# Cours d'Algèbre 6
# Filière SMA
# Année 2020-2021

Mme F. ERRAJI, Pr.

17 mai 2021

# Table des matières

**Avant-Propos** **i**

**i**

**3 Anneaux et Corps** **1**

I Rappels et Préliminaires . . . . . 1

I.1 Généralités sur les Anneaux . . . . . 1

I.2 Anneaux Produits . . . . . 4

I.3 Sous-Anneaux . . . . . 5

I.4 Homomorphismes d'Anneaux . . . . . 6

II Idéaux . . . . . 8

II.1 Notion d'Idéal . . . . . 8

II.2 Idéal Engendré par une Partie - Idéal Principal . . . . . 9

II.3 Somme et Produit d'Idéaux . . . . . 10

II.4 Idéaux Premiers et Maximaux . . . . . 11

# Chapitre 3

# Anneaux et Corps

## I Rappels et Préliminaires

### I.1 Généralités sur les Anneaux

**Définition I.1.1.** *Un anneau est un ensemble $A$ muni de deux lois de composition internes, l'une, notée comme une addition (additivement), l'autre, comme une multiplication (multiplicativement), vérifiant les propriétés suivantes :*

- *(i) $(A, +)$ est un groupe abélien,*
- *(ii) la multiplication "$\cdot$" est associative,*
- *(iii) la multiplication est distributive (à gauche et à droite) par rapport à l'addition, i.e. $x(y+z) = xy + xz$ et $(x+y)z = xz + yz$ pour tous $x, y, z \in A$.*

*L'anneau est dit commutatif si de plus la multiplication est commutative.*

*L'anneau est dit unitaire (ou unifère) lorsque $A$ admet un élément neutre pour la multiplication, distinct de son élément neutre pour l'addition. Noter qu'un anneau unitaire admet au moins deux éléments.*

**Notation**

L'élément neutre de $+$ sera noté $0_A$ ou tout simplement $0$ et est appelé élément nul. L'élément neutre de la multiplication, s'il existe, sera noté $1_A$ ou tout simplement $1$ et est appelé élément unité.

**Exemples.**

- *L'ensemble $\{0\}$, muni des lois $0+0=0$ et $0\cdot 0 = 0$ est un anneau appelé anneau nul. Cet anneau n'est pas unitaire car $0_A = 1_A$.*
- *$(\mathbb{Z}, +, \cdot)$ est un anneau commutatif unitaire. Il en est de même de $\mathbb{Q}, \mathbb{R}$ et de $\mathbb{C}$.*
- *L'ensemble des matrices carréees d'ordre $n \geq 2$ à coefficients réels, muni de l'addition et de la multiplication est un anneau non commutatif unitaire ($1 = I_n$).*

— *Soit* $(G,+)$ *un groupe abélien.* $(End(G),+,\circ)$ *est un anneau unitaire* $(1 = Id_G)$ *non commutatif.*

— $(A,+,\cdot)$ *est un anneau (commutatif, unitaire) et* $X$ *un ensemble non vide quelconque. L'ensemble* $\mathcal{F}(X,A)$ *des applications de* $X$ *dans* $A$ *muni des lois* $+$ *et* $\cdot$ *définies comme suit :*

$\forall f,g \in \mathcal{F}(X,A), \forall x \in X, \quad (f+g)(x) = f(x)+g(x)$ *et* $(f\cdot g)(x) = f(x)\cdot g(x)$

$(\mathcal{F}(X,A),+,\cdot)$ *est un anneau (commutatif, unitaire). En particulier, l'ensemble des suites réelles,* $(\mathcal{F}(\mathbb{N},\mathbb{R}),+,\cdot)$*, est un anneau commutatif unitaire.*

— *Soit* $n \geq 2$*.* $(\mathbb{Z}/n\mathbb{Z},+)$ *est un groupe abélien. On définit une multiplication dans* $\mathbb{Z}/n\mathbb{Z}$ *à partir de celle de* $\mathbb{Z}$ *en posant* $\overline{x}\,\overline{y} = \overline{x\,y}, \quad \forall \overline{x},\overline{y} \in \mathbb{Z}/n\mathbb{Z}$*.*

*Cette multiplication est bien définie (la congruence est compatible avec la multiplication), commutative, associative et distributive par rapport à* $+$*, et* $\overline{1}$ *est l'élément unité pour "*$\cdot$*". On conclut que* $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ *est un anneau commutatif unitaire.*

**Calcul dans un Anneau**

Dans un anneau $(A,+,\cdot)$ quelconque. On a les propriétés suivantes :

— $\forall a \in A, \quad a\cdot 0_A = 0_A = 0_A\cdot a$

— $\forall a,b \in A, \quad a(-b) = -(ab) = (-a)b$

— $\forall a,b \in A, \quad (-a)(-b) = ab$

— $\forall a \in A, \forall n \in \mathbb{N}^*$, on définit $a^n$ par récurrence : $a^1 = a$ et $a^n = a^{n-1}a$. On a alors, $\forall m,n \in \mathbb{N}^*, \quad a^{m+n} = a^m\cdot a^n$ et $(a^m)^n = a^{m\cdot n}$. Si $A$ est unitaire, on définit de plus $a^0 = 1$ et les formules ci-dessus restent valables pour tous $n,m \in \mathbb{N}$.

