ANNEAUX ET CORPS

Ce complément de cours prolonge le chapitre 36 ("Groupes et corps") de "Toutes les mathématiques " (TLM1).

1 Anneaux

1.1 Définition

Définition 1 *Soit* A *un ensemble muni de deux lois de composition internes notées* $+$ *et* $\times$*. On dit que* $(A,+,\times)$ *est un anneau si :*

- $(A,+)$ *est un groupe commutatif (on note* 0 *l'élément neutre).*
- *La loi* $\times$ *est associative et possède un élément neutre dans* A*, noté* 1*, différent de* 0*.*
- *La loi* $\times$ *est distributive par rapport à* $+$*, à droite et à gauche, c'est-à-dire*

$$\forall (a,b,c)\in A^3,\ a\times(b+c)=a\times b+a\times c \ \text{ et } \ (a+b)\times c=a\times c+b\times c.$$

Si de plus la loi $\times$ *est commutative, l'anneau est dit commutatif.*

Exemple 2 (1) *Les ensembles* $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ *sont des anneaux commutatifs pour l'addition et la multiplication usuelle.*

(2) *Soit* $\left(\mathbb{R}^{\mathbb{N}},+,\times\right)$ *où* $\mathbb{R}^{\mathbb{N}}$ *est l'ensemble des suites réelles muni des lois* $+$ *et* $\times$ *définies par : si* $u=(u_n)_{n\in\mathbb{N}}$, $v=(v_n)_{n\in\mathbb{N}}$ *alors* $u+v=(u_n+v_n)_{n\in\mathbb{N}}$ *et* $u\times v=(u_nv_n)_{n\in\mathbb{N}}$*. Alors* $\left(\mathbb{R}^{\mathbb{N}},+,\times\right)$ *est un anneau commutatif.*

(3) *Soit l'ensemble* $\mathcal{F}(I,\mathbb{R})=\{f:I\longrightarrow\mathbb{R}\}$ *où* I *est un ensemble. On munit* $\mathcal{F}(I,\mathbb{R})$ *de* $f+g:x\longmapsto f(x)+g(x)$ *et* $f\times g:x\longmapsto f(x)\,g(x)$*. Alors* $\mathcal{F}(I,\mathbb{R})$ *est un anneau commutatif.*

(4) $(\mathbb{R}[X],+,\times)$, *où* $\mathbb{R}[X]$ *est l'ensemble des polynômes à coefficients réels, est un anneau commutatif.*

(5) $(\mathbb{M}_n(\mathbb{K}),+,\times)$, *où* $\mathbb{M}_n(\mathbb{K})$ *est l'ensemble des matrices carrées à coefficients dans* $\mathbb{K}=\mathbb{R}$ *ou* $\mathbb{C}$*, est un anneau non commutatif.*

Définition 3 *On dit que l'anneau* $(A,+,\times)$ *est intègre si la loi* $\times$ *est commutative et si pour* a,b *dans* A*, on a*

$$a\times b=0\Longrightarrow a=0 \ \text{ ou } \ b=0$$

Exemple 4 (1) $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$, $(\mathbb{C},+,\times)$ *sont des anneaux intègres.*

(2) $(\mathbb{R}[X],+,\times)$ *est un anneau intègre.*

(3) $A=\mathcal{F}(\mathbb{R},\mathbb{R})$ *n'est pas un anneau intègre. En effet, soient* f *et* g *définie par*

$$f(x)=\begin{cases}1 \text{ si } x\geq 0\\ 0 \text{ si } x\leq 0\end{cases}\quad \text{et}\quad g(x)=\begin{cases}0 \text{ si } x\geq 0\\ 1 \text{ si } x\leq 0\end{cases}$$

Pour tout x *réel, on a alors* $f(x)\times g(x)=0$*, c'est-à-dire* $f\times g=0_A$ *(la fonction nulle, qui est l'élément neutre de* A*). Les fonctions* f *et* g *sont appelées des diviseurs de* 0*.*

(4) *De la même manière* $\mathbb{R}^{\mathbb{N}}$*, l'ensemble des suites réelles, n'est pas un anneau intègre (exercice 3)..*

1.2 Sous-anneau

Définition 5 *Soit* $(A,+,\times)$ *un anneau et* $B\subset A$ *une partie de* A*. On dit que* B *est un sous-anneau de* A *si :*

- $(B,+)$ *est un sous-groupe de* $(A,+)$*.*
- $\forall (a,b)\in B,\ a\times b\in B$ *(donc* $\times$ *est une loi de composition interne sur* B*).*
- *L'élément neutre* 1 *de la loi* $\times$ *de* A *est dans* B*.*

Remarque : Dans ce cas $(B,+,\times)$ est alors un anneau. En pratique, pour montrer qu'un objet est un anneau, on montre donc que c'est un sous anneau d'un anneau connu.

