Université Moulay Ismaïl — A. U. 2020/2021
Faculté des Sciences et Techniques - Errachidia — Filière MIP, Module M112
Département de Mathématiques — Responsable : PROF. JAWAD SALHI

Série de Travaux-Dirigés : 2
Structures algébriques : Groupes, Anneaux et Corps

Exercice 1
Soit G un groupe d'élément neutre e tel que $\forall x \in G, x^2 = e$. Montrer que G est abélien.

Exercice 2
Soient $(G, \star)$ un groupe et H_1, H_2 deux sous-groupes de G. On suppose que $H_1 \cup H_2$ est un sous-groupe de G. Montrer que $H_1 \subset H_2$ ou $H_2 \subset H_1$.

Exercice 3
Soit G un groupe. Montrer que les parties suivantes sont des sous-groupes de G :

1. $\mathcal{Z}(G) = \{x \in G \mid \forall y \in G, xy = yx\}$ ($\mathcal{Z}(G)$ s'appelle le centre de G).
2. $aHa^{-1} = \{aha^{-1} \mid h \in H\}$ où $a \in G$ et H est un sous-groupe de G.

Exercice 4
Soit $(G, \cdot)$ un groupe fini et A, B deux sous-groupes de G. On note $AB = \{ab; a \in A, b \in B\}$. Montrer que AB est un sous-groupe de G si et seulement si $AB = BA$.

Exercice 5
Soit G un groupe multiplicatif et $f \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x^{-1} \end{array} \right.$ une application.

Montrer que f est un morphisme de groupes si et seulement si G est abélien.

Exercice 6 (Groupe des automorphismes intérieurs)
Soit $(G, \star)$ un groupe et $a \in G$. On note $\varphi_a \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & a \star x \star a^{-1} \end{array} \right.$.

1. Montrer que φ_a est un morphisme de groupes.
2. Montrer que φ_a est bijectif et déterminer $(\varphi_a)^{-1}$.

L'ensemble $\mathcal{A} = \{\varphi_a,\, a \in G\}$, muni de la loi de composition, est un groupe (on a d'ailleurs $\varphi_a \circ \varphi_b = \varphi_{ab}$), appelé groupe des automorphismes intérieurs de G.

Exercice 7
Trouver tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.

Exercice 8 (Congruence modulo un sous-groupe et théorème de Lagrange)
Soient G un groupe et H un sous-groupe de G. On appelle relation de congruence à droite modulo H sur G la relation définie pour tous $x, y \in H$ par :

$$x\mathcal{R}y \Longleftrightarrow xy^{-1} \in H.$$

1. Montrer que la relation $\mathcal{R}$ est une relation d'équivalence sur G. On note $H\backslash G$ l'ensemble quotient associé, et on l'appelle l'ensemble des classes à droites modulo H.
2. Montrer que $H\backslash G = \{Hx \mid x \in G\}$.
3. Montrer que $\mathrm{Card}(Hx) = \mathrm{Card}(H)$. (On rappelle que deux ensembles A et B ont le même cardinal s'il existe une bijection $f : A \to B$).
4. Supposons que G est fini. En déduire que le cardinal de H divise le cardinal de G.

Exercice 9 (Anneau de Boole)
Soit A un anneau tel que tout élément de A soit idempotent (i.e. $\forall x \in A, x^2 = x$).

1. Si $x \in A$ montrer que $2x = 0$. Montrer que A est commutatif.
2. Montrer que si $x, y \in A$ alors $xy(x + y) = 0$. Que dire si A est intègre ?

Exercice 10 (Eléments nilpotents d'un anneau)
Soit A un anneau. Un élément a de A est dit nilpotent si et seulement s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$.

1. Soit $(a, b) \in A^2$. Montrer que, si a est nilpotent et si $ab = ba$, alors ab est nilpotent.
2. Soit $a \in A$ nilpotent. Montrer que $1 - a$ est inversible dans A et exprimer $(1 - a)^{-1}$.
3. Soit $(a, b) \in A^2$. Montrer que, si a et b sont nilpotents et $ab = ba$, alors $a + b$ est nilpotent.

Exercice 11 (Anneau des entiers de Gauss)
On pose $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$.

1. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.
2. Donner ses éléments inversibles.

$\mathbb{Z}[i]$ est appelé l'anneau des entiers de Gauss.

Exercice 12
Soient $(K, +, \cdot)$ et $(L, +, \cdot)$ deux corps et soit $f : K \to L$ un morphisme d'anneaux.