— $(A,+)$ étant un groupe abélien, on rappelle qu'on a déjà défini $\forall k \in \mathbb{Z}, \forall a \in A$ le symbole $k\cdot a$ et on a $\forall k,p \in \mathbb{Z}, \forall a \in A$ :

$$\begin{aligned}(k+p)a &= k\cdot a + p\cdot a\\ (k\cdot p)a &= k(p\cdot a)\end{aligned}$$

**Théorème I.1.** *Soit* $(A,+,\cdot)$ *un anneau unitaire. Pour tous* $x,y \in A$ *tels que* $x\cdot y = y\cdot x$ *et pour tout* $n \in \mathbb{N}^*$*, on a les formules suivantes :*

$$(*) \quad (x+y)^n = \sum_{p=0}^{n} \mathsf{C}_n^p x^{n-p}y^p \quad \text{où} \quad \mathsf{C}_n^p = \frac{n!}{p!(n-p)!} \quad \textit{(formule du binôme)}$$

$$(**) \quad x^n - y^n = (x-y)\Big(\sum_{p=0}^{n-1} x^{n-1-p}\,y^p\Big)$$

*En particulier :*

$$x^n - 1_A = (x-1_A)(1_A + x + x^2 + \cdots + x^{n-1})$$

La preuve de $(*)$ se fait par récurrence su $n$ et en utilisant la formule $\complement_n^p = \complement_{n-1}^{p-1} + \complement_{n-1}^p, \quad \forall n, p \in \mathbb{N}^*$.

### Eléments Inversibles

**Définition I.1.2.** *Soit $(A, +, \cdot)$ un anneau unitaire. Un élément $x \in A$ est dit inversible s'il est inversible pour la loi multiplicative dans $A$, i.e. s'il existe un élément $y \in A$ tel que $x \cdot y = y \cdot x = 1$.*

*L'ensemble des éléments inversibles de $A$ est noté $\mathcal{U}(A)$.*

**Remarques.** — *$1_A$ est inversible.*

— *$0_A$ n'est pas inversible.*

— *Tout élément inversible de $A$ est régulier pour "$\cdot$".*

**Proposition I.1.1.** *Soit $(A, +, \cdot)$ un anneau unitaire. Alors $\mathcal{U}(A)$ est stable pour la multiplication dans $A$ et $(\mathcal{U}(A), \cdot)$ est un groupe d'élément neutre $1_A$. On l'appelle groupe des unités de $A$.*

**Preuve.** $\forall x, y \in \mathcal{U}(A), \quad x^{-1}$ *et* $y^{-1}$ *existent et* $(xy)(y^{-1}x^{-1}) = 1_A = (y^{-1}x^{-1})(xy)$, *donc* $x \cdot y \in \mathcal{U}(A)$.

— *L'associativité de "$\cdot$" dans $\mathcal{U}(A)$ découle de l'associativité de "$\cdot$" dans $A$.*

— $1_A \in \mathcal{U}(A)$ *et* $\forall x \in \mathcal{U}(A), \quad x \cdot 1_A = 1_A \cdot x = x$

— $\forall x \in \mathcal{U}(A), \quad \exists x_1 = x^{-1} \in A$ *tel que* $xx^{-1} = x^{-1}x = 1_A$ *donc* $x^{-1} \in \mathcal{U}(A)$. *Ainsi, $x$ est symétrisable dans $(\mathcal{U}(A), \cdot)$.*■

**Exemples.** — $\mathcal{U}(\mathbb{Z}) = \{-1, 1\}$.

— $\mathcal{U}(\mathbb{Q}) = \mathbb{Q} \setminus \{0\} = \mathbb{Q}^*$.

— *Soit $n \geq 2$. Montrer que* $\mathcal{U}(\mathbb{Z}/n\mathbb{Z}) = \{\overline{x} \in \mathbb{Z}/n\mathbb{Z} \ / x \text{ est premier avec } n\}$.

**Définition I.1.3.** *On appelle Corps (resp. corps commutatif), tout anneau unitaire (resp. anneau unitaire commutatif) dans lequel tout élément non nul est inversible.*

**Remarque.** — *Soit $A$ un anneau unitaire. $A$ est un corps si et seulement si $\mathcal{U}(A) = A \setminus \{0_A\}$.*

— $\forall n \geq 2$, *si $n$ est premier alors $\mathbb{Z}/n\mathbb{Z}$ est un corps.*

### Diviseurs de Zéro

**Définition I.1.4.** *Soit $A$ un anneau non nul. Un élément $x \in A$ est dit diviseur de zéro si $x \neq 0_A$ et s'il existe un élément $y \neq 0_A \in A$ tel que $xy = 0_A$ ou $yx = 0_A$.*

**Remarque.** *Pour tout élément $x$ non nul de $A$, $x$ est un diviseur de $0_A$ si et seulement si $x$ n'est pas régulier pour la loi "$\cdot$".*

**Définition I.1.5.** *Un anneau $A$ est dit intègre s'il est commutatif unitaire et ne contient aucun diviseur de zéro.*

**Remarque.** *Dans un anneau intègre, tout élément non nul est régulier pour la multiplication.*

**Proposition I.1.2.** *Soit $A$ un anneau commutatif unitaire. $A$ est intègre si et seulement si $\forall x, y \in A, \quad xy = 0_A \Rightarrow (x = 0_A \ \ ou \ \ y = 0_A)$.*

**Exemples.** — *$\mathbb{Z}$ est un anneau intègre.*

— *$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux intègres.*

— *$\mathbb{Z}/6\mathbb{Z}$ n'est pas intègre ($\overline{2}\,\overline{3} = \overline{0}$ et $\overline{2} \neq \overline{0}$, $\overline{3} \neq \overline{0}$).*

— *$(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \cdot)$ n'est pas intègre : soit*

$$f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{array}{ll} f(x) = x & si\ x \geq 0 \\ f(x) = 0 & si\ x < 0 \end{array} \end{array} \quad et \quad g : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{array}{ll} g(x) = 0 & si\ x \geq 0 \\ g(x) = x & si\ x < 0 \end{array} \end{array}$$

*On a $f \neq \theta$ et $g \neq \theta$ mais $f \cdot g = \theta$ où $\theta$ est l'application nulle de $\mathbb{R}$ vers $\mathbb{R}$.*