Exemple 6 (1) $\mathbb{Z}$ *est un sous-anneau de* $(\mathbb{Q},+,\times)$*.*

(2) $\mathcal{C}(I,\mathbb{R})$*, ensemble des fonctions continues sur l'intervalle* $I\subset\mathbb{R}$*, est un sous-anneau de* $(\mathcal{F}(I,\mathbb{R}),+,\times)$*.*

(3) *L'ensemble des suites bornées est un sous-anneau de* $\mathbb{R}^{\mathbb{N}}$*.*

(4) *L'ensemble des suites convergentes est un sous-anneau de* $\mathbb{R}^{\mathbb{N}}$*.*

(5) $\mathbb{Z}[i]=\{a+ib,\ (a,b)\in\mathbb{Z}\}$ *est un sous-anneau de* $(\mathbb{C},+,\times)$*. On l'appelle l'anneau des entiers de Gauss (exercice 2).*

1.3 Calcul dans un anneau

- Soit $x \in A$ alors $x \times 0_A = 0_A$ où 0_A est le neutre de la loi $+$.

Preuve. En effet, on a $x \times (x + 0_A) = x \times x + x \times 0_A$. Mais puisque 0_A est neutre, on a $x + 0_A = x$, ainsi $x \times (x + 0_A) = x \times x$. On en déduit que $x \times x + x \times 0_A = x \times x \Longrightarrow x \times 0_A = 0_A$. ■

- Soient a et b dans A, on note $a - b$ à la place de $a + (-b)$, on démontre alors que, $\forall (a, b, c) \in A^3$

$$a \times (b - c) = a \times b - a \times c \qquad (-a) \times b = -(a \times b) \qquad (-a) \times (-b) = a \times b$$

1.3.1 Notations usuelles

Soit $(A, +, \times)$ un anneau, pour $a \in A$, on note $-a$ le symétrique de a pour la loi $+$ et a^{-1} le symétrique pour la loi $\times$ lorsque a est inversible. Soit $n \in \mathbb{N}$, on note :

- Si $n = 0$, $0a = 0_A$ où 0_A est le neutre de A pour la loi $+$ et $a^0 = 1_A$ ou 1_A est le neutre pour la loi $\times$.
- Si $n > 0$, $na = \underbrace{a + \cdots + a}_{n \text{ fois}}$ et $a^n = \underbrace{a \times a \times \cdots \times a}_{n \text{ fois}}$
- Si $n < 0$, $na = (-n)(-a) = \underbrace{(-a) + \cdots + (-a)}_{-n \text{ fois}}$ et $a^n = \left(a^{-1}\right)^{-n} = \underbrace{a^{-1} \times \cdots \times a^{-1}}_{-n \text{ fois}}$

On a alors les règles usuelles
Soient $(a, b) \in A$ et $(n, p) \in \mathbb{Z}^2$

$$na + pa = (n + p)\, a \ , \ n(pa) = (np)\, a \ , \ na + nb = n(a + b) \ , \ a^n \times a^p = a^{n+p}.$$

Pour résumer, les règles de calcul de l'algèbre sont encore licites, mais si l'anneau n'est pas commutatif, alors $a \times b \neq b \times a$.

