21

Structure d'anneau

21.1 Anneaux

Définition 21.1 *Soit A un ensemble non vide muni de deux lois de composition interne notées $+$ (une addition) et $\cdot$ (une multiplication). On dit que $(A,+,\cdot)$ est un anneau si :*
- *$(A,+)$ est un groupe commutatif ;*
- *la loi $\cdot$ est associative ;*
- *la loi $\cdot$ est distributive par rapport à la loi $+$, ce qui signifie que :*

$$\forall\,(a,b,c)\in A^3,\ \begin{cases} a\cdot(b+c)=a\cdot b+a\cdot c \\ (b+c)\cdot a=b\cdot a+b\cdot c \end{cases}$$

Si la loi $\cdot$ est commutative, on dit alors que l'anneau A est unitaire.
S'il existe un élément neutre pour la loi $\cdot$, on dira alors que A est un anneau unitaire.

Si $(A,+,\cdot)$ est un anneau, on notera 0 le neutre pour l'addition et s'il existe on notera 1 le neutre pour la multiplication. L'opposé d'un élément a (i. e. le symétrique pour $+$) sera noté $-a$ et on notera $a-b$ pour $a+(-b)$.

On écrira souvent ab pour $a\cdot b$ dans un anneau.

Dans un anneau unitaire, on supposera que $0\neq 1$ (sans quoi l'anneau est réduit à $\{0\}$). Un anneau unitaire a donc au moins deux éléments.

Exemple 21.1 *Les ensembles $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ muni des opérations usuelles sont des anneaux commutatifs et unitaires.*

Exemple 21.2 *Soient E un ensemble non vide et A un anneau. On vérifie facilement que l'ensemble A^E des applications de E dans A muni des opérations d'addition et de multiplication définies par :*

$$\forall\,(f,g)\in A^E\times A^E,\ \forall x\in E,\ \begin{cases} (f+g)(x)=f(x)+g(x) \\ (f\cdot g)(x)=f(x)\cdot g(x) \end{cases}$$

est un anneau. Cet anneau est commutatif si A l'est et il est unitaire si A l'est avec comme élément neutre pour le produit l'application constante égale à 1.
En particulier l'ensemble $\mathbb{R}^{\mathbb{N}}$ des suites réelles est un anneau commutatif unitaire et pour toute partie non vide I de R, l'ensemble R^I des fonctions définies sur I et à valeurs réelles est un anneau commutatif unitaire.

Exemple 21.3 *L'ensemble $\mathcal{M}_n(\mathbb{R})$ [resp. $\mathcal{M}_n(\mathbb{C})$] des matrices carrées réelles [resp. complexes] d'ordre $n \geq 1$ muni des opérations usuelles d'addition et de multiplication est un anneau unitaire non commutatif.*

Exemple 21.4 *Plus généralement si A est un anneau commutatif unitaire, l'ensemble $\mathcal{M}_n(A)$ des matrices carrées d'ordre n à coefficients dans A est un anneau unitaire non commutatif pour les opérations d'addition et multiplication définies par :*

$$\begin{cases} M + M' = \left(\left(m_{ij} + m'_{ij}\right)\right)_{1\leq i,j\leq n} \\ MM' = \left(\left(\sum_{k=1}^{n} m_{ik}m'_{kj}\right)\right)_{1\leq i,j\leq n} \end{cases}$$

où on note $M = ((m_{ij}))_{1\leq i,j\leq n}$ la matrice ayant pour coefficient m_{ij} en ligne i et colonne j pour i, j compris entre 1 et n.
On peut aussi définir, pour $\lambda \in A$ et $M = ((m_{ij}))_{1\leq i,j\leq n} \in \mathcal{M}_n(A)$, la matrice λM par $\lambda M = ((\lambda m_{ij}))_{1\leq i,j\leq n}$.

Exercice 21.1 *Soit A un anneau commutatif unitaire. Pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ dans $\mathcal{M}_2(A)$, on définit le déterminant et la trace de M respectivement par :*

$$\det(M) = ad - bc\,;\ \mathrm{Tr}(M) = a + d$$

1. *Vérifier que, pour toutes matrices M, M' dans $\mathcal{M}_2(A)$, on a $\det(MM') = \det(M)\det(M')$.*
2. *Pour $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_2(A)$, on définit la comatrice (en fait la transposée de la comatrice) de M par $\widetilde{M} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.*
   (a) *Calculer $M\widetilde{M}$.*
   (b) *Montrer que $M^2 - \mathrm{Tr}(M)\,M + \det(M)\,I_2 = 0$, où $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.*

Solution 21.1

1. *On a :*
$$MM' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$$
et :
$$\begin{aligned} \det(MM') &= (aa' + bc')(cb' + dd') - (ca' + dc')(ab' + bd') \\ &= bcb'c' - adb'c' + ada'd' - bca'd' \\ &= ad(a'd' - b'c') + bc(b'c' - a'd') \\ &= (ad - bc)(a'd' - b'c') \\ &= \det(M)\det(M') \end{aligned}$$
(l'anneau A est commutatif)
2.