**Proposition I.1.3.** *Tout corps commutatif est un anneau intègre.*

**Preuve.** *Soit $\mathbb{K}$ un corps commutatif. $\mathbb{K}$ est alors un anneau commutatif unitaire. Soit $x, y \in \mathbb{K}$ tel que $xy = 0_{\mathbb{K}}$. Si $x \neq 0_{\mathbb{K}}$ alors $x$ est inversible dans $\mathbb{K}$ par définition d'un corps, donc $\quad x^{-1}xy = x^{-1}0_{\mathbb{K}}, \quad i.e.\ y = 0$.* ■

**Remarques.** — *La réciproque de la proposition n'est pas vraie : $\mathbb{Z}$ est un anneau intègre mais $\mathbb{Z}$ n'est pas un corps.*

— *Soit $n \geq 2$, si $n$ est premier alors $\mathbb{Z}/n\mathbb{Z}$ est intègre.*

## I.2 Anneaux Produits

**Proposition et Définition I.2.1.** *Soit $(A_i)_{i \in I}$ une famille d'anneaux. L'ensemble produit $\prod_{i \in I} A_i$ muni des lois suivantes :*

$$x + y = (x_i + y_i)_{i \in I} \quad et \quad xy = (x_i\, y_i)_{i \in I}, \quad \forall x = (x_i)_{i \in I} \in \prod_{i \in I} A_i\,, \forall y = (y_i)_{i \in I} \in \prod_{i \in I} A_i,$$

*est un anneau, dit anneau produit des $A_i$.*

*Si de plus $A_i$ est commutatif (resp. unitaire) pour tout $i \in I$, alors $\prod_{i \in I} A_i$ est commutatif (resp. unitaire, d'élément unité $1_{\prod A_i} = (1_{A_i})$).*

**Remarques.** — *Si tous les anneaux $A_i$ sont égaux à un même anneau $A$, l'anneau $\prod_{i\in I} A_i$, noté $A^I$ peut être identifié à l'anneau $\mathcal{F}(I,A)$.*

— *Si $I=\{1,2,3,\cdots,n\}$, $n\in\mathbb{N}^*$,*

$$\prod_{i\in I} A_i = \prod_{1\leq i\leq n} A_i = A_1\times A_2\times\cdots\times A_n, \quad x=(x_i)_{i\in I}=(x_1,x_2,\cdots,x_n).$$

— *Un produit $A_1\times A_2$ d'anneaux unitaires commutatifs n'est jamais intègre (même si $A_1$ et $A_2$ le sont, et même si ce sont des corps commutatifs). En effet, les éléments $(1_{A_1},0_{A_2})$ et $(0_{A_1},1_{A_2})$ sont non nuls alors que leur produit l'est.*

**Proposition I.2.1.** *Soit $A$ et $B$ deux anneaux unitaires. Alors $\mathcal{U}(A\times B)=\mathcal{U}(A)\times\mathcal{U}(B)$.*

**Preuve.** *Exercice.*

**Remarque.** *Le produit de deux corps n'est pas un corps.*

## I.3 Sous-Anneaux

**Définition I.3.1.** *Soit $(A,+,\cdot)$ un anneau et $B$ une partie de $A$. $B$ est dite sous-anneau de $A$, si $B$ est stable pour les lois $+$ et "$\cdot$" et si $(B,+,\cdot)$ est un anneau.*

Il est clair que si $A$ est un anneau commutatif, $B$ est aussi commutatif. Par contre, si $A$ est unitaire, $B$ n'est pas forcément unitaire. En effet, $\mathbb{Z}$ est un anneau unitaire mais $2\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}$ non unitaire. Il existe des sous-anneaux d'un anneau unitaire $A$ ayant un élément unité différent de celui de $A$. D'où la convention de définition suivante.

**Définition I.3.2.** *Soit $(A,+,\cdot)$ un anneau unitaire et $B$ une partie de $A$. $B$ est dite sous-anneau unitaire de $A$, si $B$ est stable pour les lois $+$ et "$\cdot$" et si $(B,+,\cdot)$ est un anneau unitaire d'élément unité $1_B=1_A$.*

**Proposition I.3.1.** *Soit $(A,+,\cdot)$ un anneau (**unitaire**) et $B$ une partie de $A$. $B$ est un sous-anneau (**unitaire**) de $A$ si et seulement si :*

— *(i) $B\neq\emptyset$*

— *(ii) $\forall x,y\in B,\quad x-y\in B$ et $xy\in B$*

— *(iii) $(\mathbf{1_A\in B})$*

**Preuve.** *Exercice.*

**Exemples.** — *$\{0_A\}$ et $A$ sont des sous-anneaux de l'anneau $A$.*

— *Les sous-anneaux de* $(\mathbb{Z},+,\cdot)$ *sont les* $n\mathbb{Z}$ *où* $n\in\mathbb{N}$. *L'unique sous-anneau unitaire de* $(\mathbb{Z},+,\cdot)$ *est* $\mathbb{Z}$.

— $\mathbb{Z}$ *est un sous-anneau unitaire de* $\mathbb{Q}$ *(de* $\mathbb{R}$ *et de* $\mathbb{C}$*).*

— *Soit* $(G,+)$ *un groupe.* $Aut(G)$ *est un sous-anneau unitaire de l'anneau* $(End(G),+,\circ)$.

— *Soit* $I$ *un intervalle de* $\mathbb{R}$. *Dans l'anneau* $(\mathcal{F}(I,\mathbb{R}),+,\cdot)$, *l'ensemble des fonctions continues forme un sous-anneau unitaire.*

— *L'intersection quelconque de sous-anneaux (unitaires) d'un anneau* $A$ *(unitaire) est aussi un sous-anneau (unitaire) de* $A$.