Pour a inversible et $p \in \mathbb{Z}$, alors $(a^p)^{-1} = \left(a^{-1}\right)^p$
Preuve. On le prouve pour $p \in \mathbb{N}$ par récurrence sur p. C'est clair si $p = 0$ ou 1. Supposons le vrai pour $p \geq 1$, alors

$$\left(a^{-1}\right)^{p+1} = \left(a^{-1}\right)^p \times a^{-1} = (a^p)^{-1} \times a^{-1}$$

et

$$\left(a^{p+1}\right)^{-1} = (a \times a^p)^{-1} = (a^p)^{-1} \times a^{-1}$$

Puis pour $p < 0$, on a $(a^p)^{-1} = \left(\left(a^{-1}\right)^{-p}\right)^{-1} \underset{-p>0}{=} \left((a^{-p})^{-1}\right)^{-1} = a^{-p}$ alors que $\left(a^{-1}\right)^p = \left(\left(a^{-1}\right)^{-1}\right)^{-p} = a^{-p}$, ce qui est bien la même chose. ■

1.3.2 Elements commutants

On notera pour simplifier le produit $a \times b$ sous la forme ab.

Définition 7 *Soient a et b dans A, on dit que a et b commutent si $ab = ba$.*

Cette notion est essentielle. Par exemple, pour le produit des matrices carrées, en général $AB \neq BA$. Le produit n'est donc pas commutatif !

Proposition 8 *Si a et b commutent alors $\forall (i, j) \in \mathbb{Z}^2$, a^i et b^j commutent.*

Preuve. *On commence par prouver que a^i et b^j commutent lorsque i et j sont dans $\mathbb{N}$. On définit la proposition $\mathcal{P}(j) =$ "$ab^j = b^j a$". La proposition est vraie au rang 0 car $b^0 = e$, élément neutre de A et $ae = ea = a$. Supposons que $\mathcal{P}(j)$ soit vrai pour $j \geq 0$ fixé. Alors*

$$ab^{j+1} = ab^j \times b \underset{HR_i}{=} \left(b^j a\right) \times b \underset{associativité}{=} b^j \times (ab) \underset{ab=ba}{=} b^j \times (ba) = b^{j+1} a$$

Ainsi $\mathcal{P}(j+1)$ est vraie. On a donc montré que, si a et b commutent, alors pour tout $j \in \mathbb{N}$, $ab^j = b^j a$. On en déduit que b^j et a commutent. On applique le résultat précédent à b^j et à a, ainsi pour tout $i \in \mathbb{N}$, $b^j a^i = a^i b^j$.
Il reste à montrer que c'est vrai pour i et j dans $\mathbb{Z}$. On montre d'abord que a^{-1} et b commutent. En effet

$$\begin{aligned} ab &= ba \Longrightarrow a^{-1}(ab)\, a^{-1} = a^{-1}(ba)\, a^{-1} \Longrightarrow \left(a^{-1}a\right)\left(ba^{-1}\right) = \left(a^{-1}b\right)\left(aa^{-1}\right) \Longrightarrow ba^{-1} = a^{-1}b \\ \text{car } aa^{-1} &= a^{-1}a = e, \text{ élément neutre de } A \end{aligned}$$

Par symétrie des rôles on a a *et* b^{-1} *qui commutent. On a donc montré que* a *et* b *commutent* $\Longrightarrow$ a *et* b^{-1} *commutent et* a^{-1} *et* b *commutent. On l'applique donc à* a *et* b^{-1} *pour avoir* a^{-1} *et* b^{-1} *commutent.*
Enfin, si $i \in \mathbb{Z}$, $i < 0$ *et* $j \in \mathbb{N}$, *alors* $a^i b^j = \left(a^{-1}\right)^{-i} b^j = b^j \left(a^{-1}\right)^{-i} = b^j a^i$ *car* a^{-1} *et* b *commutent.*
Si $i \in \mathbb{N}$ *et* $j \in \mathbb{Z}$, $j < 0$, *on échange les rôles de* a *et* b *pour avoir le même résultat.*
Si $(i,j) \in \mathbb{Z}^2$, $i < 0$ *et* $j < 0$, $a^i b^j = \left(a^{-1}\right)^{-i} \left(b^{-1}\right)^{-j} = \left(b^{-1}\right)^{-j} \left(a^{-1}\right)^{-i} = b^j a^i$ *car* a^{-1} *et* b^{-1} *commutent.* ■

1.3.3 Deux formules essentielles

On notera pour simplifier le produit $a \times b$ sous la forme ab.
Si a et b commutent alors pour tout $n \in \mathbb{N}$

$$\begin{aligned}(a+b)^n &= \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \text{ (formule du binôme)}\\ a^n - b^n &= (a-b)\sum_{k=0}^{n-1} a^{n-1-k}b^k = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} = (a-b)\left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\right)\end{aligned}$$

En particulier

$$a^2 - b^2 = (a-b)(a+b) \qquad a^3 - b^3 = (a-b)\left(a^2 + ab + b^2\right) \qquad \heartsuit$$

Remarque : Si a et b ne commutent pas, alors $(a+b)^2 = (a+b)\times(a+b) = a^2 + a\times b + b\times a + b^2 \neq a^2 + 2a\times b + b^2$.