1. Montrer que si $x \in K \setminus \{0_K\}$, alors $f(x)$ est inversible et déterminer son inverse.
2. En déduire qu'un morphisme de corps est injectif.

Exercice 13
Montrer que tout anneau intègre et fini est un corps.

Exercice 14
Soit $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{Q}$. On note :

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid (a, b) \in \mathbb{Q}^2\}.$$

Montrer que $(\mathbb{Q}[\sqrt{d}], +, \times)$ est un corps.

Exercice 15 (Endomorphisme du corps $\mathbb{R}$)
On veut montrer que le seul endomorphisme du corps $\mathbb{R}$ est l'identité. Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de corps (ou d'anneaux).

1. Montrer que pour tout $x \in \mathbb{Q}$, on a $f(x) = x$.
2. Montrer que pour tout $x \in \mathbb{R}^+$, on a $f(x) \in \mathbb{R}^+$.
3. Montrer que f est croissante.
4. Conclure.

Corrigé de la série de Travaux-Dirigés : 2
Structures algébriques : Groupes, Anneaux et Corps

Exercice 1
Soit G un groupe d'élément neutre e tel que $\forall x \in G, x^2 = e$. Montrer que G est abélien.
Solution :

Suppposons que tout carré soit égal à l'élément neutre. Alors

$$xy = y^2xyx^2 = y(yxyx)x = y(yx)^2x = yex = yx.$$

Autre méthode : Soit $x, y \in G$. En utilisant le fait que pour tout $z \in G$ on a $z^2 = 1$, i.e. $z = z^{-1}$, on en déduit que

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$

et G est abélien.

Exercice 2
Soient $(G, \star)$ un groupe et H_1, H_2 deux sous-groupes de G. On suppose que $H_1 \cup H_2$ est un sous-groupe de G. Montrer que $H_1 \subset H_2$ ou $H_2 \subset H_1$.
Solution :

Raisonnons par l'absurde et supposons que $H_1 \not\subseteq H_2$ et $H_2 \not\subseteq H_1$. Alors, il existe $x_1 \in H_1$, $x_1 \notin H_2$ et il existe $x_2 \in H_2$, $x_2 \notin H_1$. Comme $H_1 \cup H_2$ est un sous-groupe, $x_1 \star x_2 \in H_1 \cup H_2$. Si $x_1 \star x_2 \in H_1$, alors $x_2 = x_1' \star (x_1 \star x_2) \in H_1$, ce qui est absurde. De même, on parvient à une absurdité en supposant $x_1 \star x_2 \in H_2$. D'où le résultat.

Exercice 3 Soit G un groupe. Montrer que les parties suivantes sont des sous-groupes de G :

1. $\mathcal{Z}(G) = \{x \in G \mid \forall y \in G, xy = yx\}$ ($\mathcal{Z}(G)$ s'appelle le centre de G).
2. $aHa^{-1} = \{aha^{-1} \mid h \in H\}$ où $a \in G$ et H est un sous-groupe de G.

Solution :

1. 1_G est élément de $\mathcal{Z}(G)$ car $1_G y = y 1_G = y$ pour tout $y \in G$. Soient $x_1, x_2 \in \mathcal{Z}(G)$. Alors, pour tout $y \in G$, on a $x_1x_2y = x_1(x_2y) = (x_1y)x_2 = yx_1x_2$ et donc $x_1x_2 \in \mathcal{Z}(G)$. Enfin, si $x \in \mathcal{Z}(G)$, alors pour tout $y \in G$,

$$xy = yx \Longrightarrow xyx^{-1} = y \Longrightarrow yx^{-1} = x^{-1}y.$$

   On en déduit que $x^{-1} \in \mathcal{Z}(G)$ qui est donc un sous-groupe de G.
2. Puisque H est un sous-groupe de G, $1_G \in H$ et donc $a1_Ga^{-1} \in aHa^{-1}$. Mais $a1_Ga^{-1} = 1_G$ et donc $1_G \in aHa^{-1}$. soient $x = aha^{-1}$ et $y = ah'a^{-1}$ deux éléments de aHa^{-1} avec donc $h, h' \in H$. On a $xy^{-1} = aha^{-1}\big(ah'a^{-1}\big)^{-1} = aha^{-1}\big(ah'^{-1}a^{-1}\big) = ahh'^{-1}a^{-1} \in aHa^{-1}$ puisque $hh'^{-1} \in H$. aHa^{-1} est donc bien un sous-groupe de G.