**Exercices 1.** *1. Soit* $\mathbb{Z}[i]=\{a+ib\,/a,b\in\mathbb{Z}\}$.

*(-) Montrer que* $\mathbb{Z}[i]$ *est un sous-anneau unitaire de* $(\mathbb{C},+,\cdot)$ *et que* $\mathbb{Z}$ *est un sous-anneau unitaire de* $\mathbb{Z}[i]$.

*(-) Montrer que* $\mathbb{Z}[i]$ *est intègre.*

*(-) Pour* $a,b\in\mathbb{Z}$, *on pose* $N(a+ib)=a^2+b^2$, *montrer que* $N(xy)=N(x)N(y)$, *pour tous* $x,y\in\mathbb{Z}[i]$ *et déterminer* $\mathcal{U}(\mathbb{Z}[i])$.

*(-) Conclure.*

*2. Soit* $(A,+,\cdot)$ *un anneau (unitaire). Montrer que* $Z(A)=\{x\in A\,/\forall a\in A, xa=ax\}$ *est un sous-anneau (unitaire) de* $A$.

**Définition I.3.3.** *Soit* $(\mathbb{K},+,\cdot)$ *un corps. On appelle sous-corps de* $\mathbb{K}$ *tout sous-anneau unitaire* $L$ *de* $\mathbb{K}$ *tel que l'inverse de tout élément non nul de* $L$ *appartient à* $L$.

**Exemples.** — $\mathbb{Q}$ *est un sous-corps de* $\mathbb{R}$.

— $\mathbb{Q}(i)=\{p+iq\,/p,q\in\mathbb{Q}\}$ *est un sous-corps de* $\mathbb{C}$ *:* $\mathbb{Z}[i]$ *est un sous-anneau unitaire de* $\mathbb{Q}[i]$, *et non pas un sous-corps de* $\mathbb{Q}[i]$.

## I.4 Homomorphismes d'Anneaux

**Définition I.4.1.** *Soit* $A$ *et* $B$ *deux anneaux. On appelle homomorphisme d'anneaux de* $A$ *dans* $B$ *toute application* $f:A\to B$ *vérifiant :* $\forall x,y\in A$

$$f(x+y)=f(x)+f(y)\quad ;\quad f(xy)=f(x)f(y)$$

**Remarque.** *Si* $A$ *et* $B$ *sont des anneaux unitaires et* $f$ *un homomorphisme d'anneaux de* $A$ *vers* $B$, *on n'a pas forcément* $f(1_A)=f(1_B)$. *En effet,*

— *soit* $f:A\to B$ *définie par* $f(x)=0_B$, $\forall x\in A$. $f$ *est un homomorphisme d'anneaux appelé homomorphisme nul (noté* $\theta$*). On a* $f(1_A)=0_B\neq 1_A$,

— *soit* $f:A\to A\times B$ *définie par* $f(a)=(a,0_B)$, $f$ *est un homomorphisme d'anneaux et* $f(1_A)=(1_A,0_B)\neq(1_A,1_B)$.

*Dans la suite, on convient la définition suivante :*

**Définition I.4.2.** *Si $A$ et $B$ deux anneaux unitaires. On appelle homomorphisme d'anneaux de $A$ dans $B$, soit l'homomorphisme nul, soit toute application $f : A \to B$ vérifiant les trois propriétés suivantes : $\forall x, y \in A$*

$f(x+y) = f(x) + f(y) \quad ; \quad f(xy) = f(x)f(y) \quad et \quad f(1_A) = 1_B$

*Si $K$ et $K'$ sont deux corps. Un homomorphisme de corps de $K$ dans $K'$ est un homomorphisme d'anneaux unitaires de $K$ dans $K'$.*

**Exemples.** — *$p : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ tel que $k \mapsto \overline{k}$ est un homomorphisme d'anneaux.*

— *Soit $A_1$ et $A_2$ deux anneaux unitaires.*

$$\begin{array}{ccc} p_1 : A_1 \times A_2 & \to A_1 \\ (a,b) & \mapsto a \end{array} \quad ; \quad \begin{array}{ccc} p_2 : A_1 \times A_2 & \to A_2 \\ (a,b) & \mapsto b \end{array},$$

*sont deux homomorphismes d'anneaux.*

**Propriétés I.4.1.** *Soit $A, B$ et $C$ des anneaux (unitaires).*

— *(i) Soit $f : A \to B$ un homomorphisme (non nul) d'anneaux, alors l'image par $f$ de tout sous-anneau (unitaire) de $A$ est un sous-anneau (unitaire) de $B$. L'image réciproque par $f$ de tout sous-anneau (unitaire) de $B$ est un sous-anneau (unitaire) de $A$*

*En particulier, $Ker(f)$ est un sous-anneau de $A$ et $f$ sera injectif si et seulement si $Ker(f) = \{0_A\}$.*

— *(ii) si $f : A \to B$ et $g : B \to C$ sont deux homomorphismes d'anneaux, alors $g \circ f : A \to C$ est un homomorphisme d'anneaux.*

— *(iii) Si $f : A \to B$ est un homomorphisme d'anneaux bijectif alors sa bijection réciproque $f^{-1} : B \to A$ est un homomorphisme d'anneaux. On dit dans ce cas que $f$ est un isomorphisme et que les deux anneaux $A$ et $B$ sont isomorphes.*

**Théorème I.2.** *Soit $\mathbb{K}$ un corps et $A$ un anneau unitaire. Soit $f : \mathbb{K} \to A$ un homomorphisme d'anneaux. Si $f$ est non nul, $f$ est alors injectif et l'anneau unitaire $f(\mathbb{K})$ est un corps.*

