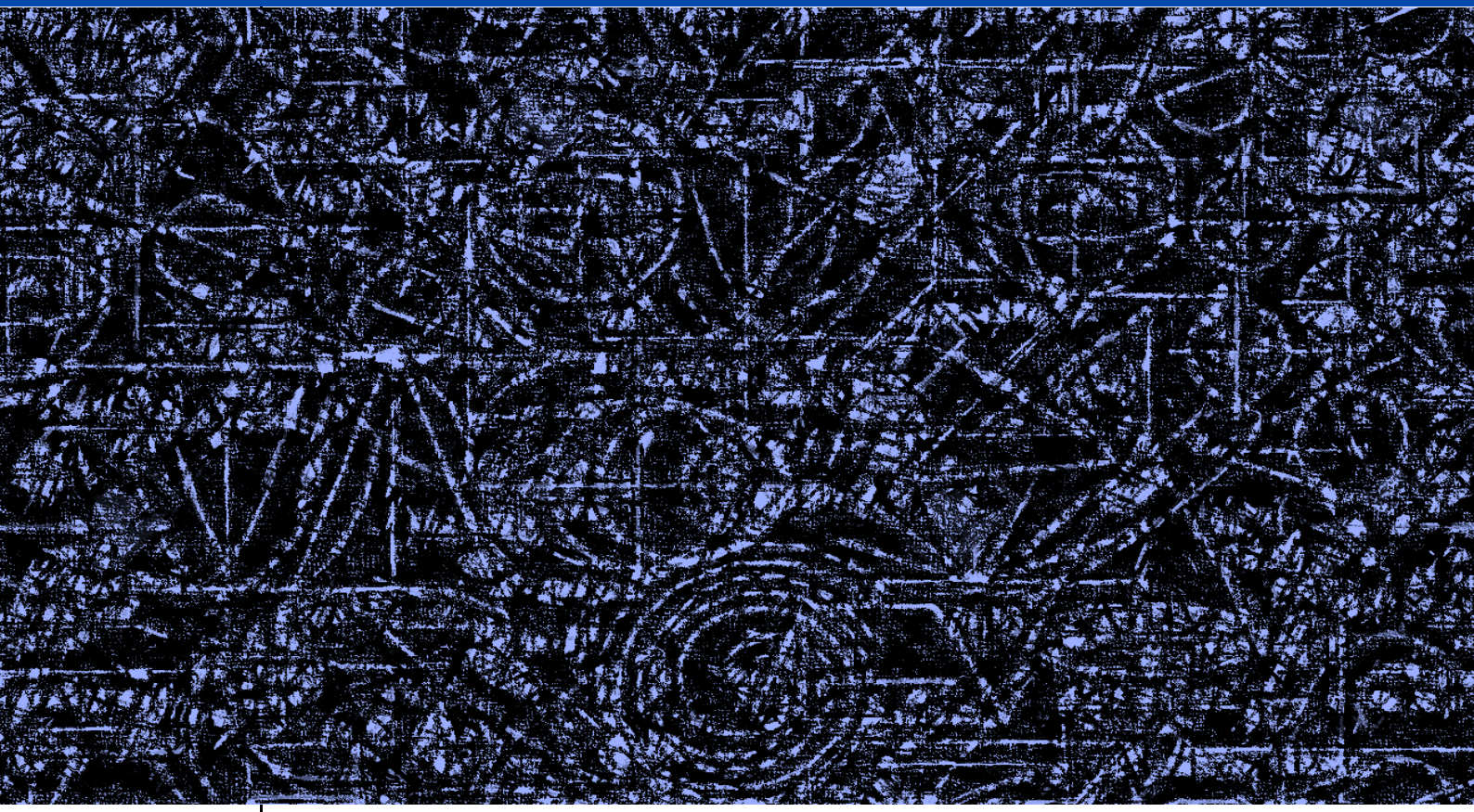
Structures algébriques : de l'anneau au corps

5



Introduction

Ce chapitre, qui est plus court, fait naturellement suite au chapitre précédent sur les structures algébriques. On s'intéresse ici aux anneaux et au corps. Cette fois-ci, on travaillera simultanément avec deux lois de composition interne définies sur un même ensemble.

Prérequis

- Structures algébriques : du magma au groupe (**chapitre 4**)

Objectifs du chapitre

- Définir la notion de **pseudo-anneau** et d'**anneau**
- Etudier les règles de calculs dans un anneau
- Etudier les anneaux remarquables (**anneau nul**, **anneaux intègres**...)
- Introduire la **nilpotence** dans un anneau et étudier quelques propriétés liées à celle-ci
- Définir la notion de **sous-anneau**
- Définir la notion de **corps** et de **sous-corps**
- Etudier quelques propriétés des corps (anneau intègre fini, **théorème de Wedderburn**...)

Le cours du chapitre 5

1 Anneaux

A Définitions

Définition 1

Soit A un ensemble muni de deux lois internes notées $+$ et $\times$.
Dire que le triplet $(A,+,\cdot)$ est un **pseudo-anneau**, signifie que :
1) le couple $(A,+)$ est un groupe abélien 2) la loi $\cdot$ est associative 3) la loi $\cdot$ est distributive sur la loi $+$.

La condition 1) justifie la notation $+$ pour la première loi et la condition 2) justifie la notation $\cdot$ pour la seconde loi.

Remarques

1. On confond volontiers le pseudo-anneau $(A,+,\cdot)$ avec l'ensemble A.
2. Un pseudo-anneau n'est jamais vide puisque le couple $(A,+)$ doit être un groupe.
3. Le triplet $(A,+,\cdot)$ est un pseudo-anneau si et seulement si $(A,+)$ est un groupe abélien, $(A,\cdot)$ est un demi-groupe et si la loi $\cdot$ est distributive sur la loi $+$.

Autrement dit, on dit « le pseudo-anneau A » au lieu de « le pseudo anneau $(A,+,\cdot)$ ».

Exemple

Le triplet $(2\mathbb{Z},+,\times)$ est un pseudo-anneau et la loi $\times$ n'admet pas de neutre dans $2\mathbb{Z}$.

Rappel : $2\mathbb{Z}=\{2k, k\in\mathbb{Z}\}$.

Définition 2

Soit A un ensemble muni de deux lois internes notées $+$ et $\times$.
Dire que le triplet $(A,+,\cdot)$ est un **anneau**, signifie que :
1) le triplet $(A,+,\cdot)$ est un pseudo-anneau 2) la loi $\cdot$ admet un neutre.

La **définition 2** est très importante pour toute la suite du cours.

Remarques

1. On confond volontiers l'anneau $(A,+,\cdot)$ avec l'ensemble A.
2. Un anneau n'est jamais vide puisque le couple $(A,+)$ doit être un groupe.
3. Le triplet $(A,+,\cdot)$ est un anneau si et seulement si $(A,+)$ est un groupe abélien, $(A,\cdot)$ est un monoïde et si la loi $\cdot$ est distributive sur la loi $+$.
4. Attention, selon les auteurs, les définitions précédentes peuvent être différentes. En effet :

L'auteur de ce cours	Chez d'autres auteurs
Pseudo-anneau	Anneau
Anneau	Anneau unitaire

5. Si la loi $\cdot$ est commutative, alors l'anneau est dit commutatif.

Exemples

1. Le triplet $(2\mathbb{Z},+,\times)$ n'est pas un anneau.
2. Les triplets $(\mathbb{Z},+,\times)$, $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des anneaux commutatifs.
3. Quand E est un ensemble, le triplet $(\mathcal{P}(E),\Delta,\cap)$ est un anneau commutatif.

La distributivité de l'intersection sur la différence symétrique fait l'objet de l'**exercice 11** du **chapitre 3**.

B Calculs dans un anneau

Soit $(A,+,\cdot)$ un anneau.
On note 0_A le neutre pour la loi $+$ et 1_A le neutre pour la loi $\cdot$. On note $-x$ l'opposé d'un élément x de A.

Théorème 1

Soit $(A,+,\cdot)$ un anneau.
0_A est un élément absorbant pour $\cdot$.

Autrement dit : $\forall x\in A, x\cdot 0_A=0_A\cdot x=0_A$.

Preuve

Soit x un élément de A.
On a : $x\cdot 0_A=x\cdot(0_A+0_A)=x\cdot 0_A+x\cdot 0_A$ et $0_A\cdot x=(0_A+0_A)\cdot x=0_A\cdot x+0_A\cdot x$.
Donc par régularité de l'addition dans A, $x\cdot 0_A=0_A$ et $0_A\cdot x=0_A$. □

Le cours du chapitre 5

Le **théorème 2** fait penser à la « règle des signes » vue au collège.

Théorème 2

Soient $(A,+,\cdot)$ un anneau, x et y deux éléments de A.

$$1)\ (-x)\cdot y=-(x\cdot y) \qquad 2)\ x\cdot(-y)=-(x\cdot y) \qquad 3)\ (-x)\cdot(-y)=x\cdot y\ .$$

Preuve

1) On a : $(-x)\cdot y+x\cdot y=((-x)+x)\cdot y=0_A\cdot y=0_A$, donc $(-x)\cdot y=-(x\cdot y)$.

2) On a : $x\cdot(-y)+x\cdot y=x\cdot(-y+y)=x\cdot 0_A=0_A$, donc $x\cdot(-y)=-(x\cdot y)$.