Exercice 4
Soit $(G, \cdot)$ un groupe fini et A, B deux sous-groupes de G. On note $AB = \{ab; a \in A, b \in B\}$. Montrer que AB est un sous-groupe de G si et seulement si $AB = BA$.
Solution :

($\Rightarrow$) Supposons que AB est un sous-groupe de G et montrons que $AB = BA$. Soit $x \in AB$. Alors $x^{-1} \in AB$ et donc $x^{-1} = ab$ pour certains $a \in A$ et $b \in B$. Par passage à l'inverse, on obtient : $x = b^{-1}a^{-1} \in BA$.
De même, si $y = ba \in BA$, alors $y^{-1} = a^{-1}b^{-1} \in AB$ et donc $y = (y^{-1})^{-1} \in AB$.
($\Leftarrow$) Supposons que $AB = BA$ et montrons que AB est un sous-groupe de G.
— Puisque A et B sont deux sous-groupes de G, alors $1_G \in A$ et $1_G \in B$ et donc $1_G = 1_G 1_G \in AB$.
— Soit $x = ab \in AB$ et $y = a'b' \in AB$. Alors, $xy = aba'b'$. Or, $ba' \in BA = AB$ et donc $ba' = a''b''$ avec $a'' \in A$ et $b'' \in B$. On en déduit que : $xy = aa''b''b' \in AB$.
— Soit $x = ab \in AB$. Alors, $x^{-1} = b^{-1}a^{-1} \in BA = AB$.

Exercice 5
Soit G un groupe multiplicatif et $f \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & x^{-1} \end{array} \right.$ une application.
Montrer que f est un morphisme de groupes si et seulement si G est abélien.
Solution :

($\Rightarrow$) Supposons que f est un morphisme de groupes. Pour tous $x, y \in G$, on a

$$xy = f(x^{-1})f(y^{-1}) = f(x^{-1}y^{-1}) = (x^{-1}y^{-1})^{-1} = yx$$

et G est abélien.
($\Leftarrow$) Réciproquement, supposons que G est abélien. Soit $x, y \in G$. On a

$$f(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = f(x)f(y)$$

et donc f est un morphisme de groupes.

Exercice 6 (Groupe des automorphismes intérieurs)
Soit $(G, \star)$ un groupe et $a \in G$. On note $\varphi_a \left| \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & a \star x \star a^{-1} \end{array} \right.$.

1. Montrer que φ_a est un morphisme de groupes.
2. Montrer que φ_a est bijectif et déterminer $(\varphi_a)^{-1}$.

L'ensemble $\mathcal{A} = \{\varphi_a, \, a \in G\}$, muni de la loi de composition, est un groupe (on a d'ailleurs $\varphi_a \circ \varphi_b = \varphi_{ab}$), appelé groupe des automorphismes intérieurs de G. **Solution :** Laissé au lecteur

Exercice 7

Trouver tous les morphismes de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$.
Solution :

Soit f un morphisme de groupes de $(\mathbb{Q}, +)$ dans $(\mathbb{Z}, +)$. $Im(f)$ est un sous-groupe de $\mathbb{Z}$ et donc $Im(f) = n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$. Supposons que $n \geq 1$. Soit x un antécédant de n. On obtient alors : $2f(\frac{x}{2}) = f(x) = n$ et donc $\frac{n}{2} = f(\frac{x}{2}) \in n\mathbb{Z}$, ce qui est absurde. On a donc $n = 0$ et f est nul.

Exercice 8 (Congruence modulo un sous-groupe et théorème de Lagrange)
Soient G un groupe et H un sous-groupe de G. On appelle relation de congruence à droite modulo H sur G la relation définie pour tous $x, y \in H$ par :

$$x\mathcal{R}y \Longleftrightarrow xy^{-1} \in H.$$

1. Montrer que la relation $\mathcal{R}$ est une relation d'équivalence sur G. On note $H\backslash G$ l'ensemble quotient associé, et on l'appelle l'ensemble des classes à droites modulo H.
2. Montrer que $H\backslash G = \{Hx \mid x \in G\}$.
3. Montrer que $\mathrm{Card}(Hx) = \mathrm{Card}(H)$. (On rappelle que deux ensembles A et B ont le même cardinal s'il existe une bijection $f : A \to B$).
4. Supposons que G est fini. En déduire que le cardinal de H divise le cardinal de G.

