13. Structures algébriques usuelles, méthodologie

I. Loi de composition interne

I.1. Définition

I.2. Propriétés

Définition. Soit E un ensemble et $*$ une lci sur E. On dit que $*$ est :

- associative si $\forall x, y, z \in E,\ x * (y * z) = (x * y) * z$.
- commutative si $\forall x, y \in E,\ x * y = y * x$.

Définition. Soit E un ensemble et $*$ une lci sur E. Soient $x, y \in E$. On dit que x et y commutent si $x * y = y * x$.

Définition. On dit qu'un ensemble $A \subset E$ est stable par la loi $*$ si $\forall x, y \in A,\ x * y \in A$. *En particulier, pour montrer que $*$ est une lci sur E, il faut montrer que E est stable par $*$.*

I.3. Éléments particuliers

Définition. Soit E un ensemble et $*$ une lci sur E. On dit que $e \in E$ est un élément neutre de E pour $*$ si $\forall x \in E,\ x * e = e * x = x$.

Proposition. Soit E un ensemble et $*$ une lci sur E. Si E admet un élément neutre, alors ce dernier est unique.

Exercice d'application 1. On définit une lci sur $\mathbb{R}$ par $\forall x, y \in \mathbb{R},\ x * y = \ln(e^x + e^y)$.

1) Vérifier que $*$ est bien définie et qu'elle est associative. Est-elle commutative ?

2) $\mathbb{R}$ admet-il un élément neutre pour $*$?

Définition. Soit E un ensemble, $*$ une lci sur E et $e \in E$ un élément neutre. Soit $x \in E$. On dit que x est inversible si il existe $y \in E$ tel que $x * y = y * x = e$. On dit alors que x est inversible et que y est un inverse de x.

Proposition. Soit E un ensemble, $*$ une lci associative sur E et $e \in E$ l'élément neutre. Soit $x \in E$ inversible. Alors, l'inverse de x est unique et est noté x^{-1}.

(m) Pour montrer qu'un élément $x \in E$ est inversible, il faut donc trouver un élément $y \in E$ tel que $x * y = e$ et tel que $y * x = e$. Il faut bien vérifier les deux égalités car un inverse à gauche n'est pas toujours un inverse à droite. En général, on commence par étudier une des deux équations (par

exemple $x*y=e$) et on essaye de trouver y en fonction de x. On vérifie ensuite que la solution trouvée est aussi un inverse de l'autre côté.

Exercice d'application 2. Donner une condition suffisante sur $*$ pour n'avoir à vérifier que $x*y=e$ pour prouver que x est inversible et que $y=x^{-1}$.

II. Groupes

II.1. Définition

Définition. On dit que $(G,*)$ est un groupe (ou que G muni de la loi $*$ est un groupe) si :

- $*$ est une lci associative sur G.
- Il existe $e\in G$ élément neutre pour $*$.
- Tous les éléments de G sont inversibles pour la loi $*$ et leur inverse appartient à G.

(m) Un groupe est donc un ensemble muni d'une lci **associative**, qui admet un **élément neutre** et qui est **stable par cette loi** et **stable par passage à l'inverse**.

Remarque : Dans un groupe, la loi $*$ est toujours associative par contre elle n'est en général pas commutative ! Si $*$ est commutatif, on dit que G est un groupe commutatif (ou abélien).

Exercice d'application 3. On pose $G=\{f_a,\ a\in\mathbb{R}\}$ où pour $a\in\mathbb{R}$, $f_a:\left\{\begin{array}{ccc}\mathbb{R}&\to&\mathbb{R}\\ x&\mapsto&x+a\end{array}\right.$. Montrer que $(G,\circ)$ est un groupe. Est-il commutatif ?

II.2. Exemples de groupes

Proposition. Soit E un ensemble. Une bijection de E dans E est appelée une permutation de E. Alors, si on note S_E l'ensemble des permutations de E, $(S_E,\circ)$ est un groupe dont l'élément neutre est Id_E.

Proposition. Groupe produit. Soient $(G_1,*_1)$ et $(G_2,*_2)$ deux groupes. Alors, $G_1\times G_2$ muni de la loi $(x_1,x_2)*(y_1,y_2)=(x_1*_1y_1,x_2*_2y_2)$ est un groupe.

II.3. Règles de calcul

Proposition. Soit $(G,*)$ un groupe. Alors :
- $\forall x\in G,\ x^{-1}\in G$ et $(x^{-1})^{-1}=x$.
- $\forall x,y\in G,\ x*y\in G$ et $(x*y)^{-1}=y^{-1}*x^{-1}$.

