Cours d'Algèbre 6
Filière SMA
Année 2020-2021

Mme F. ERRAJI, Pr.

26 mai 2021

Table des matières

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 θ 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* θ*). 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.*

$$p_1 : A_1 \times A_2 \to A_1,\ (a,b) \mapsto a \qquad p_2 : A_1 \times A_2 \to A_2,\ (a,b) \mapsto b$$

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. $Ker(f) \neq \{0_A\}$, il existe alors $x \in \mathbb{K}$ tel que $x \neq 0_A$ 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 $Kerf(f)$). En particulier, le noyau $Kerf(f)$ 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 $Kerf(f)$ et ϕ 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 $Kerf(f) = f^{-1}(\{0\}) \subset f^{-1}(J)$ d'où ϕ 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, ϕ 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 ϕ 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. *1. Si I_1 et I_2 sont deux idéaux bilatères d'un anneau A alors $I_1 + I_2$ est un idéal bilatère de A.*

2. *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 $I_1I_2 = \left\{ \sum_{i=1}^n x_iy_i \quad / \quad n \in \mathbb{N}^*, \forall i \in \{1,2,\cdots,n\}, x_i \in I_1,\, y_i \in I_2\right\}$.*

Preuve. *On vérifie que $\left\{ \sum_{i=1}^n x_iy_i \quad / \quad n \in \mathbb{N}^*, \forall i \in \{1,2,\cdots,n\}, x_i \in I_1,\, y_i \in I_2\right\}$ 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

— $M \neq A$,

— $\forall J \ \ idéal\ de\ \ A,\ M \subset J \subset A \Rightarrow (J = M \quad ou \quad J = A)$.

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* $(x) \subset M$, $(x \in M)$.■

III Anneaux Quotients

III.1 Anneau Quotient et Idéaux d'un Anneau Quotient

Soit A un anneau et I un idéal bilatère de A.

— L'idéal I est en particulier un sous-groupe du groupe abélien $(A, +)$. Il est trivialement distingué. On peut donc considérer le groupe quotient $(A/I, +)$. Rappelons que la loi quotient est définie par $\overline{x}+\overline{y} = \overline{x+y}, \forall \overline{x}, \overline{y} \in A/I$ et $\overline{x} = \{y \in A \,/\, x - y \in I\} = x + I$; et que $p : A \to A/I$ est un homomorphisme de groupes.

— On munit A/I d'une multiplication (et en faire un anneau) en posant $\overline{x}\,\overline{y} = \overline{xy}, \forall \overline{x}, \overline{y} \in A/I$ (i.e. $(x + I)(y + I) = xy + I$)

elle est bien définie, en effet, $\forall \overline{x}, \overline{x'}, \overline{y}, \overline{y'} \in A/I, \quad (\overline{x}, \overline{y}) = (\overline{x'}, \overline{y'}) \Leftrightarrow \overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'} \Leftrightarrow x - x' \in I$ et $y - y' \in I$. Comme I est un idéal bilatère, on a alors $(x - x')y \in I$ et $x'(y - y') \in I$, i.e. $xy - x'y \in I$ et $x'y - x'y' \in I$ d'où $xy - x'y' \in I$ et donc $\overline{xy} = \overline{x'y'}$,

l'associativité de la loi quotient multiplicative découle de la définition de cette loi et l'associativité de la loi "$\cdot$" dans A,

elle est distributive par rapport à l'addition : $\forall \overline{x}, \overline{y}, \overline{z} \in A/I$,

$$\overline{x}(\overline{y} + \overline{z}) = \overline{x}(\overline{y+z}) = \overline{x(y+z)} = \overline{xy + xz} = \overline{xy} + \overline{xz} = \overline{x}\,\overline{y} + \overline{x}\,\overline{z}$$
$$\text{et} \quad (\overline{x} + \overline{y})\,\overline{z} = (\overline{x+y})\,\overline{z} = \overline{(x+y)z} = \overline{xz + yz} = \overline{xzyz} = \overline{x}\,\overline{z} + \overline{y}\,\overline{z}$$

— La surjection canonique $p : A \to A/I$ vérifie aussi $p(xy) = p(x)p(y)$ pour tous $x, y \in A$, donc p est un homomorphisme d'anneaux.