3) Comme pour tout x et y de A, $(-x)\cdot y=-(x\cdot y)$, et $x\cdot(-y)=-(x\cdot y)$, il vient que :

$$(-x)\cdot(-y)=-(x\cdot(-y))=-(-(x\cdot y))=x\cdot y\ .$$ □

Remarque

En particulier, on a pour tout x de A : $-1_A\cdot x=x\cdot(-1_A)=-x$.

Théorème 3

Soient $(A,+,\cdot)$ un anneau, x, y et z des éléments de A.

La notation $y-z$ abrège $y+(-z)$.

$$1)\ x\cdot(y-z)=x\cdot y-x\cdot z \qquad 2)\ (y-z)\cdot x=y\cdot x-z\cdot x\ .$$

Preuve

1) On a : $x\cdot(y-z)=x\cdot(y+(-z))=x\cdot y+x\cdot(-z)=x\cdot y+(-(x\cdot z))=x\cdot y-x\cdot z$.

2) On a : $(y-z)\cdot x=(y+(-z))\cdot x=y\cdot x+(-z)\cdot x=y\cdot x+(-(z\cdot x))=y\cdot x-z\cdot x$. □

Théorème 4

Soient $(A,+,\cdot)$ un anneau, x et y deux éléments de A.

$$\forall n\in\mathbb{Z},\ n(x\cdot y)=(nx)\cdot y=x\cdot(ny)\ .$$

Attention à la présence des points qui sont à mettre au bon endroit. En effet, par exemple, la notation $n\cdot x$ n'a pas de sens car n et x ne sont pas deux éléments du même ensemble.

Preuve

Récurrence sur n quand $n\in\mathbb{N}$.

Quand $n=0$, on a d'une part $0(x\cdot y)=0_A$ et d'autre part $(0x)\cdot y=0_A\cdot y=0_A$.

Soit $n\in\mathbb{N}$ et supposons que $n(x\cdot y)=(nx)\cdot y$.

On a, $(n+1)(x\cdot y)=n(x\cdot y)+x\cdot y=(nx)\cdot y+x\cdot y=((nx)+x)\cdot y=((n+1)x)\cdot y$.

On traite maintenant le cas où $n\in\mathbb{Z}_-^*$.

Utilisation du **théorème 2**.

Alors $-n\in\mathbb{N}$ et donc $n(x\cdot y)=-((-n)(x\cdot y))=-((-n)x\cdot y)=-((-n)x)\cdot y=(nx)\cdot y$. □

Remarques

1. En particulier, on a pour tout $n\in\mathbb{Z}$ et pour tout $x\in A$, $nx=(n1_A)\cdot x=x\cdot(n1_A)$.

2. Lorsque cela n'est pas confus, on peut écrire « n » au lieu de « $n1_A$ ».

C Propriétés plus générales dans les anneaux

Les théorèmes qui suivent utilisent le symbole somme « Σ » appelé *sigma*. Le lecteur qui n'est pas encore à l'aise avec ce dernier pourra consulter le chapitre suivant avant de revenir sur ce paragraphe ou bien le sauter.

Considérons un anneau $(A,+,\cdot)$ et $x_1,...,x_n$ (où $n\in\mathbb{N}^*$) des éléments de A.

La somme $x_1+x_2+...+x_n$ se note $\displaystyle\sum_{i=1}^{n}x_i$.

Théorème 5

Soit $(A,+,\cdot)$ un anneau.

$$\forall n\in\mathbb{N}^*,\forall(x_1,...,x_n)\in A^n,\forall(y_1,...,y_n)\in A^n,\sum_{i=1}^{n}(x_i+y_i)=\sum_{i=1}^{n}x_i+\sum_{i=1}^{n}y_i\ .$$

Preuve

Récurrence sur n.

L'égalité est évidente quand $n=1$.

Soit $n\in\mathbb{N}^*$ tel que $\sum_{i=1}^{n}(x_i+y_i)=\sum_{i=1}^{n}x_i+\sum_{i=1}^{n}y_i$.

On a :

$$\sum_{i=1}^{n+1}(x_i+y_i)=\sum_{i=1}^{n}(x_i+y_i)+(x_{n+1}+y_{n+1})=\left(\sum_{i=1}^{n}x_i+\sum_{i=1}^{n}y_i\right)+(x_{n+1}+y_{n+1})=\left(\sum_{i=1}^{n}x_i+x_{n+1}\right)+\left(\sum_{i=1}^{n}y_i+y_{n+1}\right)$$
$$=\sum_{i=1}^{n+1}x_i+\sum_{i=1}^{n+1}y_i\,.$$ □

Le **théorème 6** fait appel aux doubles sommes qui seront étudiées dans le chapitre suivant.
Ce théorème peut se comprendre intuitivement : pour sommer tous les éléments d'un tableau, on peut sommer ligne par ligne ou bien colonne par colonne.

Théorème 6

Soit $(A,+,\cdot)$ un anneau.

$$\forall(n,p)\in(\mathbb{N}^*)^2,\forall(x_{i,j})_{\substack{1\leqslant i\leqslant n\\1\leqslant j\leqslant n}}\in E^{np},\sum_{i=1}^{n}\sum_{j=1}^{p}x_{i,j}=\sum_{j=1}^{p}\sum_{i=1}^{n}x_{i,j}\,.$$

Preuve

Récurrence sur n avec p fixé.

Pour $n=1$ on a d'une part, $\sum_{i=1}^{1}\sum_{j=1}^{p}x_{i,j}=\sum_{j=1}^{p}x_{1,j}$ et d'autre part, $\sum_{j=1}^{p}\sum_{i=1}^{1}x_{i,j}=\sum_{j=1}^{p}x_{1,j}$.

Soit $n\in\mathbb{N}^*$ tel que $\sum_{i=1}^{n}\sum_{j=1}^{p}x_{i,j}=\sum_{j=1}^{p}\sum_{i=1}^{n}x_{i,j}$.

Utilisation du **théorème 5**.

On a : $\sum_{i=1}^{n+1}\sum_{j=1}^{p}x_{i,j}=\sum_{i=1}^{n}\sum_{j=1}^{p}x_{i,j}+\sum_{j=1}^{p}x_{n+1,j}=\sum_{j=1}^{p}\sum_{i=1}^{n}x_{i,j}+\sum_{j=1}^{p}x_{n+1,j}=\sum_{j=1}^{p}\left(\sum_{i=1}^{n}x_{i,j}+x_{n+1,j}\right)$

$$=\sum_{j=1}^{p}\sum_{i=1}^{n+1}x_{i,j}\,.$$ □

Le **théorème 7** est assez utilisé en pratique.

Théorème 7

Soient $(A,+,\cdot)$ un anneau et a un élément de A.

$$\forall n\in\mathbb{N}^*,1_A-a^n=(1_A-a)\sum_{k=0}^{n-1}a^k=\left(\sum_{k=0}^{n-1}a^k\right)(1_A-a)\,.$$

Pour simplifier, les points ont été remplacés par une absence de symbole.

Preuve

Récurrence sur n.

Avec $n=1$, on a d'une part $1_A-a^1=1_A-a$ et d'autre part $(1_A-a)\sum_{k=0}^{0}a^k=(1_A-a)\cdot a^0=(1_A-a)\cdot 1_A=1_A-a$.

Soit $n\in\mathbb{N}^*$ et supposons que $1_A-a^n=(1_A-a)\sum_{k=0}^{n-1}a^k$.

On a : $(1_A-a)\sum_{k=0}^{n}a^k=(1_A-a)\left(\sum_{k=0}^{n-1}a^k+a^n\right)=(1_A-a)\sum_{k=0}^{n-1}a^k+(1_A-a)\cdot a^n=(1_A-a^n)+(1_A-a)\cdot a^n$

$$=1_A-a^n-a^{n+1}+a^n$$
$$=1_A-a^{n+1}\,.$$ □

Théorème 8

Soient $(A,+,\cdot)$ un anneau et a un élément de A.

$$\forall n\in\mathbb{N},1_A+a^{2n+1}=(1_A+a)\sum_{k=0}^{2n}(-1)^k a^k=\left(\sum_{k=0}^{2n}(-1)^k a^k\right)(1_A+a)\,.$$

Preuve

Récurrence sur n.

Avec $n=0$, on a d'une part $1_A + a^{0+1} = 1_A + a^1 = 1_A + a$ puis, $(1_A+a)\sum_{k=0}^{0}(-1)^k a^k = (1_A+a)\cdot 1_A = 1_A + a$.

Soit $n \in \mathbb{N}$ et supposons que $1_A + a^{2n+1} = (1_A+a)\sum_{k=0}^{2n}(-1)^k a^k$.

Remarquez que $2(n+1) = 2n+2$.

On a : $(1_A+a)\sum_{k=0}^{2n+2}(-1)^k a^k = (1_A+a)\left(\sum_{k=0}^{2n}(-1)^k a^k - a^{2n+1} + a^{2n+2}\right)$

$= (1_A+a)\left(\sum_{k=0}^{2n}(-1)^k a^k\right) - (1_A+a)\cdot a^{2n+1} + (1_A+a)\cdot a^{2n+2}$

$= 1_A + a^{2n+1} - (1_A+a)\cdot a^{2n+1} + (1_A+a)\cdot a^{2n+2}$

$= 1_A + a^{2n+1} - a^{2n+1} - a^{2n+2} + a^{2n+2} + a^{2n+3}$

Remarquez que $2n+3 = 2(n+1)+1$.

