarque : on peut préciser le lien entre x et l'entier de la manière suivante :
   $$\forall n \in \mathbb{N} \quad \alpha^n \leq x < \alpha^{n+1} \iff n \leq \frac{\ln(x)}{\ln(\alpha)} < n + 1,$$
   l'entier n cherché est $\lfloor \log_\alpha(x) \rfloor$.

   (c) • Pour $n \in \mathbb{N}^*$, $\alpha^n \in U^+$. En effet, puisque $\alpha \in U$ et que U est un groupe, $\alpha^n \in U$. De plus, puisque $n \in \mathbb{N}^*$, $\alpha^n \geq \alpha > 1$. On a bien $\underline{U^+ \supset \{\alpha^n \mid n \in \mathbb{N}^*\}}$.
   • Soit $x \in U^+$. D'après (b), il existe un entier $n \in \mathbb{N}$ tel que $\alpha^n \leq x < \alpha^{n+1}$. Puisque $x \geq \alpha$, nécessairement $n \in \mathbb{N}^*$. Montrons que $x = \alpha^n$. Supposons que ce n'est pas le cas. On a alors $\alpha^n < x < \alpha^{n+1}$, puis $1 < x\alpha^{-n} < \alpha$. Or, $x\alpha^{-n}$ est un élément de U puisque c'est le cas de x et de α^n et que U est un groupe. On a obtenu de surcroît que $1 < x\alpha^{-n}$, ce qui donne $x\alpha^{-n} \in U^+$. L'inégalité $x\alpha^{-n} < \alpha$ est absurde par minimalité de α donc $x = \alpha^n$: $\underline{U^+ \subset \{\alpha^n \mid n \in \mathbb{N}^*\}}$.
   Par double-inclusion $\boxed{U^+ = \{\alpha^n \mid n \in \mathbb{N}^*\}}$.

9. Ici, il y avait une ERREUR dans l'énoncé. Bien sûr, l'ensemble U est symétrique par rapport à 0 donc
   $$\forall x \in A \quad x \in U \cap]1, +\infty[\iff -x \in U \cap]-\infty, -1[.$$
   Or, puisque les α^n et les $-\alpha^n$ sont dans U, leurs inverses α^{-n} et $-\alpha^{-n}$ sont aussi dans U. Le résultat à démontrer était donc plutôt
   $$\boxed{U = \{\alpha^n \mid n \in \mathbb{Z}\} \cup \{-\alpha^n \mid n \in \mathbb{Z}\}}$$
   L'inclusion réciproque est désormais claire. Réciproquement, considérons $x \in U$. Par symétrie, on peut supposer que $x \geq 0$. Si $x > 1$, il s'écrit $x = \alpha^n$ avec $n \in \mathbb{N}^*$. Si $x < 1$, alors $x^{-1} > 1$ et donc $x^{-1} \in U^+$. Il existe alors $n \in \mathbb{N}^*$ tel que $x^{-1} = \alpha^n$, ce qui donne $x = \alpha^{-n}$.

10. (a) On note $x = a + b\sqrt{2} \in A$, avec $(a,b) \in \mathbb{N}^2$. On constate que si $a^2 - 2b^2 = \pm 1$ alors $(a,b) \neq (0,0)$ et puisque a et b sont de même signe positif, $|x| \geq 1$ (question 7) puis $x \geq 1$ puisque x est positif. D'après la question précédente et la description des éléments positifs de U, il existe $n \in \mathbb{N}$ tel que $x = \alpha^n$. Réciproquement, si x s'écrit ainsi, alors $N(x) = \pm 1$ et $a^2 - 2b^2 = \pm 1$.
   (b) On note encore $x = a + b\sqrt{2} \in A$. On sait que $N(x) = a^2 - 2b^2$.
   • Si $a^2 - 2b^2 = 1$ alors il existe $k \in \mathbb{N}$ tel que $a + b\sqrt{2} = (1 + \sqrt{2})^k$.
   Mais $1 = a^2 - 2b^2 = N(x) = N\left((1 + \sqrt{2})^k\right) = N(1 + \sqrt{2})^k = (-1)^k$ montre que k est pair : $k = 2n$ avec $n \in \mathbb{N}$.
   • Si $x = (1 + \sqrt{2})^{2n}$ alors $N(x) = N\left((1 + \sqrt{2})^{2n}\right) = (-1)^{2n} = 1$, et $a^2 - 2b^2 = 1$.
   (c) On note encore $x = a + b\sqrt{2} \in A$. On calcule par la formule du binôme que
   $$(1 + \sqrt{2})^{2n} = \sum_{p=0}^{2n} \binom{2n}{p} (\sqrt{2})^p = \underbrace{\left(\sum_{k=0}^{n} \binom{2n}{2k} 2^k\right)}_{\in\mathbb{Z}} + \underbrace{\left(\sum_{k=0}^{n} \binom{2n}{2k+1} 2^k\right)}_{\in\mathbb{Z}} \sqrt{2}.$$
   On conclut grâce à la question précédente et l'unicité de l'écriture