Preuve. La formule du binôme se démontre par récurrence sur n. Soit $\mathcal{P}(n) = "(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}"$.

La propriété est vraie au rang 0, en effet

$$\begin{aligned}(a+b)^0 &= e\\ \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k} &= \binom{0}{0} a^0 b^0 = 1 \times e \times e = e \text{ car } \binom{0}{0} = 1\end{aligned}$$

On suppose que $\mathcal{P}(n)$ est vraie au rang $n \geq 0$ fixé. Alors

$$\begin{aligned}(a+b)^{n+1} &= (a+b)\times(a+b)^n = (a+b)\times\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}\\ &= a\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} + b\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} = \sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} + \sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k}\\ \text{car } b\left(a^k b^{n-k}\right) &= a^k b \times b^{n-k} = a^k b^{n+1-k} \text{ (a et b commutent !).}\end{aligned}$$

Dans la somme $\sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k}$ on pose $j = k+1$, alors $0 \leq k \leq n \Longrightarrow 1 \leq j \leq n+1$ et $n - k = n - (j-1) = n + 1 - j$ d'où

$$\sum_{k=0}^{n}\binom{n}{k}a^{k+1}b^{n-k} = \sum_{j=1}^{n+1}\binom{n}{j-1}a^j b^{n+1-j} = \binom{n}{n}a^{n+1}b^{n+1-0} + \left[\sum_{j=1}^{n}\binom{n}{j-1}a^j b^{n+1-j}\right]$$

Et l'on a également (on pose $j = k$)

$$\sum_{k=0}^{n}\binom{n}{k}a^k b^{n+1-k} = \sum_{j=0}^{n}\binom{n}{j}a^j b^{n+1-j} = \left[\sum_{j=1}^{n}\binom{n}{j}a^j b^{n+1-j}\right] + \binom{n}{0}a^0 b^{n+1-0}$$

Ce qui donne

$$\begin{aligned}(a+b)^{n+1} &= \binom{n}{n}a^{n+1}b^{n+1-0}+\left[\sum_{j=1}^{n}\binom{n}{j-1}a^j b^{n+1-j}+\sum_{j=1}^{n}\binom{n}{j}a^j b^{n+1-j}\right]+\binom{n}{0}a^0 b^{n+1-0}\\ &= \binom{n}{n}a^{n+1}b^{n+1-0}+\left[\sum_{j=1}^{n}\left[\binom{n}{j-1}+\binom{n}{j}\right]a^j b^{n+1-j}\right]+\binom{n}{0}a^0 b^{n+1-0}\end{aligned}$$

Mais d'après la relation de Pascal,

$$\binom{n}{j-1}+\binom{n}{j}=\binom{n+1}{j},\ \text{et}\ \binom{n}{n}=1=\binom{n+1}{n+1}\ ,\ \binom{n}{0}=1=\binom{n+1}{0}.$$

Bref, tout cela donne

$$\begin{aligned}(a+b)^{n+1} &= \binom{n+1}{n+1}a^{n+1}b^{n+1-0}+\left[\sum_{j=1}^{n}\binom{n+1}{j}a^j b^{n+1-j}\right]+\binom{n+1}{0}a^0 b^{n+1-0}\\ &= \sum_{j=0}^{n+1}\binom{n+1}{j}a^j b^{n+1-j}\end{aligned}$$

ce qui prouve l'hérédité et démontre la formule du binôme.
Pour la seconde relation, on a

$$\begin{aligned}(a-b)\sum_{k=0}^{n-1}a^{n-1-k}b^k &= a\sum_{k=0}^{n-1}a^{n-1-k}b^k-b\sum_{k=0}^{n-1}a^{n-1-k}b^k=\sum_{k=0}^{n-1}a^{n-k}b^k-\sum_{k=0}^{n-1}a^{n-1-k}b^{k+1}\\ \text{car}\ \left(ba^{n-1}\right)b^k &= \left(a^{n-1}b\right)b^k\end{aligned}$$