**Preuve.** *Si $f \neq \theta$ alors on a $f(1_{\mathbb{K}}) = 1_A$.*

*Supposons que $f$ est non injectif, i.e. $Ker(f) \neq \{0_{\mathbb{K}}\}$, il existe alors $x \in \mathbb{K}$ tel que $x \neq 0_{\mathbb{K}}$ et $f(x) = 0_A$. On en déduit que $x$ admet un inverse $x^{-1} \in \mathbb{K}$ et que*

$$0_A = f(x)f(x^{-1}) = f(xx^{-1}) = f(1_{\mathbb{K}}) = 1_A$$

*Ce qui est absurde. Donc $f$ est injectif. Il est alors clair que $f(\mathbb{K})$ est un corps isomorphe à $\mathbb{K}$.*■

**Remarque.** *Un homomorphisme non nul de corps $f : K \to K'$ est toujours injectif.*

# II Idéaux

## II.1 Notion d'Idéal

**Définition II.1.1.** *Soit $(A,+,\cdot)$ un anneau. Une partie $I$ de $A$ est dite idéal à gauche (resp. à droite) de $A$ si $(I,+)$ est un groupe et pour tout $a \in A$, pour tout $x \in I$, $ax \in I$ (resp. $xa \in I$).*

*On dit que $I$ est un idéal bilatère si $I$ est un idéal à gauche et un idéal à droite.*

**Proposition II.1.1.** *Soit $(A,+,\cdot)$ un anneau et $I$ une partie de $A$. $I$ est un idéal bilatère de $A$ si et seulement si*

- *(i) $(I,+)$ est un sous-groupe de $(A,+)$,*
- *(ii) $\forall a,b \in A, \forall x \in I, \quad axb \in I$.*

**Remarques.**

- *$\{0_A\}$ et $A$ sont deux idéaux bilatères de l'anneau $A$, appelés idéaux triviaux.*
- *Si $A$ est un anneau unitaire et $I \subseteq A$, $I$ est un idéal bilatère de $A$ si et seulement si*
  *(i) $I \neq \emptyset$,*
  *(ii) $\forall x,y \in I, \quad x+y \in I$,*
  *(iii) $\forall a,b \in A, \forall x \in I, \quad axb \in I$*
- *Lorsque $A$ est un anneau commutatif, les notions d'idéal à gauche, à droite et bilatère sont identiques et on parle alors simplement d'idéal de $A$.*
- *Les idéaux de $(\mathbb{Z},+,\cdot)$ sont les $n\mathbb{Z}$ où $n \in \mathbb{N}$.*
- *Soit $(A,+,\cdot)$ un anneau unitaire et $I$ un idéal à gauche (resp. à droite) de $A$. On a alors : $1_A \in I \Leftrightarrow I = A$.*
- *Tout idéal bilatère d'un anneau $A$ est un sous-anneau de $A$.*

**Proposition II.1.2.** *Soit $f : A \to B$ un homomorphisme d'anneaux.*

- *(a) Soit $J$ un idéal à gauche (resp. à droite, bilatère) de $B$, alors $f^{-1}(J)$ est un idéal à gauche (resp. à droite, bilatère) de $A$ (il contient $Ker(f)$). En particulier, le noyau $Ker(f)$ est un idéal bilatère de $A$.*
- *(b) Supposons que $f$ est surjectif. L'image $f(I)$ de tout idéal à gauche (resp. à droite, bilatère) $I$ de $A$ est un idéal à gauche (resp. à droite, bilatère) de $B$ (de $f(A)$ si $f$ n'est pas surjectif).*
- *(c) Supposons que $f$ est surjectif. L'application $\phi : J \mapsto f^{-1}(J)$ est une bijection de l'ensemble $\mathscr{C}$ des idéaux bilatères de $B$, sur l'ensemble $\mathscr{D}$ des idéaux bilatères de $A$ contenant $Ker(f)$ et $\phi$ respecte l'inclusion.*

**Preuve.** — *(a) et (b) : exercice.*

— *(c) : d'après (a), si $J$ est un idéal bilatère de $B$ alors $f^{-1}(J)$ est un idéal bilatère de $A$ et comme $0_A \in J$, on a alors $Ker(f) = f^{-1}(\{0\}) \subset f^{-1}(J)$ d'où $\phi$ est une application de $\mathscr{C}$ sur $\mathscr{D}$.*

*Soit $J, J' \in \mathscr{C}$ tel que $\phi(J') = \phi(J)$, i.e. $f^{-1}(J') = f^{-1}(J)$, alors $f(f^{-1}(J')) = f(f^{-1}(J))$, ceci équivaut à $J' = J$ (car $f$ est surjectif). Ainsi, $\phi$ est injective.*

*Finalement, comme pour toute partie $X$ de $A$, $f^{-1}(f(X)) = X + Ker(f)$, on a alors, pour tout idéal $I$ de $A$ tel que $Ker(f) \subset I$, $\quad f^{-1}(f(I)) = I + Ker(f) = I$, i.e. $\phi(f(I)) = I$, ce qui prouve que $\phi$ est surjective.*

## II.2 Idéal Engendré par une Partie - Idéal Principal

**Proposition II.2.1.** *L'intersection d'une famille d'idéaux à gauche (resp. à droite, bilatère) d'un anneau $A$, est un idéal à gauche (resp. à droite, bilatère) de $A$.*

**Preuve.** *Exercice.*

**Définition II.2.1.** *Soit $(A, +, \cdot)$ un anneau commutatif et $X$ une partie non vide de $A$. On appelle idéal engendré par $X$, noté $(X)$, l'intersection de tous les idéaux de $A$ qui contiennent $X$. C'est le plus petit idéal, au sens de l'inclusion, contenant $X$. Si $X = \{a_1, a_2, \cdots, a_n\}$, on note $(X)$ par $(a_1, a_2, \cdots, a_n)$.*

**Proposition II.2.2.** *Soit $(A, +, \cdot)$ un anneau unitaire commutatif et $X$ une partie non vide de $A$. Alors,*
$(X) = \left\{a_1x_1 + a_2x_2 + \cdots + a_nx_n \,/ n \in \mathbb{N}^*, \forall i \in \{1, 2, \cdots, n\}, a_i \in A \quad et \quad x_i \in X\right\}$.