Proposition. Soit $(G,*)$ un groupe et $a,x,y\in G$. Alors :
- $a*x=a*y\Rightarrow x=y$. *On peut simplifier à gauche dans un groupe.*
- $x*a=y*a\Rightarrow x=y$. *On peut simplifier à droite dans un groupe.*

(m) Le point important est que dans un groupe, on a toujours le droit de multiplier par des éléments du groupe et puisqu'un groupe est stable par passage à l'inverse, on peut aussi multiplier par leur inverse (autrement dit multiplier par a^{-1} pour démontrer la proposition précédente).

Exercice d'application 4. Soit $(G, *)$ un groupe. On note e l'élément neutre.

1) Soient $a, b \in G$ tels que $a^2 = e$, $b^2 = e$ et $(a * b)^2 = e$. Montrer que a et b commutent.

2) Soit $a \in G$ tel qu'il existe $n \in \mathbb{N}^*$ tel que $a^n = e$. Montrer que $\forall b \in G,\ (b * a * b^{-1})^n = e$.

II.4. Sous-groupes

Définition. Soit $(G, *)$ un groupe. On dit que H est un sous-groupe de G si $H \subset G$ et que $(H, *)$ est un groupe.

(m) Pour montrer que H est un sous-groupe de G, il suffit donc de montrer que $H \subset G$ (ce qui est en général direct), que H contient l'élément neutre (en général direct aussi) et que H est stable par $*$ et stable par passage à l'inverse (ces deux points sont en général plus difficiles). Il n'est pas utile de montrer que $*$ est associative puisque l'on sait que $*$ est associative sur G donc elle l'est aussi sur H car $H \subset G$.

Proposition. Soit $(G, *)$ un groupe et $H \subset G$. Alors :

$$H \text{ est un sous-groupe de } G \Leftrightarrow \left\{ \begin{array}{l} H \neq \emptyset \\ \forall x, y \in H,\ x * y^{-1} \in H \end{array} \right. .$$

Exercice d'application 5. Soit $(G, *)$ un groupe commutatif de neutre e. Pour $n \in \mathbb{N}^*$, on pose

$$H_n = \{x \in G \ / \ x^n = e\}.$$

Montrer que H_n est un sous-groupe de G.

III. Morphisme de groupes

III.1. Définition

Définition. Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes et $\varphi : G_1 \to G_2$. On dit que φ est un morphisme de groupes si :

$$\forall x, y \in G_1,\ \varphi(x *_1 y) = \varphi(x) *_2 \varphi(y).$$

Exercice d'application 6. $\varphi_1 : \left\{ \begin{array}{ccc} (\mathbb{Z}, +) & \to & (\mathbb{Z}, +) \\ n & \mapsto & 3n \end{array} \right.$ et $\varphi_2 : \left\{ \begin{array}{ccc} (\mathbb{Z}, +) & \to & (\mathbb{Z}, +) \\ n & \mapsto & |n| \end{array} \right.$ sont-elles des morphismes de groupe ?

Proposition. Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes de neutres respectifs e_1 et e_2 et $\varphi : G_1 \to G_2$ un morphisme de groupes. Alors :

- $\varphi(e_1) = e_2$.
- $\forall x \in G_1,\ (\varphi(x))^{-1} = \varphi(x^{-1})$.

Proposition. Soient $(G_1, *_1)$ et $(G_2, *_2)$ deux groupes et $\varphi : G_1 \to G_2$ un morphisme de groupes. Alors :

- Si H_1 est un sous-groupe de G_1, alors $\varphi(H_1)$ est un sous-groupe de G_2.
- Si H_2 est un sous-groupe de G_2, alors $\varphi^{-1}(H_2)$ est un sous-groupe de G_1.

Exercice d'application 7. Vérifier que $\varphi : \left\{ \begin{array}{ccc} (\mathbb{Z}, +) & \to & (\mathbb{Q}_+^*, \times) \\ n & \mapsto & 2^n \end{array} \right.$ est un morphisme de groupe et en déduire que $\{2^n,\ n \in \mathbb{Z}\}$ est un groupe pour la loi $\times$.