Dans la seconde somme on pose $j=k+1$, ainsi $\sum_{k=0}^{n-1}a^{n-1-k}b^{k+1}=\sum_{j=1}^{n}a^{n-j}b^j$. Par conséquent

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

Enfin

$$\sum_{k=0}^{n-1}a^{n-1-k}b^k=\sum_{j=0}^{n-1}a^j b^{n-1-j}\ \text{en posant}\ j=n-1-k$$

■

2 Corps

2.1 Définition

Définition 9 *Soit $(A,+,\times)$ un anneau d'éléments neutres 0 et 1. On dit que A est un corps si :*

- *La loi $\times$ est commutative.*
- *Tous les éléments de A sauf 0 sont inversibles pour la loi $\times$.*

Remarque 1 : Soit $x\in A$, alors x^{-1} (qui désigne l'inverse pour la loi $\times$, l'inverse pour la loi $+$ étant noté $-x$) est alors différent de 0. En effet, si $x^{-1}=0$ alors $0=x\times 0=x\times x^{-1}=1$.

Remarque 2 : Il revient au même de dire que $(A,+,\times)$ et $(A,+,\times)$ sont des groupes commutatifs tels que la multiplication soit distributive sur l'addition (TLM1, page 465).

Exemple 10 (1) $\mathbb{R}$ *et* $\mathbb{C}$*, munis de l'addition et de la multiplication usuelles sont des corps.*
(2) $\mathbb{R}(X)$*, l'ensemble des fractions rationnelles à coefficients réels est un corps.*

2.2 Sous-corps

Définition 11 *Soit* $(K,+,\times)$ *un corps et* $L \subset K$ *une partie de* K, *on dit que* L *est un sous-corps de* K *si :*

- $(L,+,\times)$ *est un sous-anneau de* $(K,+,\times)$.
- *Tous les éléments de* L *sauf* 0 *sont inversibles pour la loi* $\times$. *(c'est-à-dire* L *est un corps)*

Exemple 12 (1) $\mathbb{Q}$ *est un sous-corps de* $\mathbb{R}$.

(2) $\mathbb{Q}\left[\sqrt{2}\right] = \left\{a+b\sqrt{2},\ (a,b)\in\mathbb{Q}\right\}$ *est un sous-corps de* $\mathbb{Q}$.

Exercices

Exercice 1 On définit l'ensemble $A = \mathbb{Z}\left[\sqrt{2}\right] = \left\{x\in\mathbb{R},\ \exists\,(a,b)\in\mathbb{Z},\ x = a+b\sqrt{2}\right\}$.

1) Montrer que tout élément x de A s'écrit de manière unique $x = a+b\sqrt{2}$ avec a et b dans $\mathbb{Z}$.
2) Montrer que A est un sous anneau de $(\mathbb{R},+,\times)$.
3) Si $x = a+b\sqrt{2}$, on définit $N(x) = a^2-2b^2$. Vérifier que $N(xy) = N(x)\,N(y)$.
4) Montrer que $x\in A$ est inversible si et seulement si $N(x) = \pm 1$.
5) Vérifier que pour tout $n\in\mathbb{N}$, $u = \pm\left(1\pm\sqrt{2}\right)^n$ est inversible dans A.
6) Que dire de u si $n\in\mathbb{Z}$?.

Exercice 2 (Les entiers de Gauss). On note $\mathbb{Z}[i] = \left\{a+ib,\ (a,b)\in\mathbb{C}^2\right\}$.

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

Exercice 3 On note $\mathbb{R}^{\mathbb{N}}$ l'ensemble des suites réelles. On sait (exemple) que $\left(\mathbb{R}^{\mathbb{N}},+,\times\right)$ est un anneau commutatif. En utilisant les suites $u = (u_n)_{n\in\mathbb{N}}$ et $v = (v_n)_{n\in\mathbb{N}}$ définies par $u_n = 1+(-1)^n$ et $v_n = 1-(-1)^n$, vérifier que $\left(\mathbb{R}^{\mathbb{N}},+,\times\right)$ n'est pas intègre.

Exercice 4 On note toujours $\mathbb{R}^{\mathbb{N}}$ l'ensemble des suites réelles.

