Exercices - Anneaux et Corps -

Corrigé

EX2.1 # Par hypothèse, on a

$$((1_A+y).x)^2=(1_A+y)^2.x^2$$

Comme $(1_A+y).x=1_A.x+y.x=x+y.x$, on obtient

$$((1_A+y).x)^2=(x+y.x)^2=x^2+x.y.x+y.x.x+(y.x)^2$$
$$=x^2+x.y.x+y.x^2+y^2.x^2 \quad (\text{car } (y.x)^2=y^2.x^2)$$

D'autre part, comme $(1_A+y)^2=1_A+2y+y^2$, on obtient

$$((1_A+y).x)^2=(1_A+y)^2.x^2=(1_A+2y+y^2).x^2$$
$$=x^2+2y.x^2+y^2.x^2$$

D'où, en comparant les deux expressions, il vient.

$$x.y.x=y.x^2$$

De la même manière, en utilisant

$$(x.(1_A+y))^2=x^2.(1_A+y)^2, \text{ on trouve}$$

$$x.y.x=x^2.y.$$

En remplaçant x par 1_A+x dans $y.x^2=x^2.y$, on trouve

$$y.(1_A+x)^2=(1_A+x)^2.y$$

d'où
$$y.(1_A+2x+x^2)=(1_A+2x+x^2).y$$

d'où
$$y+2y.x+y.x^2=y+2x.y+x^2.y$$

d'où
$$2(y.x-x.y)=0_A \quad (\text{car } y.x^2=x^2.y)$$

c-à-dire
$$(y.x-x.y)+(y.x-x.y)=0_A$$

La deuxième hypothèse de l'exercice implique

$$y.x-x.y=0_A$$

d'où $\quad y.x = x.y$

Alors l'anneau A est commutatif.

EX2.2 : La distributivité implique

$$(1_A - a).(1_A + a + a^2) = 1_A + a + a^2 - a - a^2 - a^3$$
$$= 1_A - a^3$$
$$= 1_A \quad \text{puisque } a^3 = 0_A$$

De même

$$(1 + a + a^2).(1_A - a) = 1_A + a + a^2 - a - a^2 - a^3$$
$$= 1_A - a^3$$
$$= 1_A \quad \text{puisque } a^3 = 0_A.$$

Finalement, $1_A - a$ est inversible d'inverse $1_A + a + a^2$.

EX2.3 : Comme l'anneau A est commutatif, la binôme donne

$$(a+b)^5 = a^5 + 5a^4.b + 10a^3.b^2 + 10a^2.b^3 + 5a.b^4 + b^5.$$

Par hypothèse $b^2 = 0_A$ d'où $b^3 = b^4 = b^5 = 0_A$

et $a^3.b^2 = a^2.b^3 = a.b^4 = 0_A$

Finalement

$$(a+b)^5 = a^5 + 5a^4.b.$$

EX2.4 : Par hypothèse, ab est inversible, alors

$(\exists x \in A)$; $\quad (a.b).x = 1_A$ et $x.(a.b) = 1_A$

c-à-d $\quad a.(bx) = 1_A = (x.a).b$

d'où $(b.x)$ est l'inverse à droite de a,

et $(x.a)$ est l'inverse à gauche de b.

D'autre part, par distributivité, on a

$$(b.a).(b.x.a - 1_A) = (ba)(bxa) - (ba)$$
$$= b(abx)a - ba$$

d'où $\quad (ba)\big((bx)a - 1_A\big) = b.1_A.a - b.a$

$$= 0_A$$

Or (ba) n'est pas un diviseur de 0_A, alors

$$(bx).a - 1_A = 0_A$$

d'où $\quad (bx)a = 1_A \quad$ et $\quad b(xa) = 1_A$

donc (bx) est aussi l'inverse à gauche de a,

et (xa) est aussi l'inverse à droite de b.

Finalement, a et b sont inversibles d'inverses respectifs bx et xa.

<u>EX2.5</u> $\quad a$ et b sont nilpotents signifie que.

$$(\exists\, n, p \in \mathbb{N}\setminus\{0,1\})\ ; \quad a^n = 0_A \ \text{ et } \ b^p = 0_A$$