III.2. Image et noyau

Définition. Soient G_1 et G_2 deux groupes et $\varphi : G_1 \to G_2$ un morphisme de groupes. Alors on pose :

- $\mathrm{Im}(\varphi) = \varphi(G_1)$ l'image de φ. *C'est l'ensemble des éléments de G_2 qui ont un antécédent dans G_1 par φ.*
- $\ker(\varphi) = \varphi^{-1}(\{e_2\})$ le noyau de φ. *C'est l'ensemble des éléments $x \in G_1$ tels que $\varphi(x) = e_2$.*

Proposition. Soient G_1 et G_2 deux groupes et $\varphi : G_1 \to G_2$ un morphisme de groupes. Alors :

- φ est surjective si et seulement si $\mathrm{Im}(\varphi) = G_2$.
- φ est injective si et seulement si $\ker(\varphi) = \{e_1\}$.

III.3. Isomorphismes

Définition. Soient G_1 et G_2 deux groupes et $\varphi : G_1 \to G_2$. On dit que φ est un isomorphisme si c'est un morphisme de groupes bijectif.

Proposition. Une composée de morphisme de groupes est un morphisme de groupes. La réciproque d'un isomorphisme est un isomorphisme.

Proposition. Soient G_1 et G_2 deux groupes. On dit que G_1 est isomorphe à G_2 si il existe un isomorphisme de G_1 dans G_2. Le fait d'être isomorphe est une relation d'équivalence sur l'ensemble des groupes.

Exercice d'application 8. Montrer que $(\mathbb{R}, +)$ et $(\mathbb{R}_+^*, \times)$ sont isomorphes.

IV. Anneaux et corps

IV.1. Anneaux

Définition. On dit que $(A, +, *)$ est un anneau si :

- $(A, +)$ est un groupe commutatif de neutre $0_A \in A$.
- $*$ est une lci associative sur A (A est donc stable par $*$) et A contient l'élément neutre pour $*$ noté 1_A.

- $*$ est distributive par rapport à $+$:

$$\forall x, y, z \in A,\ x * (y + z) = (x * y) + (x * z) \text{ et } (y + z) * x = (y * x) + (z * x).$$

On note $-x$ l'inverse de x pour la loi $+$. *On pourra dire que $-x$ est l'opposé de x.*

Si de plus, $*$ est commutative, on dit que $(A, +, *)$ est un anneau commutatif.

Définition. Soit $(A, +, *)$ un anneau. On dit que A est intègre si :

$$\forall x, y \in A,\ x \times y = 0_A \Rightarrow (x = 0_A \text{ ou } y = 0_A).$$

Ou autrement dit, le produit de deux éléments non nuls n'est jamais nul.

IV.2. Règles de calcul

Proposition. Soit $(A, +, \times)$ un anneau. Alors :
- $\forall x \in A,\ 0_A \times x = x \times 0_A = 0_A$.
- $\forall x \in A,\ (-1_A) \times x = x \times (-1_A) = -x$.
- $\forall x, y \in A,\ (-x) \times y = x \times (-y) = -(x \times y)$.
- $\forall x, y \in A,\ (-x) \times (-y) = x \times y$.

Proposition. Soit $(A, +, \times)$ un anneau. Alors :
- $\forall x \in A, a_1, \ldots, a_n \in A,\ x \times \left(\sum_{i=1}^{n} a_i\right) = \sum_{i=1}^{n} (x \times a_i)$.
- $\forall x \in A, a_1, \ldots, a_n \in A,\ \left(\sum_{i=1}^{n} a_i\right) \times x = \sum_{i=1}^{n} (a_i \times x)$.
- $\forall a_1, \ldots, a_n, b_1, \ldots, b_n \in A,\ \sum_{i=1}^{n} (a_i + b_i) = \left(\sum_{i=1}^{n} a_i\right) + \left(\sum_{i=1}^{n} b_i\right)$.

Proposition. Soit $(A, +, \times)$ un anneau. Soient $a, b \in A$ tels que a et b commutent (autrement dit tels que $a \times b = b \times a$). Alors :
- $\forall n \in \mathbb{N},\ (a + b)^n = \sum_{k=0}^{n} \binom{n}{k} (a^k \times b^{n-k})$.
- $\forall n \in \mathbb{N}^*,\ a^n - b^n = (a - b) \times \left(\sum_{k=0}^{n-1} a^k \times b^{n-1-k}\right)$.

IV.3. Sous-anneaux

Définition. Soit $(A, +, \times)$ un anneau. On dit que B est un sous-anneau de A si $B \subset A$ et que $(B, +, \times)$ est un anneau.