(a) On a :

$$\begin{aligned} M\widetilde{M} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \\ &= \det(M)\, I_2 \end{aligned}$$

(b) On a :

$$\begin{aligned} M^2 - \operatorname{Tr}(M)\, M + \det(M)\, I_2 &= M^2 - \operatorname{Tr}(M)\, M \cdot I_2 + M \cdot \widetilde{M} \\ &= M\left(M - \operatorname{Tr}(M)\, I_2 + \widetilde{M}\right) \end{aligned}$$

avec :

$$\begin{aligned} M - \operatorname{Tr}(M)\, I_2 &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} a+d & 0 \\ 0 & a+d \end{pmatrix} \\ &= \begin{pmatrix} -d & b \\ c & -a \end{pmatrix} = -\widetilde{M} \end{aligned}$$

ce qui donne :

$$M^2 - \operatorname{Tr}(M)\, M + \det(M)\, I_2 = 0.$$

Exercice 21.2 *Soit E un ensemble non vide. Montrer que l'ensemble $\mathcal{P}(E)$ des parties de E muni des opérations Δ de différence symétrique et $\cap$ d'intersection est un anneau commutatif et unitaire (c'est l'anneau de Boole).*

Solution 21.2 *On rappelle que pour A, B dans $\mathcal{P}(E)$, on a :*

$$A\Delta B = (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A),$$

la réunion étant disjointe.
De la commutativité des opérateurs $\cup$ et $\cap$, on déduit que Δ est commutative.
Pour A, B, C dans $\mathcal{P}(E)$, on a :

$$\begin{aligned} (x \in (A\Delta B)\,\Delta C) &\Leftrightarrow (x \in A\Delta B \text{ et } x \notin C) \text{ ou } (x \in C \text{ et } x \notin A\Delta B) \\ &\Leftrightarrow (x \in A \text{ et } x \notin B \text{ et } x \notin C) \text{ ou } (x \in B \text{ et } x \notin A \text{ et } x \notin C) \\ &\text{ou } (x \in C \text{ et } x \notin A \text{ et } x \notin B) \text{ ou } (x \in C \text{ et } x \in A \cap B) \\ &\Leftrightarrow (x \in A \text{ et } x \notin B \text{ et } x \notin C) \text{ ou } (x \in B \text{ et } x \notin A \text{ et } x \notin C) \\ &\text{ou } (x \in C \text{ et } x \notin A \text{ et } x \notin B) \text{ ou } (x \in A \cap B \cap C) \end{aligned}$$

et :

$$\begin{aligned} (x \in A\Delta(B\Delta C)) &\Leftrightarrow (x \in A \text{ et } x \notin B\Delta C) \text{ ou } (x \in B\Delta C \text{ et } x \notin A) \\ &\Leftrightarrow (x \in A \text{ et } x \notin B \text{ et } x \notin C) \text{ ou } (x \in A \text{ et } x \in B \cap C) \\ &\text{ou } (x \in B \text{ et } x \notin C \text{ et } x \notin A) \text{ ou } (x \in C \text{ et } x \notin B \text{ et } x \notin A) \\ &\Leftrightarrow (x \in A \text{ et } x \notin B \text{ et } x \notin C) \text{ ou } (x \in A \cap B \cap C) \\ &\text{ou } (x \in B \text{ et } x \notin C \text{ et } x \notin A) \text{ ou } (x \in C \text{ et } x \notin B \text{ et } x \notin A) \end{aligned}$$

D'où l'égalité $(A\Delta B)\,\Delta C = A\Delta(B\Delta C)$.
L'ensemble vide est le neutre pour Δ et pour tout $A \in \mathcal{P}(E)$, on a :

$$A\Delta A = (A \cup A) \setminus (A \cap A) = A \setminus A = \emptyset,$$

c'est-à-dire que A est l'opposé de A pour la loi Δ (tous les éléments de $\mathcal{P}(E)\setminus\{\emptyset\}$ sont d'ordre 2, ce qui permet de retrouver la commutativité de $(\mathcal{P}(E),\Delta)$ et le fait que $\mathcal{P}(E)$ est de cardinal une puissance de 2 si E est fini).
En définitive, $(\mathcal{P}(E),\Delta)$ est un groupe commutatif.
On vérifie facilement que $\cap$ est commutative et associative. L'ensemble E est le neutre pour $\cap$. Pour A,B,C dans $\mathcal{P}(E)$, on a :

$$\begin{aligned}(x\in A\cap(B\Delta C)) &\Leftrightarrow (x\in A \text{ et } x\in B\Delta C)\\ &\Leftrightarrow (x\in A \text{ et } x\in B \text{ et } x\notin C) \text{ ou } (x\in A \text{ et } x\in C \text{ et } x\notin B)\\ &\Leftrightarrow (x\in A\cap B \text{ et } x\notin C) \text{ ou } (x\in A\cap C \text{ et } x\notin B)\\ &\Leftrightarrow (x\in A\cap B \text{ et } x\notin A\cap C) \text{ ou } (x\in A\cap C \text{ et } x\notin A\cap B)\\ &\Leftrightarrow (x\in (A\cap B)\setminus(A\cap C)) \text{ ou } (x\in (A\cap C)\setminus(A\cap B))\\ &\Leftrightarrow x\in (A\cap B)\,\Delta\,(A\cap C)\end{aligned}$$

c'est-à-dire que $\cap$ est distributive par rapport à Δ.
En définitive, $(\mathcal{P}(E),\Delta,\cap)$ est un anneau commutatif et unitaire.

Exercice 21.3 *Soient A_1,A_2 deux anneaux. Montrer que le produit direct $A_1\times A_2$ muni des lois :*

$$\begin{cases}((a_1,a_2),(b_1,b_2))\mapsto (a_1,a_2)+(b_1,b_2)=(a_1+b_1,a_2+b_2)\\ ((a_1,a_2),(b_1,b_2))\mapsto (a_1,a_2)\cdot(b_1,b_2)=(a_1\cdot b_1,a_2\cdot b_2)\end{cases}$$

est un anneau.

Solution 21.3 *Laissée au lecteur.*

De manière plus générale, si $A_1,\cdots,A_p$ sont des anneaux, on peut alors munir le produit direct $\prod_{k=1}^{p}A_k=A_1\times\cdots\times A_p$ d'une structure d'anneau comme dans le cas où $p=2$. Si $A_k=A$ pour tout k compris entre 1 et p, on note alors A^p cet anneau produit.

Avec le théorème qui suit, on donne un résumé des règles de calculs utilisables dans un anneau.