Comme l'anneau est commutatif, la binôme donne

$$(a+b)^{n+p} = \sum_{k=0}^{n+p} C_{n+p}^k\, a^k\, b^{n+p-k}$$

Si $k \geqslant n$; $a^k = 0_A$

~~Si $k < n$, alors $n+p-k \geqslant p$; $b^{n+p-k} = 0_A$~~

Si $k \leqslant n$, alors $n+p-k \geqslant p$ et donc $b^{n+p-k} = 0_A$

Finalement, on obtient

$$(a+b)^{n+p} = 0_A \quad \text{donc } a+b \text{ est nilpotent.}$$

<u>EX2.6</u> $\quad$ Il suffit de remarquer que :

$$(\forall n \in \mathbb{N}) : \quad (1_A - a).\Big(\sum_{k=0}^{n} a^k\Big) = \sum_{k=0}^{n} a^k(1_A - a) = 1_A - a^{n+1}$$

En prenant n tel que $a^{n+1} = 0_A$, il vient que $1_A - a$ est inversible d'inverse

$$(1_A - a)^{-1} = \sum_{k=0}^{n} a^k$$

EX2.7 ab est nilpotent, alors

$$(\exists n \in \mathbb{N}\setminus\{0,1\}) \; ; \; (ab)^n = 0_A$$

On a :

$$(ba)^{n+1} = \underbrace{(ba).(ba).\dots(ba)}_{(n+1)-\text{termes}}$$

$$= b\underbrace{(ab)(ab)\dots(ab)}_{n-\text{termes}}a \quad \text{(d'après l'associativité)}$$

$$= b(ab)^n a$$

$$= b.0_A.a = 0_A.$$

Finalement (ba) est aussi nilpotent.

EX2.8 1) si ϕ est un morphisme d'anneaux, alors

$$\phi(x+y) = \phi(x) + \phi(y)$$

d'où $$(x+y)^2 = x^2 + y^2.$$

d'où $$(x+y).(x+y) = x^2 + y^2$$

d'où $$x^2 + y.x + x.y + y^2 = x^2 + y^2$$

d'où $$y.x + x.y = 0_A$$

En particulier, pour $y = x$, on obtient

$$x^2 + x^2 = 0_A \quad \text{d'où} \quad x^2 = -x^2.$$

2) si ϕ est surjectif, alors

$$(\forall a \in A)(\exists x \in A) \; ; \quad \phi(x) = a$$

c-à-dire $x^2 = a$.

Or d'après question 1), on a $x^2 = -x^2$, alors

$$(\forall a \in A) \; ; \quad a = -a$$

De plus, on a d'après la question 1) :

$(\forall x, y \in A)$; $\quad xy = -(yx)$

d'où $\quad xy = (-y)x$

$\quad\quad = yx \quad$ (puisque $y = -y$)

d'où $\quad (\forall x, y \in A)$; $\quad xy = yx$

Finalement, l'anneau A est commutatif.

EX 2.9 $\quad$ 1) Il suffit de vérifier que A est un sous-anneau de l'anneau $(\mathbb{R}, +, \times)$.

\# $\quad 1 = 1 + 0.\sqrt{5}$ avec $1 ; 0 \in \mathbb{Q}$, alors $1 \in A$.

\# $\quad$ Si $a = x + y\sqrt{5}$ et $b = x' + y'\sqrt{5}$ deux éléments de A, on a

$$a - b = (x - x') + (y - y')\sqrt{5} \text{ avec } x - x' ; y - y' \in \mathbb{Q}$$

d'où $\quad a - b \in A$

$\Rightarrow$ $(A, +)$ est un sous-groupe de $(\mathbb{R}, +)$.

\# $\quad$ si $a = x + y\sqrt{5}$ et $b = x' + y'\sqrt{5}$ éléments de A, on a

$$ab = \underbrace{(xx' + 5yy')}_{\in \mathbb{Q}} + \underbrace{(xy' + x'y)}_{\in \mathbb{Q}}\sqrt{5}$$

donc A est stable pour la multiplication dans $\mathbb{R}$

Finalement ; A est un sous-anneau de $(\mathbb{R}, +, \times)$ et donc $(A, +, \times)$ est un anneau pour + et × usuels.

2) De la même manière que pour A, vérifier que B est un sous-anneau de $(\mathbb{C}, +, \times)$.

3) Remarquons que $\sqrt[3]{2} = 0 + 1.\sqrt[3]{2} \in C$, montrons par l'absurd que C n'est pas stable par multiplication.
En effet, si C est stable, alors

$$\sqrt[3]{4} = \sqrt[3]{2} \times \sqrt[3]{2} \in C.$$

c-à-dire

$$(\exists u, v \in \mathbb{Z})\ ;\ \sqrt[3]{4} = u + v\sqrt[3]{2} \quad (*)$$

De $u = \sqrt[3]{4} - v\sqrt[3]{2}$, il vient que

$$\begin{aligned} u^2 &= \sqrt[3]{16} - 2v\sqrt[3]{8} + v^2\sqrt[3]{4} \\ &= 2\sqrt[3]{2} - 4v + v^2\sqrt[3]{4} \\ &= 2\sqrt[3]{2} - 4v + v^2(u + v\sqrt[3]{2}) \quad (\text{d'après } (*)) \\ &= uv^2 - 4v + (v^3+2)\sqrt[3]{2} \end{aligned}$$