Proposition. Soit $(A, +, \times)$ un anneau et $B \subset A$. Alors :

$$B \text{ est un sous-anneau de } A \Leftrightarrow \begin{cases} (B, +) \text{ est un sous-groupe de } A \\ 1_A \in B \\ B \text{ est stable par } \times \end{cases}.$$

(m) C'est très souvent cette caractérisation que l'on utilise pour démontrer qu'un ensemble est un anneau en prouvant que c'est un sous-anneau d'un anneau connu. Cela permet en particulier de ne pas reprouver les propriétés des lois + et × (associativité, commutativité de +, distributivité de × par rapport à +) qui sont automatiquement vraies car $(A, +, \times)$ est un anneau.

Exercice d'application 9. On pose $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Z}\}$. Montrer que $(\mathbb{Z}[\sqrt{2}], +, \times)$ est un sous-anneau de $\mathbb{R}$.

IV.4. Éléments inversibles

Définition. Soit $(A, +, \times)$ un anneau. Soit $x \in A$. On dit que x est inversible s'il existe $y \in A$ tel que $x \times y = y \times x = 1_A$. *Autrement dit si x est inversible pour la loi $\times$ et que son inverse est dans A.* Si x est inversible, son inverse est unique et est noté x^{-1}.

Exercice d'application 10. Vérifier que $1 + \sqrt{2}$ est un élément inversible de $\mathbb{Z}[\sqrt{2}]$.

Proposition. Soit $(A, +, \times)$ un anneau. Alors, l'ensemble des éléments inversibles pour la loi $\times$ est un groupe pour la loi $\times$ de neutre 1_A.

IV.5. Corps

Définition. On dit que $(\mathbb{K}, +, \times)$ est un corps si :
- $(\mathbb{K}, +, \times)$ est un anneau commutatif.
- $\forall x \in \mathbb{K}^* = \mathbb{K} \setminus \{0_\mathbb{K}\},\ x$ est inversible.

Autrement dit, un corps est un anneau commutatif donc tous les éléments à part $0_\mathbb{K}$ sont inversibles. En particulier, $(\mathbb{K}^*, \times)$ est alors un groupe commutatif.

Proposition. Un corps est intègre.

Définition. Soit $(\mathbb{K}, +, \times)$ un corps. On dit que $\mathbb{L}$ est un sous-corps de $\mathbb{K}$ si $\mathbb{L} \subset \mathbb{K}$ et que $(\mathbb{L}, +, \times)$ est un corps.

Proposition. Soit $(\mathbb{K}, +, \times)$ un corps et $\mathbb{L} \subset \mathbb{K}$. Alors :

$$\mathbb{L} \text{ est un sous-corps de } \mathbb{K} \Leftrightarrow \begin{cases} (\mathbb{L}, +, \times) \text{ est un sous-anneau de } \mathbb{K} \\ \forall x \in \mathbb{L}^*,\ x \text{ est inversible et } x^{-1} \in \mathbb{L} \end{cases}.$$

(m) C'est très souvent cette caractérisation que l'on utilise pour démontrer qu'un ensemble est un corps en prouvant que c'est un sous-corps d'un corps connu. Cela permet en particulier de ne pas reprouver les propriétés des lois + et × (associativité, commutativité, distributivité de × par rapport à +) qui sont automatiquement vraies car $(\mathbb{K}, +, \times)$ est un corps.

Exercice d'application 11. On pose $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2},\ a, b \in \mathbb{Q}\}$. Montrer que $(\mathbb{Q}[\sqrt{2}], +, \times)$ est un sous-corps de $\mathbb{R}$.

Définition. Soient $(A, +, \times)$ et $(B, +, \times)$ deux anneaux et $\varphi : A \to B$. On dit que φ est un morphisme d'anneaux si :

- $\forall x, y \in A,\ \varphi(x + y) = \varphi(x) + \varphi(y)$.
- $\forall x, y \in A,\ \varphi(x \times y) = \varphi(x) \times \varphi(y)$.
- $\varphi(1_A) = 1_B$.

Si de plus, φ est bijective, on dit que φ est un isomorphisme (d'anneaux).

V. Correction des exercices

Exercice d'application 1.

1) Pour tout $x, y \in \mathbb{R}$, $e^x + e^y > 0$ donc la loi $*$ est bien définie. De plus, si on considère $x, y, z \in \mathbb{R}$, alors :

$$\begin{aligned} x * (y * z) &= x * (\ln(e^y + e^z)) \\ &= \ln(e^x + e^{\ln(e^y+e^z)}) \\ &= \ln(e^x + e^y + e^z). \end{aligned}$$

On calcule de même $(x * y) * z$ et on trouve le même résultat. La loi $*$ est donc associative. On a également $\forall x, y \in \mathbb{R},\ x * y = y * x$, ce qui entraine que $*$ est commutative.