**Preuve.** *Soit $I = \left\{a_1x_1 + \cdots + a_nx_n \,/ n \in \mathbb{N}^*, \forall i \in \{1, 2, \cdots, n\}, a_i \in A \quad et \quad x_i \in X\right\}$.*

*On montre que $I$ est un idéal de $A$ contenant $X$. Pour tout $x \in X$, $x = 1_Ax \in I$, donc $X \subset I$. Pour tous $x, y \in I$, $x = \sum_{1 \leq i \leq n} a_ix_i$ où $n \in \mathbb{N}^*, a_1, \cdots, a_n \in A, x_1, \cdots, x_n \in X$ et $y = \sum_{1 \leq j \leq m} b_jy_j$ où $m \in \mathbb{N}^*, b_1, \cdots, b_m \in A, y_1, \cdots, y_m \in X$. On a alors $x + y \in I$ par définition de $I$, et $\forall a \in A, ax = \sum_{1 \leq i \leq n} aa_ix_i \in I$.*

*Soit $K$ un idéal contenant $X$. Soit $x \in I$, $x = \sum_{1 \leq i \leq n} a_ix_i$ avec $n \in \mathbb{N}^*, a_1, \cdots, a_n \in A$ et $x_1, x_2, \cdots, x_n \in X$. $x_1, x_2, \cdots, x_n \in K$ et par suite $x \in K$ puisque $K$ est un idéal, d'où $I \subset K$. Ainsi, $I$ est le plus petit idéal contenant $X$, ce qui prouve que $I = (X)$.*■

**Définition II.2.2.** *Soit $(A, +, \cdot)$ un anneau commutatif unitaire. Un idéal $I$ de $A$ est dit principal s'il existe $x \in A$ tel que $I$ est engendré par $\{x\}$, i.e. $\exists x \in A$ tel que $I = (x) = \{ax \,/\, a \in A\}$.*

**Remarque.** $(x) = xA = Ax$, $\forall x \in A$.

**Exemple.** *Tout idéal de $\mathbb{Z}$ est principal.*

**Proposition II.2.3.** *Soit $(A,+,\cdot)$ un anneau commutatif unitaire.*
*$\forall x \in A$, $xA = A \iff x \in \mathcal{U}(A)$.*

**Preuve.** *Soit $x \in A$. Si $xA = A$ alors $1_A \in xA$, i.e. il existe $y \in A$ tel que $xy = 1_A$, ce qui prouve que $x \in \mathcal{U}(A)$.*

*Réciproquement, si $x \in \mathcal{U}(A)$, $\exists y \in A$ tel que $xy = 1_A$, d'où $1_A \in xA$ et par suite $xA = A$.*■

Le corollaire suivant est important et montre aussi que la notion d'idéal n'a d'intérêt que pour des anneaux qui ne sont pas des corps.

**Corollaire II.1.** *Soit $A$ un anneau commutatif unitaire.*
*$A$ est un corps $\iff$ les seuls idéaux de $A$ sont $\{0_A\}$ et $A$.*

**Preuve.** *Supposons que $A$ est un corps. Soit $I$ un idéal de $A$. Si $I \neq \{0_A\}$, il existe dans $I$ un élément $x$ non nul, donc inversible dans $A$ puisque $A$ est un corps, et par suite $1_A = x^{-1}x \in I$, d'où $I = A$.*

*Réciproquement, supposons que $A$ n'admet que $\{0_A\}$ et $A$ comme idéaux. Soit $x$ un élément non nul de $A$. L'idéal $xA$ engendré par $x$ étant alors distinct de $\{0_A\}$, et, par suite, nécessairement $xA = A$, d'où $x \in \mathcal{U}(A)$ d'après la proposition précédente. Ainsi, tout élément non nul de $A$ est inversible dans $A$. On conclut alors que $A$ est un corps.*■

**Exercice 1.** *Montrer que si $A$ est un anneau intègre fini alors $A$ est un corps.*

## II.3 Somme et Produit d'Idéaux

**Proposition et Définition II.3.1.** *Soit $(A,+,\cdot)$ un anneau commutatif unitaire. Soit $I_1, I_2$ deux idéaux de $A$. La somme de $I_1$ et $I_2$ est l'idéal noté $I_1+I_2$ engendré par $(I_1 \cup I_2)$. On a alors $I_1 + I_2 = \{x + y \,/\, x \in I_1 \ \text{ et } \ y \in I_2\}$*

**Preuve.** *Soit $I_1$ et $I_2$ deux idéaux de $A$. Alors $I_1$ et $I_2$ sont deux sous-groupes du groupe abélien $(A,+)$ et par suite $I_1 + I_2$ est le sous-groupe engendré par $I_1 \cup I_2$, donc $I_1 \cup I_2 \subset I_1 + I_2$.*

*Soit maintenant $a \in A$ et $z \in I_1 + I_2$. Il existe $x \in I_1$ et $y \in I_2$ tel que $z = x + y$, d'où $az = ax + ay$. Comme $ax \in I_1$ et $ay \in I_2$ car $I_1$ et $I_2$ sont des idéaux, on conclut que $az \in I_1 + I_2$.*■

**Remarques.** *Soit $A$ un anneau commutatif unitaire.*

— *Soit $x, y \in A$, $(x) + (y) = \{ax + by \,/\, a, b \in A\}$.*

— *On définit de même la somme d'une famille* $(I_j)_{j\in J}$ *d'idéaux de* $A$*, (où* $J$ *est un ensemble fini ou infini) comme l'idéal engendré par* $\bigcup_{j\in J} I_j$*, on la note* $\sum_{j\in J} I_j$*.*
*Un élément de cet idéal est somme finie d'éléments d'un nombre fini d'idéaux de la famille.*