$= 1_A + a^{2n+3}$. □

Théorème 9

Soient $(A,+,\cdot)$ un anneau et a un élément de A.

1) $\forall n \in \mathbb{N}^*, \forall (x_1,...,x_n) \in A^n, \sum_{i=1}^{n} a x_i = a\sum_{i=1}^{n} x_i$ 2) $\forall n \in \mathbb{N}^*, \forall (x_1,...,x_n) \in A^n, \sum_{i=1}^{n} x_i a = \left(\sum_{i=1}^{n} x_i\right) a$.

Comme vous l'avez peut-être remarqué, on a pris l'habitude de mettre i comme indice de sommation quand il y a des indices (**théorèmes 5** et **6**) et k quand ces des puissances (**théorème 7** et **8**).

Preuve

Nous démontrons ici que le 1) (l'autre se fera de la même manière).

Récurrence sur n.

Evident quand $n=1$.

Soit $n \in \mathbb{N}^*$ et supposons que $\sum_{i=1}^{n} a x_i = a\sum_{i=1}^{n} x_i$.

On a : $\sum_{i=1}^{n+1} a x_i = \sum_{i=1}^{n} a x_1 + a x_{n+1} = a\sum_{i=1}^{n} x_i + a x_{n+1} = a\left(\sum_{i=1}^{n} x_i + x_{n+1}\right) = a\sum_{i=1}^{n+1} x_i$. □

Théorème 10

Soit $(A,+,\cdot)$ un anneau.

$$\forall (n,p) \in (\mathbb{N}^*)^2, \forall (x_1,...,x_n) \in A^n, \forall (y_1,...,y_p) \in A^p, \sum_{i=1}^{n}\sum_{j=1}^{p} x_i y_j = \sum_{j=1}^{p}\sum_{i=1}^{n} x_i y_j = \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{p} y_j\right).$$

Preuve

Récurrence sur n avec p fixé.

Avec $n=1$, on a d'une part $\sum_{i=1}^{1}\sum_{j=1}^{p} x_i y_j = \sum_{j=1}^{p} x_1 y_j$, $\sum_{j=1}^{p}\sum_{i=1}^{1} x_i y_j = \sum_{j=1}^{p} x_1 y_j$ puis, $\left(\sum_{i=1}^{1} x_i\right)\left(\sum_{j=1}^{p} y_j\right) = x_1\sum_{j=1}^{p} y_j$, soit en utilisant le **théorème 9**, $\sum_{j=1}^{p} x_1 y_j$.

Soit $n \in \mathbb{N}^*$ et supposons que $\sum_{i=1}^{n}\sum_{j=1}^{p} x_i y_j = \sum_{j=1}^{p}\sum_{i=1}^{n} x_i y_j = \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{p} y_j\right)$.

Utilisation du **théorème 5**.

On a d'une part, $\sum_{i=1}^{n+1}\sum_{j=1}^{p} x_i y_j = \sum_{i=1}^{n}\sum_{j=1}^{p} x_i y_j + \sum_{j=1}^{p} x_{n+1} y_j = \sum_{j=1}^{p}\sum_{i=1}^{n} x_i y_j + \sum_{j=1}^{p} x_{n+1} y_j = \sum_{j=1}^{p}\left(\sum_{i=1}^{n} x_i y_j + x_{n+1} y_j\right)$

$= \sum_{j=1}^{p}\left(\sum_{i=1}^{n+1} x_i y_j\right)$.

D'autre part, $\sum_{i=1}^{n+1}\sum_{j=1}^{p} x_i y_j = \sum_{i=1}^{n}\sum_{j=1}^{p} x_i y_j + \sum_{j=1}^{p} x_{n+1} y_j = \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{p} y_j\right) + \sum_{j=1}^{p} x_{n+1} y_j$

$$= \left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{p} y_j\right) + x_{n+1}\sum_{j=1}^{p} y_j$$

$$= \left(\sum_{i=1}^{n} x_i + x_{n+1}\right)\left(\sum_{j=1}^{p} y_j\right)$$

$$= \left(\sum_{i=1}^{n+1} x_i\right)\left(\sum_{j=1}^{p} y_j\right). \qquad \square$$

Le théorème suivant est plus délicat à démontrer car il utilise le *changement de variable* et la **formule de Pascal** qui seront revus respectivement dans les **chapitres 6** et **10**.

Blaise Pascal (1623-1662) était un mathématicien français.

Isaac Newton (1642-1727) était un mathématicien britannique.
Dans ce théorème très important, l'hypothèse de la commutativité des éléments x et y est fondamentale.

Théorème 11 **Binôme de Newton**

Soient $(A,+,\cdot)$ un anneau, x et y deux éléments commutant de A.

$$\forall n \in \mathbb{N}, (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Preuve

Récurrence sur n.

On a d'une part $(x+y)^0 = 1_A$ et d'autre part $\sum_{k=0}^{0} \binom{0}{k} x^k y^{-k} = 1(1_A \cdot 1_A) = 1_A$.

Soit $n \in \mathbb{N}$ et supposons que $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.

On a : $(x+y)^{n+1} = (x+y)^n \cdot (x+y) = \left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right)(x+y) = \left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right) x + \left(\sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}\right) y$

Puisque x et y commutent, il en est de même pour x et y^{n-k} (**exercice 5** du **chapitre 4**).

$$= \sum_{k=0}^{n} \binom{n}{k} x^{k+1} y^{n-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k+1}$$

Changement de variable $l = k+1$.

$$= \sum_{l=1}^{n+1} \binom{n}{l-1} x^l y^{n+1-l} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k}$$

Retour à la variable initiale.

$$= \sum_{k=1}^{n+1} \binom{n}{k-1} x^k y^{n+1-k} + \sum_{k=0}^{n} \binom{n}{k} x^k y^{n+1-k}$$

Puisque $\binom{n}{-1} = 0$ et $\binom{n}{n+1} = 0$.

$$= \sum_{k=0}^{n+1} \binom{n}{k-1} x^k y^{n+1-k} + \sum_{k=0}^{n+1} \binom{n}{k} x^k y^{n+1-k}$$

Utilisation du **théorème 5**.

$$= \sum_{k=0}^{n+1} \left(\binom{n}{k-1} + \binom{n}{k}\right) x^k y^{n+1-k}$$

Utilisation de la **formule de Pascal**.

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k y^{n+1-k}. \qquad \square$$

D Eléments inversibles d'un anneau

Théorème 12

Soit $(A,+,\cdot)$ un anneau.

L'ensemble des éléments inversibles pour $\cdot$ est un groupe.

Le **théorème 12** est une conséquence immédiate de l'**exercice 72** du **chapitre 4**.

Remarques

1. L'ensemble des éléments inversibles de l'anneau A se note habituellement $A^\times$.
2. L'ensemble des éléments inversible d'un anneau n'est jamais vide puisqu'il contient l'élément 1_A.

Donc $(A^\times,\cdot)$ est un groupe.

Le cours du chapitre 5

Exemples

1. Pour la multiplication, les éléments inversibles de $\mathbb{Z}$ sont -1 et 1. Il vient donc que $(\{-1,1\},\times)$ est un groupe.

2. Pour la multiplication, les éléments inversibles de $\mathbb{R}$ sont tous les nombres réels non nuls. Donc $(\mathbb{R}^*,\times)$ est un groupe.

E Anneau-produit

On sait depuis le chapitre précédent que si G et H sont des groupes, alors il en est de même pour $G\times H$ muni de la loi produit des lois de G et H.
Il se passe en fait la même chose avec les anneaux.

Théorème 13

Soient $(A,+_1,\times_1)$ et $(B,+_2,\times_2)$ deux anneaux et $+$ (resp. $\times$) la loi produit des lois $+_1$ et $+_2$ (resp. $\times_1$ et $\times_2$).
Le triplet $(A\times B,+,\times)$ est un anneau.

Autrement dit, un produit d'anneau est encore un anneau (appelé d'ailleurs **anneau-produit**).
Rappelons que les lois $+$ et $\times$ sont définis sur $A\times B$ par :
$\forall (x,y),(x',y')\in A\times B,$
$\begin{cases}(x,y)+(x',y')=(x+_1x',y+_2y')\\(x,y)\times(x',y')=(x\times_1x',y\times_2y')\end{cases}.$

Preuve

Il est clair que le couple $(A\times B,+)$ est un groupe (de neutre $(0_A,0_B)$) et que le couple $(A\times B,\times)$ est un monoïde (de neutre $(1_A,1_B)$).

Il reste à justifier la distributivité de la loi $\times$ sur la loi $+$.

$$\begin{aligned}\forall (x,y),(x',y'),(x'',y'')\in A\times B,(x,y)\times((x',y')+(x'',y'')) &= (x,y)\times(x'+_1x'',y'+_2y'')\\ &= (x\times_1(x'+_1x''),y\times_2(y'+_2y''))\\ &= (x\times_1x'+_1x\times_1x'',y\times_2y'+_2y\times_2y'')\\ &= (x\times_1x',y\times_2y')+(x\times_1x'',y\times_2y'')\\ &= (x,y)\times(x',y')+(x,y)\times(x'',y'').\end{aligned}$$

Utilisation de la distributivité dans les anneaux A et B.