Pour $u = (u_n)_{n\in\mathbb{N}}$ et $v = (v_n)_{n\in\mathbb{N}}$, on pose $w = u*v = (w_n)_{n\in\mathbb{N}}$ où $w_n = \sum_{k=0}^{n} u_k v_{n-k}$.

1) Montrer que $\left(\mathbb{R}^{\mathbb{N}},+,*\right)$ est un anneau commutatif.
2) On note θ la suite nulle. Si u et v sont deux suites différentes de θ, on pose

$$\begin{aligned} p &= \min\{n\in\mathbb{N},\ u_n\neq 0\} \text{ le premier indice pour lequel } u_n\neq 0,\\ q &= \min\{n\in\mathbb{N},\ v_n\neq 0\},\\ w &= u*v. \end{aligned}$$

Que peut-on dire de w_{p+q} ? En déduire que $\left(\mathbb{R}^{\mathbb{N}},+,*\right)$ est intègre.

3) $\left(\mathbb{R}^{\mathbb{N}},+,*\right)$ est-il un corps ?

Exercice 5 Soit $(A,+,\times)$ un *anneau intègre* ayant un nombre *fini* d'éléments $a_1, a_2, a_3, \cdots, a_n$, avec $a_1 = 0$ (élement neutre pour l'addition) et $a_2 = 1$ (élement neutre pour la multiplication). Démontrer que A est un corps.

Solutions des exercices

Exercice 1 1) Soit $x\in A$, supposons que x s'écrive de deux manières, $x = a+b\sqrt{2} = a'+b'\sqrt{2}$ où $(a,a',b,b')\in\mathbb{Z}^4$. Si $b\neq b'$, par différence, on obtient $\sqrt{2} = \dfrac{a-a'}{b'-b}\in\mathbb{Q}$. Or on sait que $\sqrt{2}\notin\mathbb{Q}$ (exemple 28.14 de TLM1, page 349). ainsi $b = b'$ et $a = a'$.

2) L'élément 1 s'écrit bien $1 = 1+0\times\sqrt{2}$ donc $1 \in A$. On sait déjà que $A \neq \varnothing$, montrons que $(A,+)$ est un sous groupe de $(\mathbb{R},+)$. Si $x = a+b\sqrt{2}$ et $y = c+d\sqrt{2}$ où $(a,b,c,d) \in \mathbb{Z}^4$, alors $x-y = (a-c)+(b-d)\sqrt{2} \in A$ car $a-c$ et $b-d$ sont dans $\mathbb{Z}$.

Pour avoir un sous anneau, il suffit de montrer que $x \times y$ est dans A. Mais $x \times y = ac + 2bd + \sqrt{2}(ad+bc) \in A$ car $ac+2bd$ et $ad+bc$ sont dans $\mathbb{Z}$.

3) Avec les notations qui précèdent, on a $N(x)N(y) = \left(a^2-2b^2\right)\left(c^2-2d^2\right)$ et $N(x\times y) = (ac+2bd)^2 - 2(ad+bc)^2$. En développant les deux termes, on a bien le même résultat. En fait, on peut aussi remarquer que si l'on introduit $\overline{x} = a-b\sqrt{2}$, on a $N(x) = x\overline{x}$, d'où

$$N(x)N(y) = x\overline{x}y\overline{y} = (xy)(\overline{xy})$$

on vérifie alors que $\overline{xy} = \overline{(xy)}$ ce qui est simple si l'on "voit" que l'on passe de x à $\overline{x}$ en remplaçant $\sqrt{2}$ par $-\sqrt{2}$. Cela doit faire penser à la conjugaison dans $\mathbb{C}$ qui consiste à remplacer i par $-i$.

4) Montrons les deux implications. Supposons x inversible, il existe $y \in A$ tel que $x\times y = 1$, ainsi $N(xy) = N(x)N(y) = N(1) = 1$. On remarque ensuite que $N(x)$ et $N(y)$ sont des entiers. Leur produit vaut 1, donc ils valent 1 ou -1. Conclusion $N(x) = \pm 1$.

Réciproquement, si $N(x) = \pm 1$, alors $x\times\overline{x} = \pm 1$ et ainsi $\overline{x}$ ou $-\overline{x}$ (selon que $N(x) = 1$ ou -1) est l'inverse de x. Remarquons, pour finir, que l'inverse de x, qui est non nul, est bien $\dfrac{1}{x}$ car A est un sous anneau de $\mathbb{R}$.