Théorème 21.1 *Dans un anneau $(A,+,\cdot)$, on a les règles de calcul suivantes :*
- $a\cdot 0=0\cdot a=0$;
- $(-a)\cdot b=a\cdot(-b)=-a\cdot b$;
- $(-a)\cdot(-b)=a\cdot b$;
- $(a-b)\cdot c=a\cdot c-b\cdot c$;
- $a\cdot(b-c)=a\cdot b-a\cdot c$;
- $n(a\cdot b)=(na)\cdot b=a\cdot(nb)$;
- $a\cdot\left(\sum_{k=1}^{p}b_k\right)=\sum_{k=1}^{p}a\cdot b_k$;
- $\left(\sum_{k=1}^{p}b_k\right)\cdot a=\sum_{k=1}^{p}b_k\cdot a$;

où $a,b,c,a_1,\cdots,a_p$ sont des éléments de A, p un entier naturel non nul et n un entier relatif.

Démonstration.
- On a $a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$ et simplifiant par $a\cdot 0$ dans le groupe $(A,+)$, on en déduit que $a\cdot 0=0$.

- De $0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$, on déduit que $(-a) \cdot b = -a \cdot b$.
- On en déduit que $(-a) \cdot (-b) = -a \cdot (-b) = -(-a \cdot b) = a \cdot b$ (dans un groupe, l'opposé de l'opposé et l'élément).
- On en déduit aussi que $(a - b) \cdot c = a \cdot c + (-b) \cdot c = a \cdot c - b \cdot c$.
- On montre d'abord par récurrence sur $n \geq 0$ que $n(a \cdot b) = (na) \cdot b$. C'est vrai pour $n = 0$ et supposant que c'est vrai pour $n \geq 0$, on a :

$$\begin{aligned}(n+1)(a \cdot b) &= n(a \cdot b) + a \cdot b = (na) \cdot b + a \cdot b \\ &= (na + a) \cdot b = ((n+1)a) \cdot b\end{aligned}$$

  Ensuite avec $(-n)(a \cdot b) = -n(a \cdot b) = -(na) \cdot b = (-na) \cdot b$, on déduit que le résultat est valable pour les entiers relatifs.
- Les deux derniers résultats se montrent facilement par récurrence sur $p \geq 1$.

■

Sur $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, une formule intéressante est celle du binôme de Newton. Elle est en fait valable sur anneau unitaire quand les éléments commutent.

Théorème 21.2 *Soit $(A, +, \cdot)$ un anneau unitaire.*
Si a et b commutent dans A, on a alors pour tout entier naturel n :

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

(formule du binôme de Newton).

Démonstration. On procède par récurrence sur $n \geq 0$. Pour $n = 0$ et $n = 1$, c'est évident. En supposant le résultat acquis au rang $n \geq 1$, on a :

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

et tenant compte de $C_n^{k-1} + C_n^k = C_{n+1}^k$ (triangle de Pascal), cela s'écrit :

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

Le résultat est donc vrai pour tout $n \geq 0$. ■

Remarque 21.1 *Si a et b ne commutent pas, la formule du binôme n'est plus nécessairement vrai. Par exemple dans $\mathcal{M}_n(\mathbb{R})$ en considérant deux matrices A et B telles que $AB \neq BA$, on a :*

$$(A+B)^2 = A^2 + AB + BA + B^2 \neq A^2 + 2AB + B^2.$$

Par exemple, les matrices $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *et* $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *donnent :*

$$AB = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix},\ BA = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$

et pour $c \neq 0$, *on a* $AB \neq BA$.

Remarque 21.2 *La formule du binôme peut aussi se montrer en utilisant un argument de dénombrement. Comme* a *et* b *commutent,* $(a+b)^n = (a+b)\cdots(a+b)$, *le produit étant effectué* n *fois, est un somme de monomes* $a^k b^{n-k}$ *et, pour* k *fixé entre* 0 *et* n, *il y a autant de monomes* $a^k b^{n-k}$ *que de produits* $aabaa\cdots$ *où* a *intervient* k *fois et* b *intervient* $n-k$ *fois. Dans une telle liste, il y a* C_n^k *façons de choisir la position des* k *éléments* a *(les* a *étant placés, les* b *le sont automatiquement), ce qui donne la formule.*

L'identité remarquable qui suit, pour a et b qui commutent, est aussi intéressante.

Théorème 21.3 *Soit* $(A, +, \cdot)$ *un anneau unitaire.*
Si a *et* b *commutent dans* A, *on a alors pour tout entier naturel* n *:*

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

Démonstration. On procède par récurrence sur $n \geq 0$. Pour $n = 0$, c'est évident. En supposant le résultat acquis au rang $n \geq 0$, on a :

$$\begin{aligned} b^{n+2} - a^{n+2} &= \left(b^{n+1} - a^{n+1}\right) b + ba^{n+1} - a^{n+2} \\ &= (b-a)\sum_{k=0}^{n} a^k b^{n+1-k} + (b-a)\, a^{n+1} \\ &= (b-a)\left(b^{n+1} + ab^n + \cdots + a^{n-1}b^2 + a^n b\right) + (b-a)\, a^{n+1} \\ &= (b-a)\sum_{k=0}^{n+1} a^k b^{n+1-k}. \end{aligned}$$

Le résultat est donc vrai pour tout $n \geq 0$. ∎

Remarque 21.3 *Si* a *et* b *ne commutent pas, ce résultat n'est plus nécessairement vrai. Par exemple dans* $\mathcal{M}_n(\mathbb{R})$ *en considérant deux matrices* A *et* B *telles que* $AB \neq BA$, *on a :*

$$(B-A)(B+A) = B^2 - AB + BA - A^2 \neq B^2 - A^2.$$

Par exemple, les matrices $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *et* $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *donnent :*

$$AB = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix},\ BA = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix}$$

et pour $c \neq 0$, *on a* $AB \neq BA$.