On a ainsi le théorème suivant :

Théorème III.1. *Soit* $(A, +, \cdot)$ *un anneau et* I *un idéal bilatère de* A. *L'ensemble quotient* A/I *muni des lois quotients induites par celles de l'anneau* A *est un anneau appelé l'anneau quotient de* A *par* I *et la surjection canonique* $p : A \to A/I$ *est un homomorphisme d'anneaux.*

Remarque. *Si A est commutatif, A/I est commutatif.*
Si A est unitaire et I est distinct de A, A/I est unitaire, d'élément unité $1_{A/I} = \overline{1_A}$ ($1_A \notin I$ d'où $\overline{1_A} \neq \overline{0_A}$ et $\forall \overline{x} \in A/I$, $\overline{x} = \overline{x \cdot 1_A} = \overline{x} \cdot \overline{1_A}$).

Exemples.
— *Les anneaux quotients de $(\mathbb{Z}, +, \cdot)$ sont de la forme $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}$. A noter que l'anneau quotient d'un anneau intègre n'est pas un anneau intègre.*
— *Les seuls idéaux de $\mathbb{R}$ sont $\{0\}$ et $\mathbb{R}$, donc les anneaux quotients de $\mathbb{R}$ sont $\mathbb{R}/\{0\} = \{\overline{x} \,/ x \in \mathbb{R}\} \simeq \mathbb{R}$ et $\mathbb{R}/\mathbb{R} = \{\overline{0}\} \simeq \{0\}$.*

Proposition III.1.1. *Soit A un anneau et I un idéal bilatère de A. Alors les idéaux bilatères de l'anneau quotient A/I sont de la forme J/I où J est un idéal bilatère de A contenant I.*

Preuve. *On considère l'homomorphisme surjectif canonique $p : A \to A/I$, $Ker(p) = I$. D'après la proposition II.1.2, l'application*

$$\begin{array}{ccccc} \phi^{-1} : \{J & / J \text{ idéal de } A \text{ et } I \subset J\} & \longrightarrow & \{K & / K \text{ idéal de } A/I\} \\ & J & \longmapsto & & \phi^{-1}(J) = p(J) \end{array}$$

est bijective. Donc, pour tout idéal K de A/I, il existe un idéal unique J de A tel que $I \subset J$ et $K = \phi^{-1}(J) = p(J) = J/I$. ■

Application à l'anneau $\mathbb{Z}$
Soit $n \in \mathbb{N}^*$. Les idéaux de l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $d\mathbb{Z}/n\mathbb{Z}$ où d est un diviseur de n.

Proposition III.1.2. *Soit A un anneau commutatif unitaire et I un idéal de A. Les idéaux premiers (resp. maximaux) de A/I sont les idéaux de la forme P/I (resp. M/I), où P est un idéal premier (resp. M un idéal maximal) de A contenant I.*

Preuve. *Il résulte de la proposition précédente, de la propriété II.4.1 et de l'exercice qui la suit.* ■

Théorème III.2. *Soit A un anneau commutatif unitaire et I un idéal de A.*
— *I est premier si et seulement si A/I est intègre.*
— *I est maximal si et seulement si A/I est un corps.*

Preuve.
— *Si I est premier, $I \neq A$ ainsi l'anneau commutatif A/I est unitaire ; et si $\overline{x}, \overline{y} \in A/I$ tel que $\overline{x}\,\overline{y} = \overline{0}$ alors $xy \in I$, d'où $x \in I$ ou $y \in I$ et par suite $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$.*
Réciproquement, si A/I est intègre alors A/I est unitaire et donc $1 \notin I$ (car $\overline{1} \neq \overline{0}$), ainsi $I \neq A$; de plus, si $x, y \in A$ tel que $xy \in I$ alors $\overline{x}\,\overline{y} = \overline{xy} = \overline{0}$, ce qui implique que $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$ et il s'en suit que $x \in I$ ou $y \in I$.