Solution :

1. — $x\mathcal{R}x$ car $xx^{-1} = 1_G \in H$.
   — Si $x\mathcal{R}y$, alors $xy^{-1} \in H$, d'où $(xy^{-1})^{-1} = yx^{-1} \in H$, donc $y\mathcal{R}x$.
   — Si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $xz^{-1} = (xy^{-1})(yz^{-1}) \in H$, donc $x\mathcal{R}z$.
2. Montrons que $H\backslash G = \{Hx \mid x \in G\}$, où l'on a noté $H\backslash G$ l'ensemble quotient : $G/\mathcal{R} = \{\bar{x} | x \in G\}$. Soit $x \in G$. Pour tout $y \in G$, on a :

$$\begin{aligned} y \in \bar{x} \Leftrightarrow x\mathcal{R}y &\Leftrightarrow xy^{-1} \in H \\ &\Leftrightarrow \exists h \in H : xy^{-1} = h \\ &\Leftrightarrow \exists h \in H : y^{-1} = x^{-1}h \\ &\Leftrightarrow \exists h \in H : y = h^{-1}x \\ &\Leftrightarrow y \in Hx \end{aligned}$$

   Donc : $H\backslash G = \{\bar{x} | x \in G\} = \{Hx \mid x \in G\}$.

3. Montrons que $\mathrm{Card}(Hx) = \mathrm{Card}(H)$. Soit $x \in G$ et considérons l'application $\begin{array}{rccc} \varphi_x : & H & \longrightarrow & Hx \\ & h & \longmapsto & hx. \end{array}$
   — φ_x est injective : Soit $h_1, h_2 \in H$ tel que $\varphi_x(h_1) = \varphi_x(h_2)$. alors $h_1x = h_2x$ et en multipliant à droite par x^{-1}, on obtient : $h_1 = h_2$.
   — φ_x est surjective : Soit $y \in Hx$. Par définition de Hx, il existe $h \in H$ tel que $y = hx = \varphi_x(h)$. D'où φ_x est bijective et donc $\mathrm{Card}(Hx) = \mathrm{Card}(H)$.
4. Supposons que G est fini. Montrons que $\mathrm{Card}(H)$ divise $\mathrm{Card}(G)$. Les classes d'éqquivalences forment une partition de G, donc s'il y a k classes, alors $\mathrm{Card}(G) = k\,\mathrm{Card}(H)$. En effet,

$$\begin{aligned} \mathrm{Card}(G) = \sum_{\bar{x} \in G/\mathcal{R}} \mathrm{Card}(\bar{x}) &= \sum_{\bar{x} \in G/\mathcal{R}} \mathrm{Card}(Hx) \\ &= \sum_{\bar{x} \in G/\mathcal{R}} \mathrm{Card}(H) \\ &= \mathrm{Card}(H) \sum_{\bar{x} \in G/\mathcal{R}} 1 \\ &= \mathrm{Card}(H)\,\mathrm{Card}(G/\mathcal{R}). \end{aligned}$$

   D'où le résultat.

Exercice 9 (Anneau de Boole)
Soit A un anneau tel que tout élément de A soit idempotent (i.e. $\forall x \in A, x^2 = x$).

1. Si $x \in A$ montrer que $2x = 0$. Montrer que A est commutatif.
2. Montrer que si $x, y \in A$ alors $xy(x+y) = 0$. Que dire si A est intègre ?

Solution :

1. Soit $x \in A$. Alors $(2x)^2 = 2x$ donc $4x^2 = 2x$, ce qui entraine $4x = 2x$ et donc $2x = 0$. Ce qui s'écrit encore $x = -x$.
   Montrons que A est commutatif. Soit $x, y \in A$, alors $x + y \in A$. Ainsi, par définition de A, on obtient $(x+y)^2 = x + y$ et donc $x^2 + xy + yx + y^2 = x + y = x^2 + y^2$. D'où, $xy + yx = 0$ et donc $xy = -yx = yx$. Ce qui montre que A est commutatif.
2. Soit $x, y \in A$, alors $xy(x+y) = xyx + xy^2 = x^2y + xy^2 = 2xy = 0$.
   Sopposons que A est intègre. Alors A a au plus deux éléments. En effet, sinon il existe $x, y \in A$ distincts et différents de 0. Donc $(x+y) \neq 0$ (car sinon $x = -y = y$) et A étant intègre $xy(x+y) \neq 0$, absurde.

Exercice 10 (Eléments nilpotents d'un anneau)
Soit A un anneau. Un élément a de A est dit nilpotent si et seulement s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$.