5) Puisque $N(x\times y) = N(x)N(y)$, une récurrence simple montre que $N(x)^n = N(x^n)$. On a donc

$$N(u) = N(\pm 1)\,N\left(1\pm\sqrt{2}\right)^n = (\pm 1)^2 \times \left(1^2 - 2(\pm 1)^2\right)^n = (-1)^n = \pm 1$$

On en déduit que u est inversible.

6) Si $n \in \mathbb{Z}$, $n < 0$, alors $-n \in \mathbb{N}$ et $v = \pm\left(1\pm\sqrt{2}\right)^{-n}$ est inversible dans A. Mais alors, son inverse est $\dfrac{1}{v} = u$ est aussi inversible. Le résultat demeure donc si $n \in \mathbb{Z}$.

En application, cela donne des solutions à l'équation diophantienne (TLM1 page 346) $a^2 - 2b^2 = \pm 1$. Par exemple $\left(1+\sqrt{2}\right)^3 = 7+5\sqrt{2}$ a pour norme ± 1 car il est inversible. On vérifie, qu'en effet $7^2 - 2\times 5^2 = -1$.

Exercice 2 1) On vérifie que $1 = 1+0\times i \in \mathbb{Z}[i]$, puis que si $u = a+ib$ et $v = c+id$ avec $(a,b,c,d) \in \mathbb{Z}^4$, on a

$$\begin{aligned} u-v &= (a-c)+i(b-d) \in \mathbb{Z}[i] \text{ car } (a-c) \text{ et } (c-d) \text{ sont dans } \mathbb{Z} \\ u\times v &= (ac-bd)+i(ad+bc) \in \mathbb{Z}[i] \text{ car } (ac-bd) \text{ et } (ad+bc) \text{ sont dans } \mathbb{Z} \end{aligned}$$

Ceci prouve que $\mathbb{Z}[i]$ est un sous anneau de C.

2) Si $z = a+ib \neq 0 \in \mathbb{Z}[i]$ est inversible, son inverse est le même que dans $\mathbb{C}$. Ainsi

$$\frac{1}{z} = \frac{1}{a+ib} \in \mathbb{Z}[i].$$

Puisque $\dfrac{1}{a+ib} = \dfrac{a-ib}{a^2+b^2} = \dfrac{a}{a^2+b^2} - i\dfrac{b}{a^2+b^2} \in \mathbb{Z}[i]$, il vient $\dfrac{a}{a^2+b^2} \in \mathbb{Z}$ et $\dfrac{b}{a^2+b^2} \in \mathbb{Z}$.

Par multiplication de $\dfrac{a}{a^2+b^2}$ par $b \in \mathbb{Z}$, on en déduit que $\dfrac{ab}{a^2+b^2} \in \mathbb{Z}$. Or on a les inégalités

$$\begin{aligned} (a-b)^2 &\geq 0 \Longleftrightarrow 2ab \leq a^2+b^2 \Longleftrightarrow \frac{ab}{a^2+b^2} \leq \frac{1}{2}, \\ (a+b)^2 &\geq 0 \Longleftrightarrow -2ab \leq a^2+b^2 \Longleftrightarrow \frac{ab}{a^2+b^2} \geq -\frac{1}{2}. \end{aligned}$$

On a donc $-\dfrac{1}{2} \leq \dfrac{ab}{a^2+b^2} \leq \dfrac{1}{2}$ et $\dfrac{ab}{a^2+b^2} \in \mathbb{Z}$. Cela impose $\dfrac{ab}{a^2+b^2} = 0$ et ainsi $a = 0$ ou $b = 0$.

Pour finir, si $a = 0$, on a $\dfrac{b}{a^2+b^2} = \dfrac{1}{b} \in \mathbb{Z}$ d'où $b = \pm 1$. De même si $b = 0$, $\dfrac{a}{a^2+b^2} = \dfrac{1}{a} \in \mathbb{Z}$ d'où $a = \pm 1$.

Conclusion, les seuls éléments inversibles de $\mathbb{Z}[i]$ sont $1, -1, i$ et $-i$.