— *Supposons que I est maximal, alors $I \neq A$ et donc A/I est unitaire. Et, si J est un idéal de A/I alors $J = K/I$ où K est un idéal de A tel que $I \subset K$, il résulte de la maximalité de I que $K = I$ ou $K = A$, et par suite $J = \{\overline{0}\}$ ou $J = A/I$. Donc les seuls idéaux de A/I sont $\{\overline{0}\}$ et A/I. Ce qui prouve que A/I est un corps.*

Inversement, si A/I est un corps alors A/I est unitaire et par suite $I \neq A$; De plus, si K est un idéal de A tel que $I \subset K \subset A$ alors K/I est un idéal de A/I. Par conséquent, $K/I = \{\overline{0}\}$ ou $K/I = A/I$, d'où$K = I$ ou $K = A$. ■

Exemples. — *Les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et les $p\mathbb{Z}$ où p est un nombre premier.*

— *Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ où p est un nombre premier.*

— *Soit $n \in \mathbb{N}^*$, les idéaux maximaux de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme $p\mathbb{Z}/n\mathbb{Z}$ où p est un nombre premier et p divise n.*

III.2 Propriété Universelle, Théorèmes d'Isomorphisme

Théorème III.3. *(Propriété universelle de l'anneau quotient) Soit A un anneau, I un idéal bilatère de A et p l'homomorphisme surjectif canonique de A dans A/I. Pour tout anneau A' et tout homomorphisme d'anneaux $f : A \to A'$ tel que $I \subseteq Ker(f)$, il existe un unique homomorphisme d'anneaux :$\overline{f} : A/I \to A'$ tel que $f = \overline{f} \circ p$. De plus, on a $Im(\overline{f}) = Im(f)$ et $Ker(\overline{f}) = Ker(f)/I$ (si f est surjectif, $\overline{f}$ l'est aussi et si $Ker(f) = I$ alors $\overline{f}$ est injectif).*

Preuve. *Comme f est un homomorphisme de groupes de $(A, +)$ dans $(A', +)$ tel que $I \subseteq Ker(f)$ (avec $I \trianglelefteq (A, +)$, il existe alors un unique homomorphisme de groupes : $\overline{f} : (A/I, +) \to (A', +)$ tel que $f = \overline{f} \circ p$, i.e. $\overline{f}(\overline{x}) = f(x), \forall \overline{x} \in A/I$. On a pour tous $\overline{x}, \overline{y} \in A/I$:*
$\overline{f}(\overline{x}\,\overline{y}) = \overline{f}(\overline{xy}) = \overline{f} \circ p(xy) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y})$
donc $\overline{f}$ est un homomorphisme d'anneaux. ■

Nous allons donner maintenant -comme dans le cas des groupes- un certain nombre de conséquences classiques de cette construction : décomposition canonique des homomorphismes d'anneaux et théorème d'isomorphisme d'anneaux.

Corollaire III.1. *(1^{er} théorème d'isomorphisme - décomposition canonique) Soit $f : A \to A'$ un homomorphisme d'anneaux. Soit p l'homomorphisme surjectif canonique de A dans $A/Ker(f)$ et j l'homomorphisme injectif canonique de $Im(f)$ dans A'. Il existe alors un unique isomorphisme $\overline{f} : A/Ker(f) \to Im(f)$ tel que $f = j \circ \overline{f} \circ p$. $f = j \circ \overline{f} \circ p$ est appelée la décomposition canonique de l'homomorphisme f.*

Preuve. *En appliquant le théorème précédent à l'homomorphisme* $g : A \to Im(f)$ *défini par* $\forall x \in A,\ g(x) = f(x)$ *et à* $I = Ker(g) = Kerf(f)$, *on obtient un isomomorphisme d'anneaux* $\overline{f} : A/Kerf(f) \to Im(f)$ *tel que* $g = \overline{f} \circ p$. *Et finalement, on a* $f = j \circ g = j \circ \overline{f} \circ p$.■

Corollaire III.2. *(*2^{me} *théorème d'isomorphisme) Soit* A *un anneau. Soit* I *et* J *deux idéaux bilatères de* A. *Alors* $I + J/J$ *et* $I/I \cap J$ *sont des anneaux isomorphes.*

Preuve. *Comme tout idéal bilatère de* A *est un sous-anneau de* A *et tout sous-anneau est un anneau, alors* $I + J$ *et* I *sont des anneaux,* J *est un idéal bilatère de* $I + J$ *et* $I \cap J$ *est un idéal bilatère de* I. *Ainsi,* $I + J/J$ *et* $I/I \cap J$ *sont des anneaux.*