21.2 Éléments inversibles dans un anneau unitaire

Pour ce paragraphe $(A,+,\cdot)$ est un anneau unitaire.

On note $A^\times$ l'ensemble des éléments de A inversibles pour la multiplication, c'est-à-dire l'ensemble des éléments $a \in A$ pour lesquels il existe un élément $a' \in A$ tel que $a \cdot a' = a' \cdot a = 1$. Quand il existe un tel inverse est unique et on le note a^{-1}.

Comme $1 \neq 0$ dans A, on a $A^\times \subset A \setminus \{0\}$ et cette inclusion peut être stricte.

Remarque 21.4 *L'exercice 20.7 nous dit que pour vérifier qu'un élément a de l'anneau unitaire A est inversible, il suffit de vérifier qu'il a un inverse à gauche (ou à droite) puisque la loi multiplicative est associative.*

Exemple 21.5 *On a $\mathbb{Z}^\times = \{-1,1\}$ et $\mathbb{R}[X]^\times = \mathbb{R}^*$ (ensemble des polynômes constants non nuls).*

Exemple 21.6 *On a $(\mathcal{M}_n(\mathbb{R}))^\times = GL_n(\mathbb{R})$ [resp. $(\mathcal{M}_n(\mathbb{C}))^\times = GL_n(\mathbb{G})$].*

Théorème 21.4 *Soit $(A,+,\cdot)$ un anneau unitaire. L'ensemble $A^\times$ des éléments inversibles de A est un groupe pour le produit.*

Démonstration. $A^\times$ est non vide puisqu'il contient 1.

Si a, b sont dans $A^\times$, on a alors :

$$b^{-1}a^{-1}ab = b^{-1}b = 1,\ abb^{-1}a^{-1} = aa^{-1} = 1,$$

c'est-à-dire que ab est inversible d'inverse $b^{-1}a^{-1}$. La multiplication définit donc une loi interne sur $A^\times$. On sait déjà que cette loi est associative, que 1 en est le neutre et tout $a \in A^\times$ est inversible par construction d'inverse $a^{-1} \in A^\times$ (on $(a^{-1})^{-1} = a$). $(A^\times,\cdot)$ est donc un groupe. ■

Définition 21.2 *On dit que $A^\times$ est le groupe des unités de A.*

Exercice 21.4 *Soit $(A,+,\cdot)$ un anneau unitaire. Montrer que si $a \in A$ est tel que $a^n = 0$ pour un entier $n \geq 1$ (on dit alors que a est nilpotent), alors $1-a$ est inversible d'inverse $\displaystyle\sum_{k=0}^{n-1} a^k$.*

Solution 21.4 *On a :*

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

pour $n \geq 1$ et $a^n = 0$ donne $(1-a)\displaystyle\sum_{k=0}^{n-1} a^k = 1$, ce qui signifie que $1-a$ est inversible d'inverse $\displaystyle\sum_{k=0}^{n-1} a^k$.

Exercice 21.5 *Soit $(A,+,\cdot)$ un anneau unitaire.*

1. *Montrer que si a, b sont deux éléments de A tels que $1-ab$ soit inversible d'inverse u, alors $1-ba$ est aussi inversible d'inverse $1 + b \cdot u \cdot a$.*
2. *En déduire que si A, B sont deux matrices réelles ou complexes, alors AB et BA ont les mêmes valeurs propres.*

Solution 21.5

1. *On a :*

$$\begin{aligned}(1-ba)(1+bua) &= 1-ba+bua-babua\\ &= 1+b(-1+u-abu)a\\ &= 1-b(-1+(1-ab)u)a\\ &= 1-b(-1+1)a=1\end{aligned}$$

puisque $(1-ab)u=1$ *(l'idée de cet in verse peut être inspirée par le calcul dans* $\mathbb{R}$ *:* $\dfrac{1}{1-ba}=1+\dfrac{ba}{1-ab}=1+bua$*).*

2. *Dire que* 0 *est valeur propre de* AB *équivaut à dire que* $\det(AB)=0$ *et comme* $\det(AB)=\det(BA)$*, celà équivaut à dire* 0 *est valeur propre de* BA*.*
Dire que $\lambda\neq 0$ *est valeur propre de* AB *équivaut à dire que* λI_n-AB *est non inversible, ce qui revient à dire que* $I_n-\dfrac{1}{\lambda}AB$ *est non inversible et cela équivaut à dire que* $I_n-\dfrac{1}{\lambda}BA$ *est non inversible, donc que* λ *est aussi valeur propre de* BA*.*

Remarque 21.5 *On peut en fait montrer que si* A,B *sont deux matrices réelles ou complexes, alors* AB *et* BA *ont le même polynôme caractéristique.*

Définition 21.3 *On dit que* $a\in A$ *est un diviseur de* 0 *si* $a\neq 0$ *et s'il existe* $b\neq 0$ *dans* A *tel que* $a\cdot b=0$*.*

Remarque 21.6 *Un diviseur de* 0 *dans un anneau unitaire n'est jamais inversible (pour la multiplication) et, par contraposée, un élément inversible ne peut être un diviseur de* 0*.*

Remarque 21.7 *Si* a *est un diviseur de* 0*, une égalité de la forme* $a\cdot b=a\cdot c$ *ne peut être simplifiée a priori. Un élément simplifiable pour le produit ne peut donc être un diviseur de* 0*.*

Définition 21.4 *Un anneau est dit intègre s'il est commutatif et n'admet pas de diviseur de* 0*.*

Dans un anneau intègre, on a :

$$a\cdot b=0\Leftrightarrow a=0 \text{ ou } b=0.$$

Exemple 21.7 *Dans un anneau de Boole* $(\mathcal{P}(E),\Delta,\cap)$*, on a pour toute partie* A *de* E *:*

$$A\cap(E\setminus A)=\emptyset$$

et donc tout $A\neq\emptyset$ *est un diviseur de* $\emptyset$ *(le* 0 *pour la loi* Δ*). Donc cet anneau n'est pas intègre.*