2) Si on note y l'éventuel élément neutre, on cherche $y \in \mathbb{R}$ tel que $\forall x \in \mathbb{R},\ x * y = y * x = x$. On veut donc en particulier $\ln(e^x + e^y) = x \Leftrightarrow e^x + e^y = e^x \Leftrightarrow e^y = 0$. Ceci est absurde. Il n'y a donc pas d'élément neutre pour $*$.

Exercice d'application 2. Si $*$ est commutative, on a $x * y = y * x$ ce qui implique que $x * y = e$ implique $y * x = e$, et on a donc x inversible d'inverse y.

Exercice d'application 3. Remarquons que pour $a = 0$, on a $\mathrm{Id}_{\mathbb{R}} \in G$. De plus, $\circ$ est associative. Vérifions que G est stable pour $\circ$. Si $a, b \in \mathbb{R}$, on a :

$$f_a \circ f_b : x \mapsto f_a(f_b(x)) = f_b(x) + a = x + b + a = f_{a+b}(x).$$

On a donc $f_a \circ f_b = f_{a+b} \in G$ donc G est stable pour $\circ$. Enfin, on remarque que $f_a \circ f_{-a} = f_{-a} \circ f_a = \mathrm{Id}_{\mathbb{R}}$. Tout élément de G a donc un inverse dans G. On a donc $(G, \circ)$ qui est bien un groupe.

On remarque qu'il s'agit d'un groupe commutatif puisque pour tout $a, b \in \mathbb{R}$, $f_a \circ f_b = f_{a+b} = f_b \circ f_a$.

Exercice d'application 4.

1) Puisque $a^2 = e$, on a $a * a = e$, d'où $a^{-1} = a$. De même, on a $b^{-1} = b$. Puisque $(a * b)^2 = e$, on a (par associativité de $*$) :

$$\begin{aligned} & a * b * a * b = e \\ \Leftrightarrow\ & a * b * a * b * (b * a) = b * a \\ \Leftrightarrow\ & a * b * a * (b * b) * a = b * a \\ \Leftrightarrow\ & a * b * a * a = b * a \\ \Leftrightarrow\ & a * b = b * a. \end{aligned}$$

On a donc bien a et b qui commutent.

2) On a par associativité de $*$:

$$\begin{aligned} (b * a * b^{-1})^n &= b * a * b^{-1} * b * a * b^{-1} * b * a * \ldots b^{-1} * b * a * b^{-1} \\ &= b * a * a * \ldots * a * b^{-1} \\ &= b * a^n * b^{-1} \\ &= b * e * b^{-1} \\ &= b * b^{-1} \\ &= e. \end{aligned}$$

Exercice d'application 5. Soit $n \in \mathbb{N}^*$. On a $e \in G$ car $e^n = e * e * \ldots * e = e$. On a clairement $H_n \subset G$. Prenons à présent $x, y \in H_n$. On a alors puisque $*$ est commutative que :

$$(x * y)^n = x * y * x * y * \ldots * x * y = x * x * \ldots * x * y * y * \ldots * y = x^n * y^n.$$

On a donc $(x*y)^n = e*e = e$ d'où $x*y \in H_n$. Il ne reste plus qu'à vérifier que pour $x \in H_n$, $x^{-1} \in H_n$ pour montrer que H_n est un sous-groupe de G. Or, puisque $x^n = e$, on a $x^n*(x^{-1})^n = (x^{-1})^n$. Puisque $x^n*(x^{-1})^n = x*x*\ldots*x*x^{-1}*x^{-1}*\ldots*x^{-1} = e$. On a donc $x^{-1} \in H_n$ ce qui prouve que H_n est un sous-groupe de G.

Exercice d'application 6. On a $\varphi_1(0) = 0$ et pour $n_1, n_2 \in \mathbb{Z}$, $\varphi_1(n_1+n_2) = 3(n_1+n_2) = 3n_1+3n_2 = \varphi_1(n_1) + \varphi_1(n_2)$. On en déduit que φ_1 est un morphisme de groupe.

On a par contre $\varphi_2(-1+1) = \varphi_2(0) = 0$ et $\varphi_2(-1) + \varphi_2(1) = 2$. On en déduit que φ_2 n'est pas un morphisme de groupe.