Considérons l'homomorphisme surjectif canonique $p : I + J \to I + J/J$ *et soit* $g : I \to I + J/J$ *la restriction de* p *à* I. g *est un homomorphisme d'anneaux ; il est surjectif et* $Ker(g) = Ker(p) \cap I = J \cap I$. *On conclut alors d'après le premier théorème d'isomorphisme que* $I/I \cap J \simeq I + J/J$.■

Théorème III.4. *Soit* I *et* J *deux idéaux bilatères d'un anneau* A *tel que* $I \subset J$ *alors les anneaux* A/J *et* $A/I/J/I$ *sont isomorphes.*

Preuve. *L'homomorphisme surjectif canonique* $p : A \to A/J$ *dont le noyau contient* I *induit alors un homomorphisme d'anneaux* $\overline{f} : A/I \to A/J$ *tel que* $\overline{f} \circ q = p$ *où* q *est l'homomorphisme surjectif canonique de* A *sur* A/I. *De plus,* $Im(\overline{f}) = Im(p) = A/J$ *et* $Ker(\overline{f}) = Ker(p)/I = J/I$. *Il en résulte alors d'après le premier théorème de l'isomorphisme que* $A/I/J/I \simeq A/J$.■

Application à $\mathbb{Z}$.
Soit $n, m \in \mathbb{N}^*$. $\mathbb{Z}/nm\mathbb{Z}/n\mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z}$.

Théorème III.5. *(Théorème Chinois) Soit* A *un anneau commutatif unitaire et* I, J *deux idéaux de* A *tel que* $I + J = A$. *L'anneau* A/IJ *est alors isomorphe à l'anneau produit* $A/I \times A/J$.

Preuve. *On considère l'application* $f : A \to A/I \times A/J$ *définie par* $f(x) = (\overline{x}, \dot{\overline{x}}) = (x+I, x+J)$. f *est un homomorphisme d'anneaux. On a alors d'après le premier théorème d'isomorphisme* $A/Ker(f) \simeq Im(f)$. *Or* $Ker(f) = \left\{x \in A \ / \ \overline{x} = \overline{0} \ \text{ et } \ \dot{\overline{x}} = \dot{\overline{0}}\right\} = \{x \in A \ / \ x \in I \ \text{ et } \ x \in J\} = I \cap J$

et puisque, par hypothèse $I + J = A$, *on a alors, d'après la propostion II.3.2,* $IJ = I \cap J = Ker(f)$, *donc pour avoir le résultat, il reste à montrer que* f *est surjectif. Soit* $(\overline{x}, \dot{\overline{x}}) \in A/I \times A/J$. *Comme par hypothèse* $I + J = A$, *alors il existe* $u \in I, v \in J$ *tel que* $1 = u + v$, *d'où* $(\overline{x}, \dot{\overline{y}}) = (\overline{x}\overline{1}, \dot{\overline{x}}\dot{\overline{1}}) = (\overline{xv}, \dot{\overline{yu}})$. *Si on prend* $a = xv + yu \in A$ *on a alors* $f(a) = (\overline{x}, \dot{\overline{a}}) = (\overline{xv}, \dot{\overline{yu}}) = (\overline{x}, \dot{\overline{y}})$, *ce qui prouve que* f *est surjectif.*■

Corollaire III.3. *Soit $n, m \in \mathbb{N}^*$. Si n et m sont premiers entre-eux alors les anneaux $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes.*

III.3 Caractéristique d'un Anneau

Lemme et Définition III.3.1. *Soit A un anneau commutatif unitaire. Il existe un unique homomorphisme d'anneaux, non nul, $f : \mathbb{Z} \to A$ défini par $f(n) = n1_A, \forall n \in \mathbb{Z}$. On l'appelle l'homomorphisme canonique de $\mathbb{Z}$ dans A.*

Preuve. *Si f est un homomorphisme d'anneaux non nul de $\mathbb{Z}$ dans A alors $f(1) = 1_A$, d'où $f(2) = f(1+1) = f(1)+f(1) = 1_A+1_A = 2 \cdot 1_A$, et par récurrence on aura $f(n) = n1_A$ pour tout $n \in \mathbb{N}^*$.*

Soit maintenant $n \leq 0$. Si $n = 0$ on a $f(0) = 0_A = 01_A$.