De même, on montre que $((x',y')+(x'',y''))\times(x,y)=(x',y')\times(x,y)+(x'',y'')\times(x,y)$. □

Exemple

Le triplet $(\mathbb{Z}^2,\oplus,\otimes)$ est un anneau-produit de l'anneau $(\mathbb{Z},+,\times)$ par lui-même.

Théorème 14

Soient $(A,+_1,\times_1)$ et $(B,+_2,\times_2)$ deux anneaux et $+$ (resp. $\times$) la loi produit des lois $+_1$ et $+_2$ (resp. $\times_1$ et $\times_2$).

$$(A\times B)^\times=A^\times\times B^\times.$$

Attention à l'ordre des ensembles.

Preuve

Procédons par équivalence pour plus de souplesse.

$$\begin{aligned}\forall (x,y)\in A\times B,(x,y)\in A^\times\times B^\times &\Leftrightarrow \begin{cases}x\in A^\times\\y\in B^\times\end{cases}\Leftrightarrow\begin{cases}\exists x'\in A,x\times_1x'=x'\times_1x=1_A\\\exists y'\in B,y\times_2y'=y'\times_2y=1_B\end{cases}\\ &\Leftrightarrow\exists (x',y')\in A\times B,\begin{cases}(x,y)\times(x',y')=(1_A,1_B)\\(x',y')\times(x,y)=(1_A,1_B)\end{cases}\\ &\Leftrightarrow (A,B)\in(A\times B)^\times.\end{aligned}$$

Utilisation de la propriété caractéristique des couples.

□

F L'anneau-nul

Est-il possible que les neutres d'un d'anneau coïncident ? La réponse est donnée dans le théorème suivant :

Théorème 15

Soit $(A,+,\cdot)$ un anneau.

$$A=\{0_A\}\Leftrightarrow 0_A=1_A.$$

Le lecteur vérifiera facilement que le triplet $(\{0_A\},+,\cdot)$ est un anneau.
Ce théorème montre qu'il n'y a que l'**anneau nul** (c'est-à-dire réduit à un singleton) où les neutres coïncident. Autrement dit, un anneau à plus d'un élément a nécessairement des neutres distincts.

Preuve

($\Rightarrow$) Evident.
($\Leftarrow$) En supposant que $0_A=1_A$, il vient que pour tout x de A : $x=x\cdot 1_A=x\cdot 0_A=0_A$. □

Le cours du chapitre 5

G Anneaux intègres

Parmi les anneaux, il y a les anneaux dits **intègres**. Pour définir cette notion, nous avons besoin de la définition suivante qui est délicate :

Définition 3

Soient $(A,+,\cdot)$ un anneau et x un élément de A.

1) Dire que x est un **diviseur de zéro à gauche** dans A, signifie que : $\begin{cases} x \neq 0_A \\ \exists y \in A \setminus \{0_A\}, x \cdot y = 0_A \end{cases}$.

2) Dire que x est un **diviseur de zéro à droite** dans A, signifie que : $\begin{cases} x \neq 0_A \\ \exists y \in A \setminus \{0_A\}, y \cdot x = 0_A \end{cases}$.

Autrement dit, x est un diviseur de zéro quand il est diviseur de zéro à gauche et à droite.

3) Dire que x est un **diviseur de zéro** dans A, signifie que : $\begin{cases} x \neq 0_A \\ \exists y \in A \setminus \{0_A\}, x \cdot y = y \cdot x = 0_A \end{cases}$.

Remarque

Comme vous l'avez constaté, nous convenons que l'élément 0_A n'est pas un diviseur de zéro.

Exemples

1. L'anneau-produit $(\mathbb{Z}^2, \oplus, \otimes)$ contient des diviseurs de zéro. Par exemple, les couples $(1,0)$ et $(0,1)$.

Il est clair que $(1,0) \otimes (0,1) = (0,0)$.

2. L'anneau $(\mathbb{R}^{\mathbb{R}}, +, \times)$ contient des diviseurs de zéro. Par exemple les applications f et g définies par :

$$f : \mathbb{R} \longrightarrow \mathbb{R} \quad \text{et} \quad g : \mathbb{R} \longrightarrow \mathbb{R}.$$
$$x \mapsto \begin{cases} 0 \text{ si } x \leqslant 0 \\ x \text{ si } x \geqslant 0 \end{cases} \qquad x \mapsto \begin{cases} x \text{ si } x \leqslant 0 \\ 0 \text{ si } x \geqslant 0 \end{cases}$$

Il est clair que $f \times g = 0_{\mathbb{R}^{\mathbb{R}}}$.

3. L'anneau nul n'a aucun diviseur de zéro.
4. L'anneau $(\mathbb{Z}, +, \times)$ n'a aucun diviseur de zéro (puisqu'un produit nul entraîne nécessairement que l'un des facteurs du produit le soit).

Définition 4

Soit $(A,+,\cdot)$ un anneau non nul.

Dire que l'anneau A est **intègre** signifie qu'il n'admet aucun diviseur de zéro dans A.

Dans la **définition 4** nous excluons le cas particulier de l'anneau nul car il rendrait faux certains théorèmes.
Nous avons aussi décidé dans cette définition de ne pas inclure la commutativité car nous étudierons plus loin les *quaternions* (la structure associée est un anneau intègre non commutatif).

Nous allons réécrire le fait que l'anneau A est intègre qu'avec des quantificateurs.
Notons P l'assertion « $x \neq 0_A$ », Q l'assertion « $y \neq 0_A$ » et R l'assertion « $xy = 0_A$ ».

Quand A n'est pas intègre, l'assertion suivante est vérifiée : $\exists (x,y) \in A^2, R \wedge (P \wedge Q)$.

Utilisation d'une loi de De Morgan.

Ainsi, par négation, quand A est intègre, l'assertion suivante est vérifiée : $\forall (x,y) \in A^2, \neg R \vee ((\neg P) \vee (\neg Q))$.

On rappelle que, quelles que soient les assertions P et Q :
$(\neg P \vee Q) \Leftrightarrow (P \Rightarrow Q)$.

Cela revient donc au même de dire que : $\forall (x,y) \in A^2, R \Rightarrow ((\neg P) \vee (\neg Q))$.

En conséquence, dire que A est intègre, revient à dire que : $\forall (x,y) \in A^2, xy = 0_A \Rightarrow (x = 0_A) \vee (y = 0_A)$.

Exemples

1. L'anneau $(\mathbb{Z}, +, \times)$ est intègre.
2. L'anneau $(\mathbb{Z}^2, \oplus, \otimes)$ n'est pas intègre.

Théorème 16

Soient $(A,+,\cdot)$ un anneau et x un élément de A.

Si x est un diviseur de zéro, alors x n'est pas un élément régulier pour $\cdot$.

Preuve

Supposons que x est un diviseur de zéro et régulier.
Il existe alors un élément y de $A \setminus \{0_A\}$ tel que $xy = 0_A$.
L'égalité précédente devient alors $xy = x \cdot 0_A$, soit, puisque x est régulier, $y = 0_A$, ce qui est absurde. □

Remarque

Il est clair quand dans un anneau, si un élément est inversible pour la seconde loi, alors nécessairement, ce n'est pas un diviseur de zéro.

En effet, tout élément inversible dans un monoïde est régulier.

Théorème 17

Soit $(A,+,\cdot)$ un anneau intègre.

Tout élément non nul de A est régulier.

La quantification associée à ce théorème étant trop lourde, nous avons préféré la donner en français.

Preuve

Soient a un élément non nul de A, x et y deux éléments de A tels que $ax = ay$.

Les calculs bien connus dans un anneau entraînent que $a(x-y) = 0_A$.

L'anneau étant intègre, on a nécessairement $x = y$. □

L'anneau intègre n'étant pas nécessairement commutatif, on vérifie aussi que l'égalité $xa = ya$ entraine $x = y$.

H Elément nilpotent

Soit $(A,+,\cdot)$ un anneau.

Comme pour les magmas, un élément a de A qualifié d'**idempotent** vérifie l'égalité $a^2 = a$.

Définition 5

Soient $(A,+,\cdot)$ un anneau et x un élément de A.

Dire que x est **nilpotent** signifie que :

$$\exists n \in \mathbb{N}^*, x^n = 0_A.$$

La **définition 5** nous servira beaucoup en algèbre linéaire.

Remarques

1. Dans un anneau intègre, seul 0_A est nilpotent.
2. Il est clair que dans un anneau, si un élément non nul est nilpotent, alors c'est un diviseur de zéro.
3. Dans un anneau, un élément non nul et idempotent n'est jamais un élément nilpotent.
4. L'ensemble des éléments nilpotents dans un anneau est appelé le **nilradical**.
5. L'ensemble $\{n \in \mathbb{N}^*, x^n = 0_A\}$ admet un minimum (pourquoi ?). Ce dernier est appelé **indice de nilpotence**.

Le nilradical sera étudié en **licence 2**.

Théorème 18

Soient $(A,+,\cdot)$ un anneau, x et y deux éléments de A.

Si x et y sont nilpotents et commutent, alors $x+y$ est nilpotent.