Exercice 3 Il est clair que $u \neq 0$ (suite nulle) car $u_{2p} = 2$ pour tout entier naturel p. Cependant, pour tout $n \in \mathbb{N}$,

$$u_n v_n = \left(1 + (-1)^n\right)\left(1 - (-1)^n\right) = 1 - \left((-1)^n\right)^2 = 1 - (-1)^{2n} = 1 - 1 = 0.$$

Ainsi, $u \times v = 0$. Ceci prouve que $\left(\mathbb{R}^{\mathbb{N}}, +, \times\right)$ n'est pas intègre.

Exercice 4 1) On sait déjà que $(\mathbb{R}^{\mathbb{N}}, +)$ est un groupe commutatif. Pour montrer que la loi $*$ est associative, observons que le terme d'indice n de la suite $u * v$ est le coefficient de x^n dans le produit $P(x)Q(x)$ des polynômes

$$P(x) = \sum_{k=0}^{n} u_k x^k \text{ et } Q(x) = \sum_{k=0}^{n} v_k x^k.$$

L'associativité de $*$ résulte donc de l'associativité du produit des polynômes, et la commutativité de $*$ résulte de la commutativité du produit des polynômes. L'élément neutre est clairement la suite $e = (e_n)_{n\in\mathbb{N}}$ associée au polynôme $E(x) = 1$, c'est-à-dire $e_0 = 1$, $e_n = 0$ pour $n \geq 1$. Ainsi $(\mathbb{R}^{\mathbb{N}}, +, *)$ est un anneau commutatif.

2) On a d'abord

$$w_{p+q} = \sum_{k=0}^{p+q} u_k v_{p+q-k} = \sum_{k=p}^{p+q} u_k v_{p+q-k}$$

car $u_k = 0$ si $k < p$. Par ailleurs $v_{p+q-k} = 0$ si $p + q - k < q$, c'est-à-dire si $k > p$. Il en résulte que

$$w_{p+q} = \sum_{k=p}^{p} u_k v_{p+q-k} = u_p v_q \neq 0.$$

Ceci prouve que, si $u \neq \theta$ et $v \neq \theta$, alors $u * v \neq \theta$, c'est-à-dire que $(\mathbb{R}^{\mathbb{N}}, +, *)$ est intègre.

3) Le calcul précédent montre que $(\mathbb{R}^{\mathbb{N}}, +, *)$ n'est pas un corps. En effet, si $u \neq \theta$ est donné, cherchons v tel que $u * v = e$. Nécessairement, $v \neq 0$ si une telle suite existe. Avec les notations précédentes, $u * v = e$ signifie que $w_{p+q} = u_p v_q = 1$ si $p + q = 0$ (c'est-à-dire si $p = q = 0$) et $w_{p+q} = u_p v_q = 0$ si $p + q \geq 1$. Cette condition est réalisée dès lors que $p \geq 1$, et cela implique que $p = 0$ (car $u_p \neq 0$ et $v_q \neq 0$). Ainsi on doit avoir $u_0 \neq 0$, ce qui prouve que $u = (u_n)_{n\in\mathbb{N}}$ n'est pas inversible si $u_0 = 0$.

Exercice 5 Il s'agit de démontrer que tout élément non nul de A admet un inverse pour la multiplication. Soit donc $a_i \neq 0$, avec $i \geq 2$. Considérons les éléments de A définis par

$$b_1 = a_i \times a_1,\ b_2 = a_i \times a_2,\ b_3 = a_i \times a_3,\ \cdots,\ b_n = a_i \times a_n.$$

Ces éléments sont deux à deux distincts. En effet

$$b_j = b_k \Rightarrow a_i \times a_j = a_i \times a_k \Rightarrow a_i \times a_j - a_i \times a_k = 0 \Rightarrow a_i \times (a_j - a_k) = 0 \Rightarrow a_j - a_k = 0 \Rightarrow a_j = a_k$$

car $a_i \neq 0$ et A est *intègre*. Les b_j sont donc exactement n éléments de A, deux à deux distincts. Puisque $\operatorname{card} A = n$, il existe un indice j tel que $b_j = 1$, c'est-à-dire $a_i \times a_j = 1$. Ainsi a_j admet un inverse dans A, et A est bien un corps. Nous avons prouvé que *tout anneau intègre fini est un corps.*

© http ://touteslesmaths.fr