Si $n < 0$, $f(n) = f(-(-n)) = -f(-n)$ car f est un homomorphisme de groupes. Or $-n > 0$, on a alors $f(n) = -((-n)1_A) = n1_A$.

En résumé, on a $f(n) = n1_A$, $\forall n \in \mathbb{Z}$.

Réciproquement, comme $(A, +)$ est un groupe, on a $\forall a \in A$, $f_n : \mathbb{Z} \to A$ défini par $n \mapsto na$ est un homomorphisme de groupes. En particulier, pour $a = 1_A$, f est un homomorphisme de groupes.

On vérifie que $f(nm) = f(n)f(m)$, $\forall n, m \in \mathbb{Z}$, pour conclure que f est un homomorphisme d'anneaux.■

Remarques.
— *Le noyau de l'homomorphisme canonique f de A dans $\mathbb{Z}$ est un idéal de $\mathbb{Z}$. Donc, $Ker(f) = k\mathbb{Z}$ pour un unique $k \in \mathbb{N}$.*

— $\forall n \in \mathbb{Z} : (n1_A = 0_A) \Leftrightarrow (nx = 0_A, \forall x \in A)$, *autrement dit,* $\forall n \in \mathbb{Z}$, $n \in Ker(f) \Leftrightarrow nx = 0_A, \forall x \in A$.

Définition III.3.1. *Soit A un anneau commutatif unitaire. On appelle caractéristique de A, notée $CarA$, l'unique entier $k \in \mathbb{N}$ tel que $Ker(f) = k\mathbb{Z}$ où f est l'homomorphisme canonique de $\mathbb{Z}$ dans A.*

D'après la remarque précédente,
$CarA = 0 \Leftrightarrow \left[\forall n, (nx = 0_A, \forall x \in A) \Leftrightarrow n = 0\right]$
$CarA = k > 0 \Leftrightarrow \left[\forall n, (nx = 0_A, \forall x \in A) \Leftrightarrow n \in k\mathbb{Z}\right]$

Remarques.
— *Si $CarA = 0$, alors A est infini.*

— $CarA = k > 0 \Leftrightarrow$ *k est le plus petit entier strictement positif tel que $k1_A = 0_A$*
$\Leftrightarrow$ *k est le plus petit entier strictement positif tel que $kx = 0_A, \forall x \in A$.*
$\Leftrightarrow$ *L'ordre de l'élément 1_A dans le groupe $(A, +)$ est k.*

Exemples. *(1)- L'anneau $\mathbb{Z}$ est de caractéristique nulle, ainsi que les corps $\mathbb{Q}, \mathbb{R}$ et $\mathbb{C}$.*
(2)- Pour tout $n \geq 2$, $Car(\mathbb{Z}/n\mathbb{Z}) = n$.

Proposition III.3.1. *Si A est un anneau intègre et de caractéristique non nulle, alors A admet pour caractéristique un nombre premier.*

Preuve. *Soit $p = Car(A)$ avec $p \neq 0$. Supposons que $p = qr$ avec $q, r \in \mathbb{N}^*$, la relation $0_A = p1_A = (qr)1_A = (q1_A)(r1_A)$ donne par intégrité de A, $q1_A = 0$ ou $r1_A = 0$ d'où $q \in p\mathbb{Z}$ ou $r \in p\mathbb{Z}$, i.e. p/q ou p/r. Comme $p = qr$, il en résulte que $q = p$ ou $r = p$. Ainsi p est premier.* ■

Corollaire III.4. *La caractéristique d'un corps commutatif est soit nulle soit un nombre premier.*

Proposition III.3.2. *Soit A un anneau intègre de caractéristique p premier. On a alors*

- *(i) $\forall x, y \in A, \quad (x+y)^p = x^p + y^p$,*
- *(ii) l'application $F : A \to A$ définie par $F(x) = x^p$ est un homomorphisme d'anneaux, appelé homomorphisme de Fröbenius.*

Preuve. *Exercice !*

III.4 Corps des Fractions d'un Anneau Intègre.

Nous avons vu que tout corps commutatif est un anneau intègre et que la réciproque n'est pas toujours vraie. Dans le paragraphe suivant, nous allons montrer, cependant, que l'on peut construire, de façon canonique, pour tout anneau intègre, un corps qui le contient. En l'occurence, il s'agit du plus petit corps qui le contient. Ce corps commutatif est appelé *Corps des fractions* de A.