Autrement dit, la somme de deux éléments nilpotents et commutant est nilpotente.

Preuve

La preuve est courte mais astucieuse.

Supposons que x et y sont nilpotents et commutent.

Il existe alors un couple $(n,p) \in (\mathbb{N}^*)^2$ tel que $x^n = 0_A$ et $y^p = 0_A$.

D'après le binôme de Newton (puisque x et y commutent), on a :

$$(x+y)^{n+p-1} = \sum_{k=0}^{n+p-1} \binom{n+p-1}{k} x^{n+p-1-k} y^k = x^n \left(\sum_{k=0}^{p-1} \binom{n+p-1}{k} x^{p-1-k} y^k \right) + y^p \left(\sum_{k=p}^{n+p-1} \binom{n+p-1}{k} x^{n+p-1-k} y^{k-p} \right) = 0_A.$$

Ce qui prouve que $x+y$ est nilpotent. □

Le calcul de $(x+y)^{n+p}$ conduirait évidemment au même résultat.

Remarque

En gardant le « squelette » de la démonstration précédente, il est clair que $x-y$ est aussi nilpotent.

Théorème 19

Soient $(A,+,\cdot)$ un anneau, x et y deux éléments de A.

Si x et nilpotent et commute avec y, alors xy est nilpotent.

Le lecteur initié sait que le **théorème 19** n'est pas surprenant. En effet, le nilradical est un *idéal* !

Il n'est donc pas nécessaire que y soit nilpotent.

Preuve

Supposons que x est nilpotent.

Il existe alors un entier naturel non nul tel que $x^n = 0_A$, d'où $(xy)^n = x^n \cdot y^n = 0_A \cdot y^n = 0_A$. □

L'égalité $(xy)^n = x^n \cdot y^n$ n'est vraie que si x et y commutent.

Le cours du chapitre 5

I Sous-anneaux

Comme pour les sous-groupes de groupes, nous avons les **sous-anneaux** des anneaux.

Les sous-anneaux sont de belles structures mais sont quand même moins intéressantes que d'autres.
En licence 2, c'est la notion d'*idéal* qui nous intéressera.

Définition 6

Soient $(A,+,\cdot)$ un anneau et B un sous-ensemble de A.

Dire que B est un **sous-anneau** de A signifie que :

$$1)\ B \text{ est un sous-groupe de } (A,+) \qquad 2)\ \forall (x,y)\in B^2, xy\in B \qquad 3)\ 1_A \in B\,.$$

Exemples

1. Cherchons les sous-anneaux de $(\mathbb{Z},+,\times)$.

Il est clair que l'anneau $(\{0\},+,\times)$ n'est pas un sous-anneau de $\mathbb{Z}$ (car 1 est différent de 0).

De même, il est clair que $(n\mathbb{Z},+,\times)$ avec $n\geqslant 2$ n'est pas un sous-anneau de $\mathbb{Z}$ (car $1\notin n\mathbb{Z}$).

Finalement, le seul sous-anneau de $\mathbb{Z}$ est lui-même.

2. $\mathbb{Q}$ est un sous-anneau de $(\mathbb{R},+,\times)$ et $\mathbb{R}$ est un sous-anneau de $(\mathbb{C},+,\times)$.

La démonstration du **théorème 20** est immédiate.
Il donne une méthode intéressante pour montrer qu'une structure est un anneau : on montre que c'est un sous-anneau d'un anneau connu.

Théorème 20 — **Première caractérisation des sous-anneaux**

Soient $(A,+,\cdot)$ un anneau et B un sous-ensemble de A.

Le sous-ensemble B est un sous-anneau de A si et seulement si :

$$1)\ B \text{ est stable pour les lois } + \text{ et } \cdot \qquad 2)\ B \text{ est un anneau pour les lois induites } + \text{ et } \cdot \qquad 3)\ 1_A \in B\,.$$

Remarque

On pourrait légitimement croire que la condition 3) ne sert à rien puisque B est un anneau pour les lois induites $+$ et $\cdot$.

Il n'en est rien ! En effet, prenons le cas de l'anneau-produit $(\mathbb{Z}^2,\oplus,\otimes)$.

Le sous-ensemble $\mathbb{Z}\times\{0\}$ est stable pour les lois $\oplus$ et $\otimes$. De plus, c'est aussi un anneau (le lecteur pourra le vérifier facilement) de neutre $(1,0)$.

En revanche, ce neutre n'est pas le même que celui de la loi $\otimes$ définie dans $\mathbb{Z}^2$.

Il vient alors que $\mathbb{Z}\times\{0\}$ n'est pas un sous-anneau de $(\mathbb{Z}^2,\oplus,\otimes)$.

Le **théorème 21** est souvent utilisé en pratique.

Théorème 21 — **Seconde caractérisation des sous-anneaux**

Soient $(A,+,\cdot)$ un anneau et B un sous-ensemble de A.

Le sous-ensemble B est un sous-anneau de A si et seulement si :

$$1)\ \forall (x,y)\in B^2, x-y\in B \qquad 2)\ \forall (x,y)\in B^2, xy\in B \qquad 3)\ 1_A\in B\,.$$

Preuve

($\Rightarrow$) Evident.

($\Leftarrow$) Soient x et y deux éléments de B tels que $x-y\in B$, $xy\in B$ et $1_A\in B$.

On doit montrer que B est un sous-groupe de $(A,+)$.

Utilisation de la seconde caractérisation des sous-groupes vue dans le chapitre précédent.

On a $0_A = 1_A - 1_A \in B$. □

J Centre d'un anneau

Comme pour les magmas et les groupes, il est naturel de s'intéresser à l'ensemble des éléments d'un anneau qui commutent avec tous les éléments de l'anneau (via la seconde loi évidemment).

Ainsi, par définition :
$\mathcal{Z}(A)=\{x\in A, \forall y\in A, xy=yx\}$.

La notation reste la même qu'avec les groupes. Pour un anneau A, on note $\mathcal{Z}(A)$ son centre. Mais le centre d'un anneau est-il un sous-anneau de l'anneau ?

La démonstration du **théorème 22** est immédiate (voir le **théorème 24** du **chapitre 4**).

Théorème 22

Soit $(A,+,\cdot)$ un anneau.

Le centre de l'anneau A est un sous-anneau de A.

Remarque

Il est clair que si l'anneau A est commutatif, alors $\mathcal{Z}(A)=A$.

Le cours du chapitre 5

2 Corps

A Définition

Définition 7

Soit K un ensemble muni de deux lois internes $+$ et $\cdot$.
Dire que le triplet $(K,+,\cdot)$ est un **corps** signifie que :

1) $K \neq \{0_K\}$ 2) $(K,+,\cdot)$ est un anneau 3) tout élément non nul de K admet un inverse pour $\cdot$.

On entend par « non nul », différent du neutre de la première loi.

Remarques

1. On confond volontiers le corps $(K,+,\cdot)$ avec l'ensemble K.
2. Un corps a au minimum deux éléments car il n'est pas réduit au singleton $\{0_K\}$ et ne peut pas être vide.
3. Le triplet $(K,+,\cdot)$ est un corps si et seulement si $K \neq \{0_K\}$, $(K,+)$ est un groupe abélien, $(K^*,\cdot)$ est un groupe et la loi $\cdot$ est distributive sur la loi $+$.
4. Si la loi $\cdot$ est commutative, on dit que le corps est commutatif.

Nous convenons que $K^* = K \setminus \{0_K\}$.

Exemples

1. Le triplet $(\mathbb{Z},+,\times)$ n'est pas corps car par exemple, $\frac{1}{2}$ n'a pas d'inverse dans $\mathbb{Z}$.
2. Les triplets $(\mathbb{Q},+,\times)$, $(\mathbb{R},+,\times)$ et $(\mathbb{C},+,\times)$ sont des corps commutatifs.

La plupart des corps que nous rencontrerons seront commutatifs.

B Propriétés

Théorème 23

Tout corps est un anneau intègre.

Le **théorème 23** est une conséquence immédiate du **théorème 16** : tout élément non nul d'un corps est inversible et donc est régulier et donc, ne peut pas être un diviseur de zéro.

Remarques

1. Le lecteur cherchera pourquoi un produit d'anneaux intègres n'est jamais intègre.
2. Le lecteur cherchera aussi pour un produit de corps n'est jamais un corps.
3. La réciproque du **théorème 23** est évidemment faux. En effet, $(\mathbb{Z},+,\times)$ est un anneau intègre mais pas un corps.

Un anneau intègre n'est pas systématiquement un corps, mais :

Théorème 24

Soit $(A,+,\cdot)$ un anneau intègre.
Si l'anneau A est fini, alors A est un corps.

Autrement dit, tout anneau intègre fini est un corps.

Preuve

Il suffit de montrer que tout élément non nul admet un inverse dans A.
Soit alors un élément a non nul de A.
Considérons les translations γ_a et δ_a.
Puisque l'anneau A est intègre, a est régulier (**théorème 17**) et donc les applications γ_a et δ_a sont injectives.
Puisque A est un ensemble fini, ces applications sont même bijectives.
Il vient alors que les équations d'inconnue x dans A : $ax = 1_A$ et $xa = 1_A$ admettent respectivement b et b' comme unique solution.
Enfin, comme le couple $(A,\cdot)$ est un monoïde, les éléments b et b' sont égaux.
Finalement a admet bien un inverse dans A et ce dernier et un corps. □

Rappelons que dans un monoïde, si un élément admet un symétrique à gauche et à droite, alors ils sont égaux.