**Définition II.3.1.** *Soit* $(A,+,\cdot)$ *un anneau commutatif unitaire et* $I_1, I_2$ *deux idéaux de* $A$*. On appelle produit des idéaux* $I_1$ *par* $I_2$*, l'idéal noté* $I_1I_2$ *engendré par l'ensemble* $\{x_1x_2 \,/ x_1 \in I_1,\ x_2 \in I_2\}$*. i.e.* $I_1I_2 = \left(\{x_1x_2 \,/ x_1 \in I_1,\ x_2 \in I_2\}\right)$

**Proposition II.3.1.** *Soit* $(A,+,\cdot)$ *un anneau commutatif unitaire et* $I_1, I_2$ *deux idéaux de* $A$*. Alors* $I_1I_2 = \{\sum_{i=1}^n x_iy_i \quad / \quad n \in \mathbb{N}^*, \forall i \in \{1,2,\cdots,n\}, x_i \in I_1,\ y_i \in I_2\}$*.*

**Preuve.** *On vérifie que* $\{\sum_{i=1}^n x_iy_i \quad / \quad n \in \mathbb{N}^*, \forall i \in \{1,2,\cdots,n\}, x_i \in I_1,\ y_i \in I_2\}$ *est un idéal contenant la partie* $X = \{x_1x_2 \,/ x_1 \in I_1,\ x_2 \in I_2\}$ *de* $A$ *et que c'est le plus petit idéal contenant cette partie.*■

**Proposition II.3.2.** *Soit* $(A,+,\cdot)$ *un anneau commutatif unitaire et* $I, J$ *des idéaux de* $A$*.*

— *(i)* $IJ \subset I \cap J$ *et si* $I + J = A$ *on a alors* $IJ = I \cap J$*,*

— *(ii)* $IA = I$*,*

**Preuve.** *Il est clair que* $IJ \subset I \cap J$*. Montrons que si* $A = I + J$ *on a l'inclusion inverse. Comme* $A = I + J$ *alors* $1_A \in I + J$ *i.e.* $1_A = u + v$ *où* $u \in I$ *et* $v \in J$*. Soit alors,* $x \in I \cap J$*,* $x = x1_A = xu + xv = ux + xv \in IJ$*.* ■

**Application au cas de l'anneau** $\mathbb{Z}$ (A montrer !)
On considère l'anneau $(\mathbb{Z},+,\cdot)$. Pour tous $n, m \in \mathbb{N}^*$, on a :
$n\mathbb{Z} + m\mathbb{Z} = d\mathbb{Z}$ où $d = pgcd(n,m)$
$n\mathbb{Z} \cap m\mathbb{Z} = \mu\mathbb{Z}$ où $\mu = ppcm(n,m)$
$n\mathbb{Z}\, m\mathbb{Z} = nm\mathbb{Z}$
En particulier, si $n$ et $m$ sont premiers entre-eux, on aura alors $n\mathbb{Z} + m\mathbb{Z} = \mathbb{Z}$ et $nm\mathbb{Z} = n\mathbb{Z} \cap m\mathbb{Z} = n\mathbb{Z}\, m\mathbb{Z}$.
On rappelle que $n\mathbb{Z} \subset m\mathbb{Z} \Leftrightarrow m$ divise $n$

## II.4 Idéaux Premiers et Maximaux

**Définition II.4.1.** *Soit* $A$ *un anneau commutatif unitaire.*
*Un idéal* $P$ *de* $A$ *est dit premier si*

— $P \neq A$*,*

— $\forall x, y \in A,\ xy \in P \Rightarrow (x \in P \quad ou \quad y \in P)$

*Un idéal $M$ de $A$ est dit maximal s'il est maximal au sens de l'inclusion parmi les idéaux de $A$ différents de $A$. Autrement dit, $M$ est maximal si*

- $M \neq A$,
- $\forall J$ *idéal de* $A$, $M \subset J \subset A \Rightarrow (J = M$ *ou* $J = A)$.

**Exemples.**
- $\{0\}$ *est un idéal premier de* $\mathbb{Z}$ *mais il n'est pas maximal :* $\{0\} \subset 2\mathbb{Z} \subset \mathbb{Z}$ *avec* $2\mathbb{Z} \neq \{0\}$ *et* $2\mathbb{Z} \neq \mathbb{Z}$.
- $6\mathbb{Z}$ *n'est ni premier (on a* $6 = 2 \times 3 \in 6\mathbb{Z}$, $2 \notin 6\mathbb{Z}$ *et* $3 \notin 6\mathbb{Z}$*), ni maximal (*$6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}$ *avec* $3\mathbb{Z} \neq 6\mathbb{Z}$ *et* $3\mathbb{Z} \neq \mathbb{Z}$.*)*

**Propriétés II.4.1.** *Soit $A$ un anneau commutatif unitaire.*

1. $\{0\}$ *est un idéal premier si et seulement si $A$ est intègre.*
2. $\{0\}$ *est maximal si et seulement si $A$ est un corps.*
3. *Si $M$ est un idéal maximal de $A$ alors $M$ est premier.*
4. *Soit $f : A \to A'$, un homomorphisme d'anneaux unitaires, non nul.*

   *(a) L'image réciproque par $f$ d'un idéal premier de $A'$ est un idéal premier de $A$,*

   *(b) on suppose de plus $f$ surjectif alors l'image réciproque par $f$ d'un idéal maximal de $A'$ est un idéal maximal de $A$ contenant $Ker(f)$.*