Proposition III.4.1. *Soit A un anneau intègre. On note $A^* = A \setminus \{0_A\}$.*

- *(i) L'ensemble $A \times A^*$ muni des lois de composition internes addition et multiplication définies par :*
  $(a,b) + (a',b') = (ab' + ba', bb')$
  et $(a,b)(a',b') = (aa', bb')$
  est un anneau intègre d'élément neutre $(0,1)$ et d'élément unité $(1,1)$.
- *(ii) La relation binaire R définie sur $A \times A^*$ par : $(a,b)R(a',b') \Leftrightarrow ab' = a'b$ est une relation d'équivalence compatible avec l'addition et la multiplication dans $A \times A^*$.*
- *(iii) L'ensemble quotient $(A \times A^*)/R$ muni des lois quotients induites de $+$ et "$\cdot$" est un corps commutatif d'élément neutre $\overline{(0,1)}$ et d'élement unité $\overline{(1,1)}$.*

— *(iv)* A *est isomorphe à un sous-anneau unitaire du corps* $(A \times A^*)/R$, *(*A *est un sous-anneau unitaire de* $(A \times A^*)/R$*).*

— *(v) Si* K *est un corps commutatif et* A *est un sous-anneau unitaire de* K *alors* $(A \times A^*)/R$ *est isomorphe à un sous-corps de* K.

Preuve. — *(i) et (ii) sont faciles à vérifier.*

— *(iii) D'après (i) et (ii),* $((A \times A^*)/R, +, \cdot)$ *est un anneau unitaire d'élément neutre* $\overline{(0,1)}$ *et d'élément unité* $\overline{(1,1)}$. *Avec* $\overline{(0,1)} = \{(a,b) \in A \times A^* \ / a = 0\}$ *et* $\overline{(1,1)} = \{(a,b) \in A \times A^* \ / a = b\}$. *Il reste à montrer que tout élément non nul de* $(A \times A^*)/R$ *est inversible. Soit* $\overline{(a,b)} \in (A \times A^*)/R \setminus \{\overline{(0,1)}\}$, *on a* $\overline{(a,b)}\,\overline{(b,a)} = \overline{(ab,ab)} = \overline{(1,1)}$, *donc* $\overline{(a,b)}$ *est inversible et son inverse est* $\overline{(b,a)}$.

— *(iv) Soit l'application* $\varphi : A \to (A \times A^*)/R$ *définie par* $\varphi(a) = \overline{(a,1)}$.
$\forall a, b \in A$, $(a,1) + (b,1) = (a+b,1)$ *et* $(a,1)(b,1) = (ab,1)$. *D'où* $\varphi(a) + \varphi(b) = \varphi(a+b)$ *et* $\varphi(a)\varphi(b) = \varphi(ab)$. *De plus,* $\varphi(1) = \overline{(1,1)} = 1_{(A \times A^*)/R}$, *donc* φ *est un homomorphisme d'anneaux unitaires. Il est injectif, en effet,*
$\forall a \in A, \varphi(a) = \overline{(0,1)} \Leftrightarrow \overline{(a,1)} = \overline{(0,1)} \Leftrightarrow a = 0$.
Ainsi, A *est isomorphe à* $\varphi(A)$ *qui est un sous-anneau unitaire de* $(A \times A^*)/R$. *Par identification,* A *est considéré comme un sous-anneau unitaire de* $(A \times A^*)/R$.

— *(v) Soit* K *un corps commutatif tel que* A *est un sous-anneau unitaire de* K, *considérons* $f : (A \times A^*)/R \to K$ *définie par* $f(\overline{(a,b)}) = ab^{-1}$. *Montrons que* f *est bien définie (c'est-à-dire, que* $f(\overline{(a,b)})$ *ne dépend pas du représentant choisi de la classe). Soit* $\overline{(a,b)}, \overline{(a',b')} \in (A \times A^*)/R$: $\overline{(a,b)} = \overline{(a',b')} \Leftrightarrow ab' = a'b \Leftrightarrow ab^{-1} = a'b^{-1} \Leftrightarrow f(\overline{(a,b)}) = f(\overline{(a',b')})$. *Donc* f *est bien définie et injectif. Il est facile de vérifier que c'est un homomorphisme d'anneaux unitaires. Donc* $(A \times A^*)/R$ *est isomorphe à* $f((A \times A^*)/R)$ *qui est un sous-corps de* K. ■