Exemple 21.8 *Les anneaux* $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ *sont intègres.*

Exemple 21.9 *L'anneau* $\mathbb{R}[X]$ *est intègre.*

Exemple 21.10 *L'anneau* $\mathcal{M}_n(\mathbb{R})$ *[resp.* $\mathcal{M}_n(\mathbb{C})$*] est non intègre puisque non commutatif. Sans se préoccuper de la commutativité, on peut trouver des diviseurs de* 0 *dans* $\mathcal{M}_n(\mathbb{R})$*. Par exemple, pour* $n=2$*, on a* $\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&0\\0&1\end{pmatrix}=0$ *et aucune de ces deux matrice n'est nulle.*

Exemple 21.11 *Soient* A_1,A_1 *deux anneaux. Dans l'anneau produit* $A_1\times A_2$*, on a* $(a_1,0)\cdot(0,a_2)=(0,0)$*, c'est-à-dire que pour* $a_1\neq 0$ *et* $a_2\neq 0$*,* $(a_1,0)$ *et* $(0,a_2)$ *sont des diviseurs de* 0*. Donc, pour* A_1 *et* A_2 *non réduits à* $\{0\}$*,* $A_1\times A_2$ *n'est jamais intègre.*

21.3 Sous-anneaux

Définition 21.5 *Soit $(A,+,\cdot)$ un anneau. Un sous-anneau de A est une partie non vide B de A telle que $(B,+)$ est un sous-groupe de A et B est stable pour la multiplication, c'est-à-dire que pour tous a,b dans B, $a\cdot b$ est aussi dans B.*
Si l'anneau A est unitaire, B doit contenir 1.

Il est facile de vérifier qu'un sous-anneau d'un anneau et lui même un anneau.

Théorème 21.5 *Soit $(A,+,\cdot)$ un anneau et B une partie non vide de A. B est un sous-anneau de A si, et seulement si :*

$$\forall\,(a,b)\in B^2,\ \begin{cases} a-b\in B \\ a\cdot b\in B \end{cases}$$

(pour A unitaire, il faut ajouter $1\in B$).

Démonstration. Laissée au lecteur. ∎

Exemple 21.12 *Les ensembles $\mathbb{Z},\mathbb{Q},\mathbb{R}$ muni des opérations usuelles sont des sous-anneaux de $\mathbb{C}$.*

Exemple 21.13 *Pour $\mathbb{K}=\mathbb{Q},\mathbb{R}$ ou $\mathbb{C}$, l'ensemble $\mathbb{K}[x]$ des fonctions polynomiales à coefficients dans $\mathbb{K}$, est un sous-anneau de $\mathbb{K}^{\mathbb{K}}$.*

Exercice 21.6 *On appelle nombre décimal tout nombre rationnel de la forme $\dfrac{a}{10^m}$ où a est un entier relatif et m un entier naturel.*

1. *Montrer que l'ensemble D des nombres décimaux est un anneau unitaire, commutatif et intègre.*
2. *Montrer que l'ensemble des nombres décimaux inversibles est :*

$$D^\times=\left\{r=\pm 2^\alpha 5^\beta \mid (\alpha,\beta)\in\mathbb{Z}^2\right\}.$$

Solution 21.6

1. *Facile.*
2. *Un rationnel $r=\dfrac{a}{10^m}$ est inversible dans $\mathbb{D}$ si, et seulement si, il existe un entier relatif b et un entier naturel n tels que $\dfrac{a}{10^m}\dfrac{b}{10^n}=1$, ce qui revient à dire que $ab=10^{n+m}$ ou encore que 2 et 5 sont les seuls diviseurs premiers possibles de a et b.*

Exercice 21.7 *Soit $p\geq 2$ un entier sans facteurs carrés dans sa décomposition en produit de nombres premiers (c'est-à-dire que $p=\prod_{k=1}^{r} p_k$ où les p_k sont premiers deux à deux distincts).*

1. *Montrer que l'ensemble :*

$$\mathbb{Z}\left[\sqrt{p}\right]=\left\{n+m\sqrt{p}\mid (n,m)\in\mathbb{Z}^2\right\}$$

est un sous anneau de $\mathbb{R}$.

2. *Montrer que $n+m\sqrt{p}=0$ dans $\mathbb{Z}\left[\sqrt{p}\right]$ si, et seulement si, $n=m=0$ (ce qui signifie que l'écriture $a=n+m\sqrt{p}$ d'un élément de $\mathbb{Z}\left[\sqrt{p}\right]$ est unique).*
3. *Quels sont les éléments de $\mathbb{Z}$ (qui est contenu dans $\mathbb{Z}\left[\sqrt{p}\right]$) qui sont inversibles.*

4. *Montrer que si* $n+m\sqrt{p}$ *est inversible dans* $\mathbb{Z}\left[\sqrt{p}\right]$, *il en est alors de même de* $n-m\sqrt{p}$.
5. *Montrer que le groupe des éléments inversibles de* $\mathbb{Z}\left[\sqrt{p}\right]$ *est :*

$$\left(\mathbb{Z}\left[\sqrt{p}\right]\right)^{\times}=\left\{n+m\sqrt{p}\in\mathbb{Z}\left[\sqrt{p}\right]\mid n^2-pm^2=\pm1\right\}$$

Solution 21.7

1. *On a* $1=1+0\sqrt{p}\in\mathbb{Z}\left[\sqrt{p}\right]$. *Pour* $a=n+m\sqrt{p}$ *et* $a'=n'+m'\sqrt{p}$ *dans* $\mathbb{Z}\left[\sqrt{p}\right]$, *on a :*

$$\begin{cases} a-a'=(n-n')+(m-m')\sqrt{p}\in\mathbb{Z}\left[\sqrt{p}\right] \\ aa'=(nn'+pmm')+(nm'+mn')\sqrt{p}\in\mathbb{Z}\left[\sqrt{p}\right] \end{cases}$$