d'où $(v^3+2)\sqrt[3]{2} = u^2 + 4v - uv^2$

Comme $v^3 + 2 \in \mathbb{Z}$ est non nul (2 n'est pas le cube d'aucun entier et aucun rationnel), alors

$$\sqrt[3]{2} = \frac{u^2+4v-uv^2 \in \mathbb{Z}}{v^3+2 \in \mathbb{Z}} \quad \text{est un rationnel}$$

Absurde et alors la proposition initiale $\sqrt[3]{4} = u + v\sqrt[3]{2}$ est fausse, et donc C n'est pas stable par multiplication dans $(\mathbb{R}, +, \times)$.

Conclusion : $(C, +, \times)$ n'est pas un anneau.

EX 2.10 À faire en exercice.

EX 2.11 1) $I + J$ est un sous-groupe de $(A, +)$, car

- $0_A = 0_A + 0_A \in I + J$ puisque I et J sont des sous-gpes de A et donc $0_A \in I$ et $0_A \in J$.
- si $x = i + j$ avec $i \in I$ et $j \in J$ et $y = i' + j'$ avec $i' \in I$ et $j' \in J$, deux éléments de $I + J$ on a :

$$x - y = \underbrace{(i - i')}_{\in I} + \underbrace{(j - j')}_{\in J} \in I + J$$

D'autre part, la distributivité de $\times$ par rapport à $+$ donne

$$(\forall a \in A); \quad a.x = a.(i+j)$$
$$= ai + aj$$

Comme I et J sont deux idéaux, alors

$$(\forall a \in A) \quad ai \in I \quad \text{et} \quad aj \in J$$

donc $$(\forall a \in A); \quad a.x = ai + aj \in I + J$$

Finalement;

$I+J$ est un idéal de A.

\# $I.J$ est un sous-groupe de $(A,+)$. car

- $0_A = 0_A . 0_A \in I.J$
- soit $x = \sum_{k=1}^{n} i_k j_k$ et $y = \sum_{l=1}^{m} i'_l j'_l$ deux éléments de $I.J$, on a:

$$x - y = \sum_{k=1}^{n} i_k j_k + \sum_{l=1}^{m} i'_l j'_l$$
$$= \sum_{r=1}^{n+m} i''_r j''_r$$

avec $\begin{cases} i''_r = i_r \text{ et } j''_r = j_r & \text{si } 1 \leq r \leq n \\ i''_r = i'_{r-n} \text{ et } j''_r = j'_{r-n} & \text{si } n+1 \leq r \leq n+m \end{cases}$

d'où $\quad x - y \in I.J$

D'autre part, on a

$$(\forall a \in A); \quad ax = a \sum_{k=1}^{n} i_k j_k$$
$$= \sum_{k=1}^{n} (a i_k) j_k$$

Comme I est un ideal de A, alors

$(\forall k=1..n)$; $\quad a i_k \in I$

d'où
$$ax = \sum_{j=1}^{n} (a i_k)\, j_k \in I.J$$

Finalement ;

$I.J$ est un ideal de A.

2) Soit $x = \sum_{k=1}^{n} i_k j_k \in I.J$. Comme I est un ideal

on a :
$$(\forall k=1..n), \quad i_k j_k = \underbrace{\overset{\in J \subset A}{j_k} \cdot \overset{\in I}{i_k}}_{A \text{ commutatif}} \in I$$

d'où $\quad x \in I$ (car I un sous-gpe et donc stable par la somme)

De la même, on montre $\quad x \in J \quad$ d'où $\quad x \in I \cap J$

Ainsi
$$I.J \subset I \cap J$$

3) Soit $x \in (I+J).(I\cap J)$. Alors

$$x = \sum_{k=1}^{n} a_k . b_k \quad \text{avec} \quad a_k \in I+J \text{ et } b_k \in I \cap J$$

Montrons que $x \in I.J$? Puisque $I.J$ est un ideal, il suffit de montrer que $a_k b_k \in I.J$?