Exercice d'application 7. φ est bien définie de $\mathbb{Z}$ dans $\mathbb{Q}_+^*$. On a $\varphi(0) = 1$ et pour $n_1, n_2 \in \mathbb{Z}$:

$$\varphi(n_1+n_2) = 2^{n_1+n_2} = 2^{n_1} \times 2^{n_2} = \varphi(n_1) \times \varphi(n_2).$$

On en déduit que φ est un morphisme de groupe. Ceci entraine que $\mathrm{Im}(\varphi) = \varphi(\mathbb{Z})$ est un sous groupe de $\mathbb{Q}_+^*$ pour la loi $\times$, et donc que $\{2^n,\ n \in \mathbb{Z}\}$ est un groupe pour la loi $\times$.

Exercice d'application 8. L'exponentielle est un morphisme de groupe bijectif de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+^*, \times)$. Ces deux groupes sont donc isomorphes.

Exercice d'application 9. On a $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$, $1 = 1 + 0 \times \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Il reste à montrer que $\mathbb{Z}[\sqrt{2}]$ est un sous-groupe de $\mathbb{R}$ pour la loi $+$ et qu'il est stable pour la loi $\times$.

- On a $0 = 0+0\times\sqrt{2}$ donc $\mathbb{Z}[\sqrt{2}]$ est non vide. Enfin, pour $a, b, c, d \in \mathbb{Z}$, on a $a+b\sqrt{2}-(c+d\sqrt{2}) = (a-c) + (b-d)\sqrt{2}$. Puisque $a - c \in \mathbb{Z}$ et $b - d \in \mathbb{Z}$, on en déduit par caractérisation des sous-groupes que $\mathbb{Z}[\sqrt{2}]$ est un sous-groupe de $\mathbb{R}$ pour la loi $+$.
- Si $a, b, c, d \in \mathbb{Z}$, on a $(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + \sqrt{2}(ad + bc)$. Puisque $ac + 2bd \in \mathbb{Z}$ et $ad + bc \in \mathbb{Z}$, on a bien la stabilité par $\times$.

On en déduit que $\mathbb{Z}[\sqrt{2}]$ est bien un sous-anneau de $\mathbb{R}$.

Exercice d'application 10. On a $-1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ et $(1 + \sqrt{2})(-1 + \sqrt{2}) = -1 + 2 = 1$. Puisque $\times$ est commutative, on en déduit que $1 + \sqrt{2}$ est inversible d'inverse $-1 + \sqrt{2}$.

Exercice d'application 11. Pour montrer que $\mathbb{Q}[\sqrt{2}]$ est un sous-anneau de $\mathbb{R}$, on procède exactement comme dans la preuve de $\mathbb{Z}[\sqrt{2}]$ sous-anneau de $\mathbb{R}$ mais en remplaçant les $\mathbb{Z}$ par des $\mathbb{Q}$ dans la preuve.

La seule propriété à vérifier en plus est que les éléments non nuls de $\mathbb{Q}[\sqrt{2}]$ sont inversibles pour $\times$. Si $a, b \in \mathbb{Q}$ sont non tous les deux nuls, on a $a+b\sqrt{2} \neq 0$. En effet, si on avait par l'absurde $a+b\sqrt{2} = 0$, on aurait $b\sqrt{2} = -a$. Si $b \neq 0$, on aurait en divisant par b que $\sqrt{2}$ est rationnel ce qui est absurde. Si $b = 0$, on a $a = 0$ ce qui est absurde ! On prouve de la même façon que $a - b\sqrt{2} \neq 0$. On a alors :

$$\begin{aligned}
\frac{1}{a+b\sqrt{2}} &= \frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} \\
&= \frac{a-b\sqrt{2}}{a^2-2b^2} \\
&= \frac{a}{a^2-2b^2} - \frac{b}{a^2-2b^2}\sqrt{2}.
\end{aligned}$$

Puisque $\dfrac{a}{a^2-2b^2}$ et $-\dfrac{b}{a^2-2b^2}$ sont rationnels comme produits/sommes/quotients de rationnels, on a donc bien que $\dfrac{1}{a+b\sqrt{2}} \in \mathbb{Q}[\sqrt{2}]$, ce qui prouve que tous les éléments non nuls de $\mathbb{Q}[\sqrt{2}]$ sont inversibles. On a donc bien $\mathbb{Q}[\sqrt{2}]$ qui est un sous-corps de $\mathbb{R}$.