L2 MTH1314 2014-2015

Correction du devoir maison n°2

Solution de l'exercice 1

1. (a) L'ensemble $\mathbb{Z}[\sqrt{2}]$ est clairement inclus dans $\mathbb{R}$.
   (b) L'élément 0 peut s'écrire $0 = 0 + 0 \times \sqrt{2}$ et est donc dans $\mathbb{Z}[\sqrt{2}]$.
   (c) De même, $1 = 1 + 0\sqrt{2}$ est dans $\mathbb{Z}[\sqrt{2}]$.
   (d) Soient x et y deux éléments de $\mathbb{Z}[\sqrt{2}]$. Par définition, il existe m_1, n_1, m_2 et n_2 entiers tels que $x = m_1 + n_1\sqrt{2}$ et $y = m_2 + n_2\sqrt{2}$. On a

$$x + y = m_1 + n_1\sqrt{2} + m_2 + n_2\sqrt{2} = \underbrace{(m_1 + m_2)}_{\in\mathbb{Z}} + \underbrace{(n_1 + n_2)}_{\in\mathbb{Z}}\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

   L'ensemble $\mathbb{Z}[\sqrt{2}]$ est donc stable par $+$.
   (e) On a également, avec les mêmes notations,

$$xy = (m_1 + n_1\sqrt{2})(m_2 + n_2\sqrt{2}) = \underbrace{(m_1m_2 + 2n_1n_2)}_{\in\mathbb{Z}} + \underbrace{(m_1n_2 + m_2n_1)}_{\in\mathbb{Z}}\sqrt{2} \in \mathbb{Z}[\sqrt{2}].$$

   L'ensemble $\mathbb{Z}[\sqrt{2}]$ est donc stable par $\times$.
   (f) L'inverse de x pour $+$ est $-x = -m_1 - n_1\sqrt{2} = \underbrace{(-m_1)}_{\in\mathbb{Z}} + \underbrace{(-n_1)}_{\in\mathbb{Z}}\sqrt{2}$ et est donc bien un élément de $\mathbb{Z}[\sqrt{2}]$.

   Toutes ces petites propositions montrent bien que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un sous-anneau de $(\mathbb{R}, +, \times)$

2. L'existence découle immédiatement de la définition de $\mathbb{Z}[\sqrt{2}]$, il s'agit de démontrer l'unicité pour que dans la question suivante ϕ associe une unique image à chaque élément pour être bien définie. On considère donc deux couples d'entiers (m_1, n_1), (m_1', n_1') tels que

$$x = m_1 + n_1\sqrt{2} = m_1' + n_1'\sqrt{2}.$$

   Alors

$$(m_1 - m_1') + (n_1 - n_1')\sqrt{2} = 0. \tag{1}$$

   Si on suppose que $n_1 \neq n_1'$, alors

$$\sqrt{2} = \frac{m_1' - m_1}{n_1 - n_1'} \in \mathbb{Q},$$

   ce qui est absurde. Donc $n_1 = n_1'$ d'où l'on déduit également par (1) que $m_1 = m_1'$. D'où l'unicité.

3. Montrons que ϕ est un morphisme d'anneau. Pour $x = m_1 + n_1\sqrt{2}$ et $y = m_2 + n_2\sqrt{2}$ deux éléments de $\mathbb{Z}[\sqrt{2}]$,

$$\begin{aligned}
\phi(x+y) &= \phi((m_1+m_2) + (n_1+n_2)\sqrt{2}) \\
&= (m_1+m_2) - (n_1+n_2)\sqrt{2} \\
&= m_1 - n_1\sqrt{2} + m_2 - n_2\sqrt{2} = \phi(x) + \phi(y). \\
\phi(xy) &= \phi((m_1m_2 + 2n_1n_2) + (m_2n_1 + m_1n_2)\sqrt{2}) \\
&= (m_1m_2 + 2n_1n_2) - (m_2n_1 + m_1n_2)\sqrt{2} \\
&= m_1(m_2 - n_2\sqrt{2}) - n_1\sqrt{2}(m_2 - n_2\sqrt{2}) \\
&= (m_1 - n_1\sqrt{2})(m_2 - n_2\sqrt{2}) = \phi(x)\phi(y).
\end{aligned}$$

Donc ϕ est bien un morphisme d'anneau. En réalité, si vous croisez la définition de morphisme d'anneau, vous verrez qu'il faut vérifier également que $\phi(1) = 1$ (la propriété $\phi(0) = 0$ n'a pas besoin d'être vérifiée car elle découle quant à elle des précédentes, sauriez-vous le montrer ?). Ce n'était pas demandé ici mais vérifions bien que $\phi(1) = 1$.

$$\phi(1) = \phi(1 + 0\sqrt{2}) = 1 - 0\sqrt{2} = 1.$$

Montrons maintenant que ϕ est une bijection. Deux façons, on montre que ϕ est injective et surjective ou on exhibe directement la fonction réciproque. Détaillons les deux méthodes. La fonction ϕ est injective, avec les mêmes notations, si $\phi(x) = \phi(y)$ alors $m_1 - n_1\sqrt{2} = m_2 - n_2\sqrt{2}$ donc par la question précédente, $m_1 = m_2$ et $-n_1 = -n_2$ c'est-à-dire $n_1 = n_2$. D'où $x = y$ et l'injectivité. Pour la surjectivité, on voit que pour tout $x = m_1 + n_1\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$,

$$x = \phi(m_1 - n_1\sqrt{2})$$

Donc x est dans l'image de ϕ et ce pour tout $x \in \mathbb{Z}[\sqrt{2}]$. Donc ϕ est surjective. Seconde solution, on remarque directement que ϕ est sa propre réciproque en effet pour tout $x = m_1 + n_1\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$,

$$\phi \circ \phi(x) = \phi(\phi(x)) = \phi(m_1 - n_1\sqrt{2}) = m_1 + n_1\sqrt{2} = x.$$

Donc $\phi \circ \phi = \mathrm{Id}$ et ainsi ϕ est bijective et est sa propre réciproque.