   Donc $\mathbb{Z}\left[\sqrt{p}\right]$ *est un sous anneau de* $\mathbb{R}$.
2. *Si* $a=n+m\sqrt{p}=0$ *avec* $m\neq0$, *on a alors* $\sqrt{p}=-\dfrac{n}{m}\in\mathbb{Q}$, *ce qui n'est pas possible si* p *est sans facteurs carrés. En effet* $\sqrt{p}=\dfrac{a}{b}$ *avec* a,b *premiers entre eux dans* $\mathbb{N}^*$, *donne* $a^2=pb^2$, *donc* p_1 *divise* a, *soit* $a=p_1a_1$ *et* $p_1^2a_1^2=pb^2$, *soit* $p_1a_1^2=\prod_{k=2}^{r}p_kb^2$ *et* p_1 *va diviser* b *(il est premier avec* $\prod_{k=2}^{r}$ *dans le cas où* $r\geq2$*), ce qui contredit* $a\wedge b=1$. *L'égalité* $n+m\sqrt{p}=0$ *entraîne donc* $m=0$ *et* $n=0$.
3. *Si* $n\in\mathbb{Z}\subset\mathbb{Z}\left[\sqrt{p}\right]$ *est inversible, il existe alors* $n'+m'\sqrt{p}\in\mathbb{Z}\left[\sqrt{p}\right]$ *tel que* $n\left(n'+m'\sqrt{p}\right)=nn'+nm'\sqrt{p}=1$, *ce qui entraîne* $nn'=1$ *et* $nm'=0$, *soit* $m'=0$ *et* $nn'=1$ *dans* $\mathbb{Z}$, *ce qui donne* $n=n'=\pm1$. *Donc :*

$$\mathbb{Z}\cap\left(\mathbb{Z}\left[\sqrt{p}\right]\right)^{\times}=\mathbb{Z}^{\times}=\{-1,1\}$$

4. *Si* $a=n+m\sqrt{p}$ *est inversible dans* $\mathbb{Z}\left[\sqrt{p}\right]$, *il existe alors* $a'=n'+m'\sqrt{p}\in\mathbb{Z}\left[\sqrt{p}\right]$ *tel que* $aa'=1$, *soit* $(nn'+pmm')+(nm'+mn')\sqrt{p}=1$, *ce qui entraîne* $nn'+pmm'=1$ *et* $nm'+mn'=0$ *(unicité de l'écriture* $n+m\sqrt{p}$ *dans* $\mathbb{Z}\left[\sqrt{p}\right]$*). Il en résulte que :*

$$\left(n-m\sqrt{p}\right)\left(n'-m'\sqrt{p}\right)=(nn'+pmm')-(nm'+mn')\sqrt{p}=1$$

   et $n-m\sqrt{p}$ *est inversible dans* $\mathbb{Z}\left[\sqrt{p}\right]$.
5. *Si* $a=n+m\sqrt{p}$ *est inversible dans* $\mathbb{Z}\left[\sqrt{p}\right]$, *il en est alors de même de* $n-m\sqrt{p}$ *et du produit* $\left(n+m\sqrt{p}\right)\left(n-m\sqrt{p}\right)=n^2-pm^2$ *(*$\mathbb{Z}\left[\sqrt{p}\right]$ *est un groupe multiplicatif), ce qui entraîne* $n^2-pm^2=\pm1$. *Réciproquement, si* n *et* m *sont tels que* $n^2-pm^2=\pm1$, *on a alors* $\left(n+m\sqrt{p}\right)\left(n-m\sqrt{p}\right)=\pm1$ *et* $n+m\sqrt{p}$ *est inversible d'inverse* $\pm\left(n-m\sqrt{p}\right)$.
   On peut montrer que les éléments inversibles de $\mathbb{Z}\left[\sqrt{2}\right]$ *sont les éléments de la forme* $\pm\left(1+\sqrt{2}\right)^n$ *où* n *est un entier relatif, l'inverse de* $\pm\left(1+\sqrt{2}\right)^n$ *étant* $\pm\left(-1+\sqrt{2}\right)^n$.

Exercice 21.8 *On désigne par* p *un entier naturel non nul et par* $\mathbb{Z}\left[i\sqrt{p}\right]$ *l'ensemble des nombres complexes défini par :*

$$\mathbb{Z}\left[i\sqrt{p}\right]=\left\{a+ib\sqrt{p}\mid(a,b)\in\mathbb{Z}^2\right\}.$$

1. *Montrer que* $\mathbb{Z}\left[i\sqrt{p}\right]$ *est un anneau unitaire commutatif et intègre (pour* $p=1$, $\mathbb{Z}[i]$ *est l'anneau des entiers de Gauss).*
2. *Montrer que* $\mathbb{Z}\left[i\sqrt{p}\right]$ *est contenu dans tout sous anneau unitaire de* $\mathbb{C}$ *qui contient* $i\sqrt{p}$. *L'anneau* $\mathbb{Z}\left[i\sqrt{p}\right]$ *est donc le plus petit sous anneau de* $\mathbb{C}$ *(pour l'ordre de l'inclusion) qui contient* $i\sqrt{p}$, *on dit que c'est le sous anneau de* $\mathbb{C}$ *engendré par* $i\sqrt{p}$.

3. *Montrer que* $\mathbb{Z}\left[i\sqrt{p}\right]$ *est égal à l'intersection de tous les sous anneaux de* $\mathbb{C}$ *qui contiennent* i.
4. *Déterminer le groupe* $\mathbb{Z}\left[i\sqrt{p}\right]^{\times}$ *des éléments inversibles de* $\mathbb{Z}\left[i\sqrt{p}\right]$.