**Preuve.**
1. *est triviale.*
2. *On utilise le fait que les seuls idéaux d'un corps $\mathbb{K}$ sont $\{0\}$ et $\mathbb{K}$.*
3. *Soit $I$ un idéal maximal de $A$. On a alors $I \neq A$. Soit $x, y \in A$ tel que $xy \in I$. On suppose que $x \notin I$, par conséquent, $I \subsetneq I + (x)$ et puisque $I$ est maximal, il en résulte que $I + (x) = A$ et donc $1_A \in I + (x)$ ; ainsi $1_A = i + ax$ pour un certain $i \in I$ et un certain $a \in A$, d'où $y = y1_A = y\,i + axy$, comme par hypothèse $xy \in I$ on a alors $y \in I$. Ce qui montre que $I$ est premier.*
4. *Soit $f : A \to A'$, un homomorphisme d'anneaux commutatifs unitaires.*

   *(a) Soit $P$ un idéal premier de $A'$, on a alors $f^{-1}(P)$ est un idéal de $A$ contenant $Ker(f)$.*

   - $f^{-1}(P) \neq A$. *Car sinon* $1_A \in f^{-1}(P)$, *ceci équivaut à* $f(1_A) \in P$, *et donc, en vertu de l'homomorphisme de* $f$, $1_{A'} \in P$, *ce qui est contradictoire avec* $P \neq A'$.
   - $\forall x, y \in A$, $xy \in f^{-1}(P) \Leftrightarrow f(xy) \in P \Leftrightarrow f(x)f(y) \in P \Leftrightarrow$ $(f(x) \in P$ *ou* $f(y) \in P)$ *(d'après l'hypothèse)* $\Leftrightarrow (x \in f^{-1}(P)$ *ou* $y \in f^{-1}(P))$

(b) *On suppose de plus que $f$ est surjectif. Soit $J$ un idéal maximal de $A'$. Alors $f^{-1}(J)$ est un idéal de $A$ contenant $Ker(f)$. Montrons qu'il est maximal. On a $f^{-1}(J) \neq A$ car sinon $f(f^{-1}(J)) = f(A)$ ; comme $f$ est surjectif on aura alors $J = A'$. Contradiction.*

*Soit $K$ un idéal de $A$ tel que $f^{-1}(J) \subset K \subsetneq A$, on a alors $f(f^{-1}(J)) \subset f(K) \subset f(A)$. D'où, d'après la surjection de $f$, $J \subset f(K) \subset A'$, et comme par hypothèse $J$ est maximal, on en déduit que $J = f(K)$ ou $f(K) = A'$. Si $f(K) = A'$, on aura $f^{-1}(f(K)) = f^{-1}(A') = A$, i.e. $K + Ker(f) = A$, or $Ker(f) \subset f^{-1}(J) \subset K$. D'où $K = A$, ce qui est contradictoire avec $K \neq A$. Ainsi, $f(K) \neq A'$, par conséquent $f(K) = J$ et par suite $f^{-1}(f(K)) = f^{-1}(J)$. Donc $K = f^{-1}(J)$.*

**Exercice 2.** *soit $f : A \longrightarrow A'$ un épimorphisme d'anneaux commutatif unitaire.*

- *Montrer que si $P$ est un idéal premier (resp. maximal) de $A$ contenant $Ker(f)$, alors $f(P)$ est un idéal premier (resp. maximal) de $A'$.*
- *Montrer que l'application $\phi : Q \mapsto f^{-1}(Q)$ est une bijection de l'ensemble des idéaux premiers (resp. maximaux) de $A'$ sur l'ensemble des idéaux premiers (resp.maximaux) de $A$ contenant $Ker(f)$.*

**Théorème II.1.** *(Théorème d'existence d'idéaux maximaux). Tout anneau commutatif unitaire possède un idéal maximal.*

**Preuve.** *Ordonnons l'ensemble $\mathscr{E}$ des idéaux de $A$, distincts de $A$ par la relation d'inclusion. Cet ensemble $\mathscr{E}$ est non vide car $\{0\} \in \mathscr{E}$. Vérifions que $\mathscr{E}$ est inductif.*
*Soit $\mathcal{F} = (I_i)_{i\in J}$ une famille totalement ordonnée d'éléments de $\mathscr{E}$. $I = \bigcup_{i\in J} I_i$ est un idéal de $A$, et puisque pour tout $i \in J$, $1_A \notin I_i$ et $I_i \subseteq I$, on a alors $I \in \mathscr{E}$ et $I$ est un majorant de $\mathcal{F}$, donc toute famille de $\mathscr{E}$ totalement ordonnée est majorée, ce qui prouve que $\mathscr{E}$ est un ensemble inductif.*
*On conclut alors, d'après le lemme de Zorn, que $\mathcal{E}$ admet un élément maximal.*■

On rappelle le lemme de Zorn :

**Lemme 1.** *Tout ensemble ordonné inductif admet un élément maximal.*

**Théorème II.2.** *Soit $A$ un anneau commutatif unitaire et $I$ un idéal de $A$, distinct de $A$. Alors $I$ est contenu dans un idéal maximal de $A$.*

**Preuve.** *Soit $\mathscr{E} = \{J \quad / J \text{ idéal de } A \text{ et } I \subset J \subsetneq A\}$. On a $I \in \mathscr{E}$ d'où $\mathscr{E} \neq \emptyset$. $\mathscr{E}$ est ordonné par inclusion. On montre que $\mathscr{E}$ est inductif et par le lemme de Zorn, $\mathscr{E}$ admet un élément maximal. Donc $I$ est contenu dans un idéal maximal.*■

**Corollaire II.2.** *Dans un anneau commutatif unitaire, tout élément non inversible appartient à un idéal maximal.*

**Preuve.** *Si $x$ est non inversible, l'idéal $(x)$ est distinct de $A$ et d'après le théorème précédent, il existe un idéal maximal $M$ tel que $(x) \subset M$, $(x \in M)$.*■