Le théorème suivant est dû au mathématicien écossais **Joseph Wedderburn** (1882-1948). La démonstration du théorème nécessite des connaissances de licence 3 minimum, même si son énoncé est très simple.
Nous admettons ce théorème.

Le lecteur averti pourra consulter une démonstration de ce théorème au **chapitre 00** du livre d'algèbre niveau licence 3.

Théorème 25 **Théorème de Wedderburn**

Tout corps fini est commutatif.

Donc un corps non commutatif est nécessairement infini.

Le cours du chapitre 5

C Sous-corps

Définition 8

Soient $(K, +, \cdot)$ un corps et L un sous-ensemble de K.

Dire que L est un **sous-corps** de K signifie que :

1) L est un sous-anneau de $(K, +, \cdot)$ 2) $\forall x \in L \setminus \{0_L\}, x^{-1} \in L$.

Exemple

$\mathbb{Q}$ est un sous-corps de $(\mathbb{R}, +, \times)$.

Théorème 26 **Caractérisation des sous-corps**

Soient $(K, +, \cdot)$ un corps et L un sous-ensemble de K.

Le sous-ensemble L est un sous-corps de K si et seulement si :

1) L est stable pour les lois $+$ et $\cdot$ 2) L est un corps pour les lois $+$ et $\cdot$.

La démonstration du **théorème 26** est immédiate.

Les exercices du chapitre 5

1 Anneau et groupe

Soit $(A,+,\cdot)$ un anneau commutatif.

On note E l'ensemble des éléments idempotents de A.

Montrer que E est un groupe commutatif pour la loi $*$ définie par :

$$\forall (x,y)\in E^2, x*y=x+y-2xy\,.$$

2 Calcul dans un anneau

Soient $(A,+,\cdot)$ un anneau, x et y deux éléments de A tels que :

$$xy+yx=1_A \text{ et } x^2y+yx^2=x\,.$$

1) Montrer que $x^2y=yx^2$ et $2xyx=x$.

2) Etablir que x est inversible et que son inverse est $2y$.

3 Calcul dans un anneau

Soit $(A,+,\cdot)$ un anneau tel que :

$$\forall (x,y)\in A^2, (xy)^2=x^2y^2\,.$$

1) Montrer que :

$$\forall (x,y)\in A^2, xyx=x^2y=yx^2\,.$$

2) En déduire que A est commutatif.

4 ★★ Calcul dans un pseudo-anneau

Soient $(A,+,\cdot)$ un pseudo-anneau fini, x et y des éléments de A tel que $xy^2=y$.

Montrer que $yxy=y$.

5 Nilpotence et idempotence dans un pseudo-anneau

Soit $(A,+,\cdot)$ un pseudo-anneau sans élément nilpotent autre que 0_A.

On suppose que :

$$\forall (x,y)\in A^2, xy(x+y)=0_A\,.$$

Etablir que tous les éléments de A sont idempotents.

6 Calcul dans un pseudo-anneau

Soit $(A,+,\cdot)$ un pseudo-anneau tel que :

$$\forall (x,y)\in A^2, (xy)^2=xy\,.$$

1) Montrer que :

$$\forall (x,y,z)\in A^3, xyxz+xzxy=yxzx+zxyx=0_A\,.$$

Soient α et β deux éléments idempotents de A.

2) Montrer que $\alpha\beta=\beta\alpha$ et $2\alpha\beta=0_A$.

3) En déduire que :

$$\forall (x,y,z,t)\in A^4, xyzt=ztxy\,.$$

4) Montrer que, si α est un élément idempotent de A, alors :

$$\forall x\in A, \alpha x\alpha=x\alpha=\alpha x\,.$$

7 Calcul dans un pseudo-anneau

Soit $(A,+,\cdot)$ un pseudo-anneau tel que :

$$\forall x\in A, x^6=x\,.$$

Montrer que :

$$\forall x\in A, 2x=0_A\,.$$

8 Inverse dans un anneau

Soient $(A,+,\cdot)$ un anneau et a un élément de A.

On suppose qu'il existe un unique élément a' de A tel que $aa'=1_A$.

1) Montrer que a est régulier à gauche.

2) En déduire que a est inversible et que son inverse vaut a'.

9 Inverse dans un anneau

Soient $(A,+,\cdot)$ un anneau et U l'ensemble des éléments inversibles de l'anneau A.

Montrer que :

$$\forall (x,y)\in A^2, 1-xy\in U \Leftrightarrow 1-yx\in U\,.$$

10 Diviseur de zéro dans un anneau

Soient $(A,+,\cdot)$ un pseudo-anneau commutatif et D l'ensemble des diviseurs de zéro dans A.

Montrer que l'ensemble $\complement_A D$ est stable pour $\cdot$.

11 Inverse dans un anneau

Soient $(A,+,\cdot)$ un anneau, x et y deux éléments de A tels que xy soit inversible et que yx ne soit pas un diviseur de zéro.

Montrer que x et y sont inversibles.

12 Nilpotence dans un anneau 🖫

Soient $(A,+,\cdot)$ un pseudo-anneau, x et y deux éléments de A.

Montrer que si xy est nilpotent, alors yx est aussi nilpotent.

13 Nilpotence dans un anneau 🖫

Soient $(A,+,\cdot)$ un anneau et x un élément nilpotent de A.

Montrer que 1_A-x est inversible et calculer son inverse.

14 Sous-pseudo-anneau

Soient $(A,+,\cdot)$ un pseudo-anneau et X un sous-ensemble de A.

On note $C(X)$ le commutant de X dans A.

Vérifier que $C(X)$ est un sous-pseudo-anneau de A.

Un sous-pseudo-anneau est un pseudo-anneau pour les lois induites.

15 Sous-pseudo-anneau

Soient $(A,+,\cdot)$ un pseudo-anneau et e un élément idempotent de A.

Montrer que l'ensemble eAe est un sous-pseudo-anneau unitaire de A.

16 Diviseur de zéro dans un anneau

Soit $(A,+,\cdot)$ un pseudo-anneau non nul tel qu'il existe un élément a de A pour lequel, quel que soit l'élément b de A, l'une des deux équations $ax=b$ et $xa=b$ admet une solution x de A.

Montrer que, si A n'a pas de diviseur de zéro, alors A est un anneau.

17 Axiome faible de la structure d'anneau 🖫

Soit $(A,+,\cdot)$ un pseudo-anneau fini admettant un élément qui n'est pas un diviseur de zéro.

Montrer que A est un anneau.

18 Anneau commutatif

Dans un anneau $(A,+,\cdot)$, on suppose que :

$$\forall (x,y)\in A^2, (x^2-x)y=y(x^2-x)\,.$$

1) Montrer que :

$$\forall (x,y,z)\in A^3, (xy+yx)z=z(xy+yx)\,.$$

2) Montrer que A est un anneau commutatif.

19 ★ Anneau commutatif 🖫

Soient $(A,+,\cdot)$ un anneau et x un élément de A qui admet un inverse à gauche (resp. à droite).

Montrer que x est inversible si et seulement si x admet un unique inverse à gauche (resp. à droite).

Les exercices du chapitre 5

20 ★ **Anneau et centre** 🖫

Soient $(A,+,\cdot)$ un anneau, sans élément nilpotent (autre que 0_A) et x un élément idempotent de A.

Montrer que x est un élément central dans A.

21 **Anneau commutatif**

Soient $(A,+,\cdot)$ un anneau commutatif et e un élément idempotent de A qui n'est ni nul ni égal à 1_A.

On note B l'ensemble eA et C l'ensemble $(1-e)A$.

1) a) Montrer que B est stable pour les lois $+$ et $\cdot$.

b) Montrer que le triplet $(B,+,\cdot)$ est un anneau.

c) C est-il aussi un anneau pour les lois induites $+$ et $\cdot$?

2) Montrer que $B\cap C=\{0_A\}$.

3) Montrer que :

$$\forall x\in A,\exists!(y,z)\in B\times C,\ x=y+z\,.$$

22 **Inverse dans un anneau**

Soient $(A,+,\cdot)$ un anneau commutatif, x et y deux éléments de A.

On suppose que x, y et $xy-1$ sont inversible dans A.

On note $z=xy-1$ et $t=x^{-1}-(x-y^{-1})^{-1}$.

1) Montrer que $x-y^{-1}$ est inversible dans A et que $(x-y^{-1})^{-1}$ est égal à yz^{-1}.

2) Montrer que t est inversible dans A d'inverse $-zx$.

23 **Anneau et sous-anneau**

On définit sur $\mathbb{Z}^2$ deux lois internes notées $+$ et $\cdot$ par :

$$\forall (a,b),(c,d)\in\mathbb{Z}^2\times\mathbb{Z}^2,\begin{cases}(a,b)+(c,d)=(a+c,b+d)\\(a,b)\cdot(c,d)=(ac,ad+bc)\end{cases}.$$

1) Montrer que $(\mathbb{Z}^2,+,\cdot)$ est un anneau commutatif.