Solution 21.8

1. *Il suffit de montrer que* $\mathbb{Z}\left[i\sqrt{p}\right]$ *est un sous anneau de* $\mathbb{C}$.
On a $1 = 1 + i \cdot 0 \cdot \sqrt{p} \in \mathbb{Z}\left[i\sqrt{p}\right]$. *Pour* $z = a + ib\sqrt{p}$ *et* $z' = a' + ib'\sqrt{p}$, *où* a, a', b, b' *sont des entiers relatifs, on a :*
$$\begin{cases} z - z' = (a - a') + (b - b')\, i\sqrt{p} \in \mathbb{Z}\left[i\sqrt{p}\right] \\ zz' = (aa' - pbb') + (ab' + ba')\, i\sqrt{p} \in \mathbb{Z}\left[i\sqrt{p}\right] \end{cases}$$
Donc $\mathbb{Z}\left[i\sqrt{p}\right]$ *est un sous anneau de* $\mathbb{C}$ *et comme* $\mathbb{C}$, *il est unitaire commutatif et intègre.*
2. *Si un anneau* A *contient* $i\sqrt{p}$, *il contient également* 1 *(il s'agit d'anneaux unitaires) et en conséquence il contient tout élément de la forme* $a + ib\sqrt{p}$ *avec* $(a, b) \in \mathbb{Z}^2$. *On a donc* $\mathbb{Z}\left[i\sqrt{p}\right] \subset A$.
3. *En désignant par* $(A_i)_{i \in I}$ *la famille de tous les sous anneaux de* $\mathbb{C}$ *qui contiennent* $i\sqrt{p}$, *on a* $A = \bigcap_{i \in I} A_i \subset \mathbb{Z}\left[i\sqrt{p}\right]$ *puisque* $\mathbb{Z}\left[i\sqrt{p}\right]$ *est l'un de ces sous-anneaux et* $\mathbb{Z}\left[i\sqrt{p}\right] \subset A$ *puisque* A *est un anneau. On a donc bien* $\mathbb{Z}\left[i\sqrt{p}\right] = A$.
4. *Si* $z = a + ib\sqrt{p}$ *est inversible dans* $\mathbb{Z}\left[i\sqrt{p}\right]$, *il existe alors* $z' \in \mathbb{Z}\left[i\sqrt{p}\right]$ *tel que* $zz' = 1$ *et* $|z|^2 |z'|^2 = 1$ *avec* $|z|^2 = a^2 + b^2p^2 \in \mathbb{N}$ *et* $|z'|^2 \in \mathbb{N}$, *ce qui impose* $|z|^2 = |z'|^2 = 1$. *On a donc* $a^2 + b^2p^2 = 1$ *avec* $(a^2, b^2p^2) \in \mathbb{N}^2$, *ce qui équivaut à* $(a^2, b^2p^2) = (1, 0)$ *ou* $(a^2, b^2p^2) = (0, 1)$ *ou encore à* $a = \pm 1$ *et* $b = 0$ *ou* $a = 0$ *et* $b^2p^2 = 1$. *Pour* $p = 1$, *la condition* $b^2p^2 = 1$ *équivaut à* $b = \pm 1$ *et pour* $p \geq 2$, *elle n'est jamais réalisée puisque, pour tout* $b \in \mathbb{Z}$, *on a* $b^2p^2 = 0$ *ou* $b^2p^2 \geq p^2 \geq 4$. *On a donc* $\mathbb{Z}[i]^{\times} \subset \{-1, 1, -i, i\}$ *et* $\mathbb{Z}\left[i\sqrt{p}\right]^{\times} \subset \{-1, 1\}$ *pour* $p \geq 2$. *Les inclusions réciproques se vérifiant facilement. En définitive, on a :*
$$\mathbb{Z}[i\sqrt{p}]^{\times} = \begin{cases} \{-1, 1, -i, i\} & \text{si } p = 1, \\ \{-1, 1\} & \text{si } p \geq 2. \end{cases}$$

Exercice 21.9 *Soit* A *un anneau commutatif unitaire et* $\mathcal{M}_n(A)$ *l'anneau des matrices carrées d'ordre* n *à coefficients dans* A.

1. *Montrer que l'ensemble* $GL_n(A)$ *des matrices carrées d'ordre* n *à coefficients dans* A *telles que :*
$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)\, a_{i,\sigma(i)} \in A^{\times}$$
où $\mathfrak{S}_n$ *désigne l'ensemble de toutes les permutations de* $\{1, \cdots, n\}$ *et, pour* $\sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma)$ *la signature de* σ, *est un groupe multiplicatif.*
2. *Montrer que* $GL_n(A)$ *est le groupe des unités de* $\mathcal{M}_n(A)$ *(pour* $A = \mathbb{R}$ *ou* $A = \mathbb{C}$, *on retrouve un résultat classique).*

Solution 21.9 *Laissée au lecteur.*

Exercice 21.10 *On dit qu'un nombre réel* α *est algébrique s'il existe un polynôme non nul* P *dans* $\mathbb{Q}[X]$ *tel que* $P(\alpha) = 0$.
Un nombre réel qui n'est pas algébrique est dit transcendant.
On note $\mathbb{A}$ *l'ensemble des nombres réels algébriques.*