4. Soit $x = m_1 + n_1\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. On a

$$N(x) = x\phi(x) = (m_1 + n_1\sqrt{2})(m_1 - n_1\sqrt{2}) = m_1^2 - 2n_1^2 \in \mathbb{Z}.$$

Donc N est bien à valeurs dans $\mathbb{Z}$. De plus pour $y \in \mathbb{Z}[\sqrt{2}]$, on a

$$N(xy) = xy\phi(xy) = xy\phi(x)\phi(y),$$

car ϕ est un morphisme pour la multiplication. Or la multiplication des réels est commutative donc,

$$N(xy) = x\phi(x)y\phi(y) = N(x)N(y),$$

et N est aussi un morphisme pour la multiplication.

5. Si x est inversible (sous-entendu multiplicativement naturellement), il existe y dans $\mathbb{Z}[\sqrt{2}]$ tel que $xy = 1$. Donc par la propriété de morphisme,

$$N(x)N(y) = N(xy) = N(1) = 1\phi(1) = 1$$

Or $N(x)$ et $N(y)$ sont deux éléments de $\mathbb{Z}$, donc nécéssairement $N(x) = N(y) = \pm 1$. Réciproquement, si $N(x) = \pm 1$ alors $x\phi(x) = \pm 1$ et donc x est inversible d'inverse $\pm\phi(x)$ qui est bien, précisons-le, un élément de $\mathbb{Z}[\sqrt{2}]$.

6. Sans surprise, par la question précédente,
$$N(3+2\sqrt{2}) = (3+2\sqrt{2}) \times (3-2\sqrt{2}) = 9-8 = 1.$$
De même
$$N(-3+2\sqrt{2}) = (-3+2\sqrt{2}) \times (-3-2\sqrt{2}) = 9-8 = 1.$$
Donc $3+2\sqrt{2}$ et $-3+2\sqrt{2}$ sont bien inversibles dans $\mathbb{Z}[\sqrt{2}]$.

Solution de l'exercice 2

1. On fixe a dans E. Montrons que γ_a est injective. Soient x et y deux éléments de E tels que $\gamma_a(x) = \gamma_a(y)$ c'est-à-dire $a * x = a * y$. Donc par la condition 2, $x = y$ et γ_a est bien injective ce qui nous donne d'après le rappel que γ_a est bijective.

2. On en déduit notamment que γ_a est surjective. Ainsi a, qui est un élément de E, possède un antécédent par γ_a : il existe e_1 dans E tel que $\gamma_a(e_1) = a$, id est $a * e_1 = a$.

3. Soit $b \in E$, on multiplie la relation précédente par b : $a * e_1 * b = a * b$. Puis par la condition 2, on peut simplifier à gauche par a et l'on obtient $e_1 * b = b$. Il y a un gain énorme par rapport à la question précédente. Juste au dessus nous avons construit *à partir de* a un élément e_1 qui vérifie la relation $a * e_1 = a$ *uniquement* pour a. Ici nous avons la relation $e_1 * b = b$ pour n'importe quel b.

4. Pour démontrer cette question, il fallait obtenir que pour tout b on a également $b * e_1 = b$. Voici une solution possible. Exactement de la même façon (par symétrie des hypothèses) on montre également qu'il existe $e_2 \in E$ tel que $\forall b \in E$, $b * e_2 = b$. Il s'agit naturellement de montrer que e_1 et e_2 sont en réalité égaux. En prenant $b = e_1$ dans l'égalité précédente et $b = e_2$ dans l'égalité de la question précédente, on obtient d'une part que $e_1 * e_2 = e_1$ et d'autre part que $e_1 * e_2 = e_2$. Ainsi, $e_1 = e_1 * e_2 = e_2$. En renotant $e = e_1 = e_2$ et en rassemblant à nouveau les deux égalités $e_1 * b = b$ et $b * e_2 = b$, on obtient que cet élément vérifie pour tout $b \in E$ $b * e = b = e * b$ et est donc bien l'élément neutre de $(E, *)$.

5. Il nous reste à montrer que chaque élément admet un inverse dans E. Fixons à nouveau a dans E. Montrons que a possède un inverse. D'après la surjectivité de γ_a, il existe $b_1 \in E$ tel que $\gamma_a(b_1) = e$ c'est-à-dire $a * b_1 = e$. De même on a l'existence de b_2 dans E tel que $b_2 * a = e$. En multipliant la première égalité par b_2 et la seconde par b_1 on obtient, $b_2 * a * b_1 = b_2 * e = b_2$ et $b_2 * a * b_1 = e * b_1 = b_1$. Puisque les deux termes de gauche sont identiques, on en déduit que $b_2 = b_1$. En le renotant b et en reprenant les égalité précédentes, on obtient bien que $a * b = e = b * a$. Donc a est inversible d'inverse b.
   La loi de composition interne $*$ pour E est associative, il existe un élément neutre et tout élément possède un inverse dans E. L'ensemble $(E, *)$ est donc bien un groupe.