2) Montrer que l'ensemble $\{(a,0),a\in\mathbb{Z}\}$ est un sous-anneau de $\mathbb{Z}^2$.

24 **Anneau commutatif**

Soient E un ensemble et X une partie de E.

1) a) Montrer que le triplet $(\mathcal{P}(E),\Delta,\cap)$ est un anneau commutatif.

b) Cet anneau est-il intègre ? Quels sont les éléments inversibles ?

2) Montrer que l'ensemble $\{\varnothing,X,\overline{X},E\}$ est un sous-anneau de $\mathcal{P}(E)$.

25 **Pseudo-anneau et centre**

Soit $(A,+,\cdot)$ un pseudo-anneau tel que :

$$\forall x\in A,x^2-x\in\mathcal{Z}(A)\,.$$

1) Montrer que :

$$\forall (x,y)\in A^2,xy+yx\in\mathcal{Z}(A)\,.$$

2) En déduire que :

$$\forall (x,y)\in A^2,xy=yx\,.$$

26 **Ensemble des endomorphismes d'un groupe** 🖫

Soient $(G,+)$ un groupe commutatif et soit E l'ensemble des endomorphismes du groupe G.

Pour tout couple (Φ,ψ) de E^2, on définit l'application $\Phi+\psi$ par :

$$\forall x\in G,(\Phi+\psi)(x)=\Phi(x)+\psi(x)\,.$$

1) Montrer que la loi $+$ est interne dans E et que $(E,+)$ est un groupe commutatif.

2) Montrer que $(E,+,\circ)$ est un anneau.

27 **Anneau commutatif**

1) Montrer que $\mathbb{R}^2$ muni des lois suivantes $\oplus$ et $\odot$ définies par :

$$\forall (x_1,y_1),(x_2,y_2)\in\mathbb{R}^2\times\mathbb{R}^2,\begin{cases}(x_1,y_1)\oplus(x_2,y_2)=(x_1+x_2,y_1+y_2)\\(x_1,y_1)\odot(x_2,y_2)=(x_1x_2,x_1y_2+y_1x_2)\end{cases},$$

est un anneau commutatif.

2) Résoudre dans $\mathbb{R}^2$ les équations suivantes d'inconnue X :

a) $X^2=X$ b) $X^2=0_{\mathbb{R}^2}$ c) $X^2=1_{\mathbb{R}^2}$.

3) Montrer que l'anneau $\mathbb{R}^2$ n'est pas intègre.

4) Déterminer l'ensemble des éléments inversibles de $\mathbb{R}^2$.

Soit un couple $(n,X)\in\mathbb{N}^*\times\mathbb{R}^2$.

5) Calculer de deux manières différentes X^n.

28 **Anneau de Boole** 🖫

Soit $(A,+,\cdot)$ un anneau (non nul) dans lequel tous les éléments sont idempotents.

1) Donner un exemple d'un tel anneau (appelé **anneau de Boole**).

2) Montrer que pour tout x de A, $2x=0_A$ et en déduire que A est commutatif.

3) Montrer que A ne peut pas se réduire à trois éléments.

Soit $\preccurlyeq$ la relation définie sur A par :

$$\forall (x,y)\in A^2,x\preccurlyeq y\Leftrightarrow yx=x\,.$$

4) Montrer que $\preccurlyeq$ est une relation d'ordre sur A.

5) a) Montrer que :

$$\forall (x,y)\in A^2,xy(x+y)=0_A\,.$$

b) En déduire que si A admet au moins quatre éléments, alors A admet des diviseurs de zéro.

6) Montrer que :

$$\forall (x,y,z)\in A^3,(x+y)z=0_A\Leftrightarrow\begin{cases}x(y+1_A)z=0_A\\(x+1_A)yz=0_A\end{cases}.$$

George Boole (1815-1864) était un mathématicien britannique.

29 **Anneau des applications** 🖫

On considère l'anneau $(\mathbb{R}^{\mathbb{R}},+,\times)$ des applications de $\mathbb{R}$ dans $\mathbb{R}$.

1) Cet anneau est-il intègre ?

2) Déterminer les éléments inversibles de $\mathbb{R}^{\mathbb{R}}$.

3) Déterminer les fonctions applications continues vérifiant $f^2=1_{\mathbb{R}^{\mathbb{R}}}$, puis celle vérifiant $f^2=f$ (où $f^2=f\times f$).

4) Montrer que $(\mathbb{R}^{\mathbb{R}},+,\circ)$ n'est pas un anneau.

30 ★ **Nilpotence**

Soient $(A,+,\cdot)$ un anneau et a un élément de A.

On pose :

$$\forall x\in A,\Phi(x)=ax-xa\,.$$

Montrer que si a est nilpotent, alors Φ est nilpotente dans l'anneau des endomorphismes du groupe $(A,+)$.

31 **Anneau des nombres décimaux**

Soit $\mathbb{D}$ l'ensemble des nombres décimaux.

1) Ecrire cet ensemble en extension.

2) Vérifier que $\mathbb{D}$ contient $\mathbb{Z}$.

3) Montrer que $\mathbb{D}$ est un sous-anneau de $(\mathbb{Q},+,\times)$.

4) Montrer que $\mathbb{D}^\times=\left\{\pm\dfrac{2^p5^q}{10^n},(p,q,n)\in\mathbb{N}^3\right\}$.

Les exercices du chapitre 5

32 **Ensemble des éléments inversibles dans un anneau**

Soient $(A,+,\cdot)$ un anneau et B un sous-anneau de A.

1) Montrer que $B^\times$ est inclus dans $A^\times \cap B$.

2) Montrer à l'aide d'un exemple que $A^\times \cap B$ n'est pas nécessairement inclus dans $B^\times$.

33 **Sous-anneau**

Soit d un entier naturel.

On note :

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

Montrer que $\mathbb{Z}[\sqrt{d}]$ est un sous-anneau de $(\mathbb{R},+,\times)$.

34 **Sous-anneau**

Soit A l'ensemble défini par l'égalité :

$$A = \left\{\frac{m}{n}, (m,n) \in \mathbb{Z}\times\mathbb{N}^*, n \text{ impair}\right\}.$$

1) Montrer que A est sous-anneau de $(\mathbb{Q},+,\times)$.

2) Quels en sont les éléments inversibles ?

35 **Nombres dyadiques** 🖫

Soit A l'ensemble défini par l'égalité :

$$A = \left\{\frac{m}{2^n}, (m,n) \in \mathbb{Z}\times\mathbb{N}\right\}.$$

1) Montrer que A est un sous-anneau de $(\mathbb{Q},+,\times)$.

2) Quels en sont les éléments inversibles ?

On dit que A est l'ensembles des nombres dyadiques.

36 **Calcul dans un anneau**

Soient $(A,+,\cdot)$ un anneau, x et y deux éléments de A tels que :

$$xy + yx = 1_A \text{ et } x^2y + yx^2 = x.$$

1) Montrer que $x^2y = yx^2$ et $2xyx = x$.

2) Montrer que x est inversible d'inverse $2y$.

37 **Calcul dans un anneau**

Soient $(A,+,\cdot)$ un anneau où 0_A est le seul élément nilpotent et E l'ensemble de ses éléments idempotents.

1) Montrer que $E \subset \mathcal{Z}(A)$.

Soient x et y des éléments de A tels que $xyx = x$.

2) Montrer que xy et yx sont dans E et que $xy = yx$.

38 ★ **Inverse dans un anneau**

Soient $(A,+,\cdot)$ un anneau, x et y des éléments de A tels que $1-xy$ soit inversible.

Montrer que $1-yx$ est inversible et préciser son inverse.

39 **Calcul dans un corps**

Soient $(K,+,\cdot)$ un corps, x et y des éléments non nuls de K tel que :

$$x + y = 1_K \text{ et } x^{-1} + y^{-1} = 1_K.$$

Montrer que $xy = yx = 1_K$ et $x^6 = y^6 = 1_K$.

40 **Pseudo-anneau intègre et fini** 🖫

Montrer que tout pseudo-anneau intègre et fini est un corps.

41 **Sous-corps de Q** 🖫

Déterminer tous les sous-corps de $(\mathbb{Q},+,\times)$.

42 **Sous-groupe et sous-corps**

Soient $(K,+,\cdot)$ un corps commutatif et G l'ensemble des automorphismes de K.

Soient $\varphi : \mathcal{P}(K) \longrightarrow \mathcal{P}(G)$ et $\psi : \mathcal{P}(G) \longrightarrow \mathcal{P}(K)$ les applications définies par :

$$\forall A \in \mathcal{P}(K), \varphi(A) = \{g \in G, \forall x \in A, g(x) = x\} \ ;$$
$$\forall B \in \mathcal{P}(G), \psi(B) = \{x \in K, \forall g \in B, g(x) = x\}.$$

1) Vérifier que $(G,\circ)$ est un groupe.

2) a) Montrer que, pour tout $A \in \mathcal{P}(K)$, $\varphi(A)$ est un sous-groupe de G.

b) Montrer que, pour tout $B \in \mathcal{P}(G)$, $\psi(B)$ est un sous-corps de K.

3) a) Vérifier que :

$$\forall A \in \mathcal{P}(K), A \subset (\psi\circ\varphi)(A).$$

b) Vérifier que :

$$\forall B \in \mathcal{P}(G), B \subset (\varphi\circ\psi)(B).$$

4) Etablir que $\varphi\circ\psi\circ\varphi = \varphi$ et $\psi\circ\varphi\circ\psi = \psi$.