1. *Montrer que les réels* $\alpha = \sqrt{2}$ *et* $\beta = \sqrt{\dfrac{1+\sqrt{5}}{2}}$ *sont algébriques.*
2. *Montrer que le réel* $\beta = \sqrt[3]{2} + \sqrt[3]{4}$ *est algébrique.*
3. *Soient* α, β *deux nombres algébriques et* $P(X) = \sum_{k=0}^{n} a_k X^k$, $Q(X) = \sum_{k=0}^{m} b_k X^k$ *deux polynômes non nuls dans* $\mathbb{Q}[X]$ *tels que* $P(\alpha) = 0$ *et* $Q(\beta) = 0$, *avec* $a_n = b_m = 1$. *On note :*
$$\left\{\alpha^i \beta^j \mid 0 \leq i \leq n-1,\ 0 \leq j \leq m-1\right\} = \{\gamma_k \mid 1 \leq k \leq p\}$$
où $p = nm$ *et* $\gamma_1 = \alpha^0\beta^0 = 1$. *On désigne par* V *le vecteur de* $\mathbb{R}^p$ *de composantes* $\gamma_1, \cdots, \gamma_p$.
   (a) *Montrer qu'il existe deux matrices carrées d'ordre* p *à coefficients rationnels* A *et* B *telles que* $\alpha V = AV$ *et* $\beta V = BV$.
   (b) *Montrer que* $\mathbb{A}$ *est un anneau commutatif unitaire.*

Solution 21.10

1. $\alpha = \sqrt{2}$ *est annulé par* $X^2 - 2 \in \mathbb{Q}[X] \setminus \{0\}$.
On a $2\beta^2 = 1 + \sqrt{5}$ *et* $(2\beta^2 - 1)^2 = 5$. *Le réel* β *est donc annulé par le polynôme* $P(X) = X^4 - X^2 - 1 \in \mathbb{Q}[X]$ *et en conséquence il est algébrique.*
2. *On a* $\beta = \alpha + \alpha^2$, *où* $\alpha = \sqrt[3]{2}$ *est algébrique annulé par* $X^3 - 2$. *De* $\alpha^3 = 2$, *on déduit que :*
$$\beta^2 = \alpha^2 + 2\alpha + 4,\ \beta^3 = 6\left(\alpha^2 + \alpha + 1\right) = 6\beta + 6$$
β *est donc algébrique annulé par* $P(X) = X^3 - 6X - 6$.
3.
   (a) *Pour tout entier* k *compris entre* 1 *et* p *il existe deux indices* i, j *tels que* $\gamma_k = \alpha^i\beta^j$ *et* $\alpha\gamma_k = \alpha^{i+1}\beta^j$. *Pour* i *compris entre* 0 *et* $n-2$, $\alpha\gamma_k$ *est l'un des* γ_r *et pour* $i = n-1$, *on a :*
$$\alpha\gamma_k = \alpha^n\beta^j = -\sum_{r=0}^{n-1} a_r \alpha^r \beta^j$$
qui est une combinaison linéaire à coefficients rationnels des $\gamma_1, \cdots, \gamma_p$. *Il existe donc une matrice* A *dans* $\mathcal{M}_p(\mathbb{Q})$ *telle que* $\alpha V = AV$.
De manière analogue, on voit qu'il existe une matrice B *dans* $\mathcal{M}_p(\mathbb{Q})$ *telle que* $\beta V = BV$.
   (b) *On a* $1 \in \mathbb{A}$, *de manière évidente.*
Pour α, β *dans* $\mathbb{A}$, *on a avec les notations précédentes,* $(A - B)V = (\alpha - \beta)V$ *avec* V *non nul dans* $\mathbb{R}^p$, *ce qui signifie que* $\alpha - \beta$ *est une valeur propre de la matrice* $A - B$, *c'est donc une racine du polynôme caractéristique* χ_{A-B} *qui est dans* $\mathbb{Q}[X]$ *puisque* $A - B$ *est une matrice à coefficients rationnels. Il en résulte que* $\alpha - \beta$ *est algébrique. De même avec* $(AB)V = (\alpha\beta)V$ *on déduit que* $\alpha\beta$ *est algébrique.*
En conclusion $\mathbb{A}$ *est un sous-anneau de* $\mathbb{R}$.

21.4 Morphismes d'anneaux

Les anneaux considérés sont supposés unitaires.

On désigne par $(A, +, \cdot)$ et $(B, +, \cdot)$ deux anneaux unitaires. On note respectivement 0 et 1 les éléments neutres de ces anneaux pour l'addition et la multiplication (en cas d'ambiguïté, on les notera 0_A, 0_B, 1_A et 1_B).

Définition 21.6 *On dit que φ est un morphisme d'anneaux de A dans B si φ est une application de A dans B telle que :*

- $\varphi(1) = 1$;
- $\forall (a,b) \in A^2,\ \varphi(a+b) = \varphi(a) + \varphi(b)$;
- $\forall (a,b) \in A^2,\ \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$

Dans le cas où φ est de plus bijective, on dit que φ est un isomorphisme d'anneaux A sur B. Dans le cas où $A = B$, on dit que φ est un endomorphisme de l'anneau A et que c'est un automorphisme de l'anneau A si φ est de plus bijective.

On peut remarquer qu'un morphisme d'anneaux de A dans B est en particulier un morphisme de groupes de $(A,+)$ dans $(B,+)$. On a donc $\varphi(0) = 0$ et $\varphi(-a) = -\varphi(a)$ pour tout $a \in A$.

Définition 21.7 *Soit φ un morphisme d'anneaux de A dans B*

1. *Le noyau de φ est l'ensemble :*

$$\ker(\varphi) = \{x \in A \mid \varphi(x) = 0\}.$$

2. *L'image de φ est l'ensemble :*

$$\mathrm{Im}(\varphi) = \{\varphi(x) \mid x \in A\}.$$

Il est facile de vérifier que $\ker(\varphi)$ est un sous-anneau de A et $\mathrm{Im}(\varphi)$ un sous-anneau de B.

En fait pour tout $x \in \ker(\varphi)$ et tout $y \in A$, on a $\varphi(xy) = \varphi(x)\varphi(y) = 0 \cdot \varphi(y) = 0$, c'est-à-dire que $xy \in \ker(\varphi)$. Cette propriété se traduit en disant que $\ker(\varphi)$ est un idéal de l'anneau A.

Un tel morphisme est injectif [resp. surjectif] si, et seulement si, $\ker(\varphi) = \{0\}$ [resp. $\mathrm{Im}(\varphi) = B$].