1. Soit $(a, b) \in A^2$. Montrer que, si a est nilpotent et si $ab = ba$, alors ab est nilpotent.
2. Soit $a \in A$ nilpotent. Montrer que $1 - a$ est inversible dans A et exprimer $(1-a)^{-1}$.
3. Soit $(a, b) \in A^2$. Montrer que, si a et b sont nilpotents et $ab = ba$, alors $a + b$ est nilpotent.

Solution : Laissé au lecteur.

Exercice 11 (Anneau des entiers de Gauss)
On pose $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$.

1. Montrer que $\mathbb{Z}[i]$ est un sous-anneau de $(\mathbb{C}, +, \times)$.
2. Donner ses éléments inversibles.

$\mathbb{Z}[i]$ est appelé l'anneau des entiers de Gauss.
Solution :

1. On a $1 = 1 + 0 \times i$ donc $1 \in \mathbb{Z}[i]$. Soient z_1 et z_2 dans $\mathbb{Z}[i]$. Il existe a_1, b_1, a_2 et b_2 dans $\mathbb{Z}$ tels que $z_1 = a_1 + ib_1$ et $z_2 = a_2 + ib_2$. On a alors
   $$z_1 - z_2 = (a_1 - a_2) + i(b_1 - b_2) \quad \text{et} \quad z_1 z_2 = (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + a_2 b_1)$$
   et comme $a_1 - a_2, b_1 - b_2, a_1 a_2 - b_1 b_2$ et $a_1 b_2 + a_2 b_1$ appartiennent à $\mathbb{Z}$, $z_1 - z_2 \in \mathbb{Z}[i]$ et $z_1 z_2 \in \mathbb{Z}[i]$.
2. Soit $z = a + ib \in \mathbb{Z}[i]^\times$, où $a, b \in \mathbb{Z}$. Alors, il existe $z' = a' + ib' \in \mathbb{Z}[i]$ tel que $zz' = 1$. Donc $|z|^2 |z'|^2 = 1$. Or, comme $z, z' \in \mathbb{Z}[i]$, alors $|z|^2, |z'|^2 \in \mathbb{N}$. Ainsi : $|z|^2 = |z'|^2 = 1$. Donc $a^2 + b^2 = 1$ et puisque $a, b \in \mathbb{Z}$, alors
   $$\left\{ \begin{array}{l} a^2 = 1 \text{ et } b^2 = 0 \\ \text{ou} \\ a^2 = 0 \text{ et } b^2 = 1 \end{array} \right.$$
   et donc $z \in \{-1, 1, i, -i\}$. D'où $\mathbb{Z}[i]^\times \subset \{-1, 1, i, -i\}$.
   Inversement, il est facile de vérifier que $\{-1, 1, i, -i\} \subset \mathbb{Z}[i]^\times$. D'où l'égalité $\mathbb{Z}[i]^\times = \{-1, 1, i, -i\}$.

Exercice 12
Soient $(K,+,\cdot)$ et $(L,+,\cdot)$ deux corps et soit $f : K \to L$ un morphisme d'anneaux.

1. Montrer que si $x \in K \setminus \{0_K\}$, alors $f(x)$ est inversible et déterminer son inverse.
2. En déduire qu'un morphisme de corps est injectif.

Solution :

1. Soit $x \in K \setminus \{0_K\}$. Alors on a $x \cdot x^{-1} = 1_K$. On applique f à cette identité, et en utilisant que f est un morphisme d'anneaux, on trouve $f(x) \cdot f\left(x^{-1}\right) = 1_L$. Ainsi, $f(x)$ est inversible, d'inverse $f\left(x^{-1}\right)$.
2. Il suffit de démontrer que le noyau de f est réduit à 0_K. Mais si $f(x) = 0$, alors $x \notin K \setminus \{0_K\}$ d'après la question précédente, et donc $x = 0$.

Exercice 13
Montrer que tout anneau intègre et fini est un corps.
Solution :

Soit $a \in A$ non nul. L'application $f_a \left| \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & ax \end{array} \right.$ est injective. En effet, puisque A est un anneau intègre et a est non nul, pour tous $x, y \in A$, on a

$$f_a(x) = f_a(y) \Longrightarrow ax = ay \Longrightarrow ax - ay = 0 \Longrightarrow a(x-y) = 0 \Longrightarrow x = y.$$

Et comme A est un ensemble fini, toute injection de A dans A est une bijection. Ainsi f_a est bijective. Soit $b \in A$ l'antécédent de 1 par f_a. Alors : $ab = f_a(b) = 1$.
On a montré que pout tout $a \in A$ non nul, $\exists b \in A$ tel que $ab = 1$. De plus, comme A est intègre, alors on aussi $ba = 1$ et donc b est l'inverse de a. En effet, puisque $ab = 1$, alors : $a(ba-1) = a(ba) - a = (ab)a - a = 1 \times a - a = a - a = 0$. Or $a \neq 0$ et A est intègre, donc $ba - 1 = 0$, i.e, $ba = 1$. D'où le résultat.