43 ★ **Du pseudo-anneau au corps**

Soit $(A,+,\cdot)$ un pseudo-anneau.

On définit dans A une loi de composition interne $*$ par :

$$\forall (x,y) \in A^2, x * y = x + y - xy.$$

1) Montrer que la loi $*$ est associative et admet un neutre.

On suppose qu'il existe un élément e de A unique tel que :

$$\forall x \in A, e * x \neq 0_A.$$

2) Montrer que :

a) $e \neq 0_A$ b) $\forall x \in A, e * x = e$ c) $\forall x \in A, \begin{cases} x * e \neq 0_A \\ x * e = e \end{cases}$.

3) En déduire que $(A,+,\cdot)$ est un corps.

44 **Calcul dans un corps**

Soit $(K,+,\cdot)$ un corps, x et y des éléments non nuls de K tels que :

$$x + y = -1_K \text{ et } x^{-1} + y^{-1} = 1_K.$$

Montrer que $xy = -1_K$ et $x^4 + y^4 = 7$.

45 **Sous-anneau de Q**

Soit p un nombre premier.

On considère l'ensemble A_p défini par l'égalité :

$$A_p = \left\{x \in \mathbb{Q}, \exists (a,b) \in \mathbb{Z}\times\mathbb{N}^*, \left(x = \frac{a}{b}\right) \wedge (p \nmid b)\right\}.$$

1) Montrer que A_p est un sous-anneau de $(\mathbb{Q},+,\times)$.

2) Est-ce que A_p est un sous-corps de $(\mathbb{Q},+,\times)$?

46 ★ **Sous-corps de C**

Soit un couple $(p,q) \in \mathbb{Q}\times\mathbb{Q}^*$ tel que l'équation :

$$(E) \ : \ x^2 - px - q = 0,$$

n'a pas de racine dans $\mathbb{Q}$.

Soit α une racine de l'équation (E). On désigne par $\mathbb{Q}[\alpha]$ l'ensemble :

$$\{a + b\alpha, (a,b) \in \mathbb{Q}^2\}.$$

1) Vérifier que si z appartient à $\mathbb{Q}[\alpha]$, il existe un unique couple (a,b) de $\mathbb{Q}^2$ tel que $z = a + b\alpha$.

2) Vérifier que $\mathbb{Q}[\alpha]$ est un sous-anneau de $(\mathbb{C},+,\times)$ qui contient $\mathbb{Q}$.

3) Montrer que α est inversible dans $\mathbb{Q}[\alpha]$.

4) En déduire que $\mathbb{Q}[\alpha]$ est un sous-corps de $(\mathbb{C},+,\times)$.

Les exercices du chapitre 5

47 ★ **Calcul dans un corps fini**

Soit $(K,+,\cdot)$ un corps fini.

Calculer le produit des éléments inversibles de K.

48 **Sous-corps de R**

Montrer que $\mathbb{Q}$ est le plus petit sous-corps de $(\mathbb{R},+,\times)$.

49 **Sous-corps de R**

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

Montrer que $\mathbb{Q}[\sqrt{2}]$ est un sous-corps de $(\mathbb{R},+,\times)$.

50 ★ **Anneau commutatif** 🖫

Soit $(A,+,\cdot)$ un anneau tel que :

$$\forall x\in A, x^3=x\,.$$

1) Déterminer les éléments nilpotents de A.

Soit e un élément de A tel que $e^2=e$, $a\in A$ et $b=ea(1-e)$.

2) a) Calculer b^2.

b) En déduire que $ea=ae$.

c) En déduire que :

$$\forall x\in A, x^2\in\mathcal{Z}(A)\,.$$

3) Montrer que l'anneau A est commutatif.

D'après ENS 2004.

51 ★★ **Anneau commutatif et anticommutatif**

Soit $(A,+,\cdot)$ un pseudo-anneau tel que :

$$\forall (x,y)\in A^2, yx\in\{xy,-xy\}\,.$$

Dire que l'anneau A est **anticommutatif** signifie que :

$$\forall (x,y)\in A^2, xy=-yx\,.$$

1) Montrer que A est commutatif ou anti-commutatif.

2) Que dire si A et un anneau ?

D'après ENS 2006.

52 **Sous-corps de C**

On pose $\mathbb{Q}[i]=\{x+iy,(x,y)\in\mathbb{Q}^2\}$.

Montrer que $\mathbb{Q}[i]$ est un sous-corps de $(\mathbb{C},+,\times)$.

Problèmes du chapitre 5

Le premier problème traite de deux pseudo-anneaux particuliers.
Le second problème traite de la dérivation... dans un anneau !

Problème I ★ Pseudo-anneaux particuliers

Soient $(A,+,\cdot)$ un pseudo-anneau, $\mathcal{Z}(A)$ son centre et $E(A)$ l'ensemble des éléments idempotents de A.

Partie I – Premier pseudo-anneau

Dans cette partie seulement, on suppose que :

$$\forall (x,y)\in A^2,\ xy\in E(A)\,.$$

1) a) Montrer que :

$$\forall (x,y)\in A^2,\ xy=0_A \Rightarrow yx=0_A\,.$$

b) En déduire que $E(A)\subset\mathcal{Z}(A)$.

2) Montrer que A est commutatif.

Partie II – Second pseudo-anneau

Dans cette partie seulement, on suppose que :

$$\forall (x,y)\in A^2,\ xy-yx\in E(A)\,.$$

3) a) Montrer que :

$$\forall (x,y)\in A^2,\ xy=0_A \Rightarrow yx=0_A\,.$$

b) En déduire que $E(A)\subset\mathcal{Z}(A)$.

4) Prouver que :

$$\forall (x,y)\in A^2,\ xy-yx=yx-xy\,.$$

5) En déduire que :

$$\forall x\in A,\ x^2\in\mathcal{Z}(A)\,.$$

6) Démontrer que :

$$\forall (x,y)\in A^2,\ (xy)^2=(yx)^2\,.$$

7) En déduire que A est commutatif.

Problème II ★ Dérivation dans un anneau

Soient $(A,+,\cdot)$ un anneau.

On appelle **dérivation** sur A toute application δ de A dans A tel que :

$$\forall (x,y)\in A^2,\ \begin{cases}\delta(x+y)=\delta(x)+\delta(y)\\ \delta(xy)=x\delta(y)+\delta(x)y\end{cases}.$$

Partie I – Crochet de Lie et exemple de dérivation

Sophus Lie (1842-1899) était un mathématicien norvégien.

Pour a et b dans A, on pose $[a,b]=ab-ba$.

1) Que vaut $[a,b]$ lorsque a et b commutent ?

Soient a, b et c des éléments de A.

2) a) Former une relation liant $[a,b]$ et $[b,a]$.

b) Etablir que $[a,b+c]=[a,b]+[a,c]$.

c) Montrer que $[a,[b,c]]+[b,[c,a]]+[c,[a,b]]=0_A$.

Charles Gustave Jacob Jacobi (1804-1851) était un mathématicien allemand.

Cette dernière relation est connue sous le nom d'**identité de Jacobi**.

Pour a un élément de A, on considère l'application d_a de A dans A définie par :

$$\forall x\in A,\ d_a(x)=ax-xa\,.$$

3) Montrer que d_a est une dérivation sur A.

Partie II – Propriétés des dérivations

Soit δ une dérivation sur A.

1) Calculer $\delta(0)$ et $\delta(1)$.

Soit x un élément de l'anneau A.

2) a) Exprimer $\delta(-x)$ en fonction de $\delta(x)$.

On suppose que x est inversible.

b) Exprimer $\delta(x^{-1})$ en fonction de $\delta(x)$ et de x^{-1}.

Soient $n \in \mathbb{N}^*$ et $(x_1, ..., x_n) \in A^n$.

3) a) Exprimer $\delta(x_1 x_2 ... x_n)$ en fonctions des x_k et des $\delta(x_k)$ pour $k \in \{1, ..., n\}$.

Soit x un élément de l'anneau A.

b) Exprimer l'élément $\delta(x^n)$.

c) Que devient cette formule si x et $\delta(x)$ commutent ?

Soit $C_\delta = \{x \in A, \delta(x) = 0_A\}$.

4) a) Montrer que C_δ est un sous-anneau de $(A, +, \cdot)$.

b) Montrer que si l'anneau A est un corps, alors C_δ est un sous-corps de $(A, +, \cdot)$.

Partie III – Manipulation de dérivations

Soient δ_1 et δ_2 deux dérivations sur A.

1) a) Peut-on affirmer que l'application $\delta_1 + \delta_2$ est une dérivation sur A ?

b) Peut-on affirmer que l'application $\delta_1 \circ \delta_2$ est une dérivation sur A ?

On note $[\delta_1, \delta_2] = \delta_1 \circ \delta_2 - \delta_2 \circ \delta_1$.

c) Montrer que $[\delta_1, \delta_2]$ est une dérivation sur A.

Soient δ une dérivation sur A, a et b deux élément de A.

2) a) Montrer que $[\delta, d_a] = d_{\delta(a)}$.

b) Montrer que $[d_a, d_b] = d_{[a,b]}$.