On a : $\quad a_k = i_k + j_k \quad$ avec $\quad i_k \in I$ et $j_k \in J$

d'où
$$a_k b_k = i_k b_k + j_k b_k$$
$$= i_k b_k + b_k j_k \quad (A \text{ commutatif})$$

avec $\quad i_k \in I$; $b_k \in I\cap J \subset J$; $b_k \in I \cap J \subset I$ et $j_k \in J$

d'où $\quad a_k b_k \in I.J \quad (\forall k=1..n)$

Finalement, $\quad x \in I.J$ et donc
$$(I+J).(I\cap J) \subset I.J$$

4) On sait d'après la question 2) que

$$I.J \subset I \cap J.$$

Il suffit alors de montrer $I \cap J \subset I.J$, on a d'après la question 3)

$$(I+J).(I \cap J) \subset I.J$$

et comme I et J sont premiers entre eux, on a

$$I + J = A$$

et donc $\quad A.(I \cap J) \subset I.J$

c-à-dire $\quad (\forall a \in A) ; \quad a.(I \cap J) \subset I.J$

En particulier, pour $a = 1_A$, on obtient

$$I \cap J \subset I.J$$

Finalement, on trouve $\quad I \cap J = I.J.$

Ex 2.12 1) Montrons que $(I:J)$ sous groupe de $(A,+)$?

- $0_A J = \{0_A\} \subset I$ d'où $0_A \in (I:J)$
- soient x et y deux éléments de $(I:J)$, on a

$$(\forall j \in J) ; \quad (x-y).j = xj - yj$$

et $\quad xj \in xJ \subset I$ (car $x \in (I:J)$)

et $\quad yj \in xJ \subset I$ (car $y \in (I:J)$)

comme I est un sous-groupe de A, il vient

$$(\forall j \in J) ; \quad (x-y)j = xj - yj \in I$$

c-à-dire $\quad (x-y)J \subset I$

d'où $\quad x - y \in (I:J)$

D'autre part, soit $a \in A$ et $x \in (I:J)$ quelconque. On a.

$$(\forall j \in J) \quad (ax)j \in a(xJ) \subset aI \subset I$$

$xJ \subset I$ puisque $x \in (I:J)$ $\qquad$ I idéal de A

d'où $\quad (\forall j \in J), \quad (ax)j \in I$

d'où $\quad (ax)J \subset I$

d'où $\quad ax \in (I:J)$

Ainsi, $(I:J)$ est un idéal de A qui contient I

car : $\quad (\forall i \in I)(\forall j \in J); \quad ij = \underbrace{j}_{\in J \subset A}\underbrace{i}_{\in I} \in I \quad$ (I idéal de A)

c-à-dire $\quad (\forall i \in I); \; iJ \subset I$

c-à-dire $\quad (\forall i \in I); \; i \in (I:J)$.

c-à-dire $\quad I \subset (I:J)$.

2) Soit $x \in (I:J).J$, alors

$$x = \sum_{k=1}^{n} a_k b_k \text{ avec } a_k \in (I:J) \text{ et } b_k \in J$$

Comme ~~I/J~~ I est un idéal et donc stable par la somme, il suffit de montrer que $a_k b_k \in I$.

On a $\quad a_k \in (I:J) \Rightarrow a_k J \subset I$

$\Rightarrow a_k j \in I \quad (\forall j \in J)$

$\Rightarrow a_k b_k \in I \quad$ (on a pris $j = b_k \in J$).

Finalement, on trouve

$$(I:J).J \subset I.$$

3) Soit $x \in (I:J+K)$, alors $x(J+K) \subset I$

d'où $\quad xJ + xK \subset I$.

Ainsi $\quad xJ \subset xJ + xK \subset I$ et $xK \subset xJ + xK \subset I$

donc $\quad x \in (I:J)$ et $x \in (I:K)$

d'où $\quad x \in (I:J) \cap (I:K)$.

Inversement, on a :

$$x \in (I:J) \cap (I:K) \Rightarrow x \in (I:J) \text{ et } x \in (I:K)$$
$$\Rightarrow xJ \subset I \text{ et } xK \subset I$$
$$\Rightarrow xJ + xK \subset I$$
$$\Rightarrow x(J+K) \subset I$$
$$\Rightarrow x \in (I : J+K)$$

Finalement, on conclut

$$(I : J+K) = (I:J) \cap (I:K)$$

D'autre part, on a :

$$x \in (I \cap J : K) \Leftrightarrow xK \subset I \cap J$$
$$\Leftrightarrow xK \subset I \text{ et } xK \subset J$$
$$\Leftrightarrow x \in (I:K) \text{ et } x \in (J:K)$$
$$\Leftrightarrow x \in (I:K) \cap (J:K)$$

Ainsi, on trouve

$$(I \cap J : K) = (I:K) \cap (J:K)$$

<u>Ex 2.13</u> à faire.