Exercice 14
Soit $d \in \mathbb{N}$ tel que $\sqrt{d} \notin \mathbb{Q}$. On note :

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid (a,b) \in \mathbb{Q}^2\}.$$

Montrer que $(\mathbb{Q}[\sqrt{d}], +, \times)$ est un corps.
Solution :

On va montrer qu'il s'agit d'un sous-corps de $(\mathbb{R}, +, \times)$. Remarquons d'abord que $\mathbb{Q}[\sqrt{d}] \subset \mathbb{R}$ et que $1 \in \mathbb{Q}[\sqrt{d}]$. soient $x, y \in \mathbb{Q}[\sqrt{d}]$. On les écrit $x = a + b\sqrt{d}$ et $y = a' + b'\sqrt{d}$ avec $a, a', b, b' \in \mathbb{Q}$. Alors :

$$\begin{aligned} x - y &= \left(a - a'\right) + \left(b - b'\right)\sqrt{d} \\ xy &= \left(aa' + dbb'\right) + \left(ab' + a'b\right)\sqrt{d} \end{aligned}$$

ce qui prouve que $x - y$ et $xy \in \mathbb{Q}[\sqrt{d}]$. D'autre part, si $x \neq 0$, on peut multiplier numérateur et dénominateur par la quantité conjugée $a - b\sqrt{d}$ et l'on obtient

$$\frac{1}{x} = \frac{1}{a + b\sqrt{d}} = \frac{a - b\sqrt{d}}{a^2 - b^2 d} = \frac{a}{a^2 - b^2 d} - \frac{b}{a^2 - b^2 d}\sqrt{d} \in \mathbb{Q}[\sqrt{d}]$$

et donc $\frac{1}{x} \in \mathbb{Q}[\sqrt{d}]$. Remarquons qu'il était possible de multiplier par la quantité conjuguée qui est non nulle car $\sqrt{d} \notin \mathbb{Q}$. D'où le résultat.

Exercice 15 (Endomorphisme du corps $\mathbb{R}$)
On veut montrer que le seul endomorphisme du corps $\mathbb{R}$ est l'identité. Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de corps (ou d'anneaux).

1. Montrer que pour tout $x \in \mathbb{Q}$, on a $f(x) = x$.
2. Montrer que pour tout $x \in \mathbb{R}^+$, on a $f(x) \in \mathbb{R}^+$.
3. Montrer que f est croissante.
4. Conclure.

Solution :

1. Puisque f est un morphisme d'anneaux, alors f(1)=1 et $\forall n \in \mathbb{Z}$, $f(n) = f(n.1) = nf(1) = n$.
   Soit $x = \frac{p}{q} \in \mathbb{Q}$, où $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$. D'après ce qui précède, on a : $p = f(p) = f(qx) = qf(x)$. Donc $f(x) = \frac{p}{q} = x$.
2. Soit $x \in \mathbb{R}^+$. On a $f(x) = f((\sqrt{x})^2) = (f(\sqrt{x}))^2 \in \mathbb{R}^+$.
3. soit $x, y \in \mathbb{R}$ tel que $x \leq y$. Comme $y - x \geq 0$, alors d'après la question (2) on a : $f(y - x) = f(y) - f(x) \geq 0$. Donc $f(x) \leq f(y)$. Ce qui montre que f est croissante.
4. Soit $x \in \mathbb{R}$. Il existe deux suites $(r_n)_{n\in\mathbb{N}}, (s_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$ convergentes vers x telles que :
   $$\forall n \in \mathbb{N},\, r_n := \frac{E(10^n x)}{10^n} \leq x < s_n := \frac{E(10^n x)}{10^n} + \frac{1}{10^n},$$
   où $E(\cdot)$ désigne la fonction partie entière.
   En utilisant le fait que f est croissante, alors : $\forall n \in \mathbb{N},\ f(r_n) = r_n \leq f(x) \leq f(s_n) = s_n$. Les suites extrémités convergent vers x et donc $f(x) = x$. Ainsi le seul endomorphisme d'anneaux de $\mathbb{R}$ dans $\mathbb{R}$ est l'identité.