Remarque. *Une généralisation de* (v) est donnée comme suit : (Propriété universelle du corps de fractions)

Pour tout corps K et tout homomorphisme injectif $f : A \to K$, il existe un unique homomorphisme d'anneaux $\overline{f} : (A \times A^*)/R \to K$ tel que $\overline{f} \circ \varphi = f$ où $\varphi : A \to (A \times A^*)/R$ est l'homomorphisme injectif défini par $\varphi(a) = \overline{(a,1)}$.

Définition III.4.1. *Le corps* $((A \times A^*)/R, +, \cdot)$ *s'appelle le corps des fractions de l'anneau intègre* A, *on le note* $Fr(A)$. *Tout élément* $\overline{(a,b)} \in Fr(A)$ *sera noté* $\frac{a}{b}$. *Ainsi,*

$$Fr(A) = \left\{\frac{a}{b} \,/\, a \in A \ \text{ et } \ b \in A^*\right\}$$
$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$$
$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \ \text{ et } \ \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

et $\frac{a}{1} = a$.

Exemples. *1. Le corps des fractions de l'anneau intègre* $\mathbb{Z}$ *est le corps des rationnels* $\mathbb{Q}$.

2. Le corps des fractions de $\mathbb{Z}[i]$ *est* $\mathbb{Q}(i)$. *A titre d'exercice !*

Exercice 3. *Soit* K *un corps et* p *sa caractéristique. Montrer que :*

— *si* $p = 0$, *il existe dans* K *un plus petit sous-corps* K_0 *isomorphe à* $\mathbb{Q}$,

— *si* $p \neq 0$, *il existe dans* K *un plus petit sous-corps* K_0 *isomorphe à* $\mathbb{Z}/p\mathbb{Z}$.

IV Divisibilité dans un Anneau Intègre - Arithmétique dans un Anneau Principal

IV.1 Diviseurs, Eléments Associés

Définition IV.1.1. *Soit* A *un anneau intègre et* $a, b \in A$.

— *(i) On dit que* a *divise* b *(ou que* b *est divisible par* a, *ou encore que* b *est un multiple de* a*) s'il existe* $c \in A$ *tel que* $b = ac$, *on note* a/b.

— *(ii) On dit que* a *et* b *sont associés si* a/b *et* b/a.

Remarques. *Soit* A *un anneau intègre et* $a, b, c \in A$. *Alors*

— a/a, $1/a$ *et* $a/0$.

— $(a/b \text{ et } b/c) \Rightarrow a/c$.

— $\forall \lambda \in \mathcal{U}(A)$, a *et* λa *sont associés.*

— *La relation d'association définie par* $aRb \Leftrightarrow a$ *et* b *sont associés, est une relation d'équivalence.*

— a *et* b *sont associés* $\Leftrightarrow \exists \lambda \in \mathcal{U}(A), b = \lambda a$.

On va caractériser les notions de divisibilité et d'association en termes d'idéaux.

Proposition IV.1.1. *Soit* A *un anneau intègre et* $a, b \in A$. *Alors*

— *(i)* $a/b \Leftrightarrow (b) \subset (a)$, *(i.e.* $bA \subset aA$*).*

— *(ii)* a *et* b *sont associés* $\Leftrightarrow (a) = (b)$ *(i.e.* $aA = bA$*)*

— *(iii)* a *est inversible* $\Leftrightarrow a$ *divise tous les éléments de* A.

Preuve. — *(i)* $a/b \Leftrightarrow \exists c \in A, b = ac \Leftrightarrow b \in (a) \Leftrightarrow (b) \subset (a)$

— *(ii) découle de la définition et de (1)*

— *(iii)* a *est inversible* $\Leftrightarrow (a) = A \Leftrightarrow \forall b \in A,\ \exists c \in A, b = ca \Leftrightarrow \forall b \in A,\ a/b.$ ■

Remarque. *Deux éléments associés ont les mêmes diviseurs et les mêmes multiples dans* A.

IV.2 Eléments Irreductibles, Eléments Premiers

Définition IV.2.1. *Soit* A *un anneau intègre et* a *un élément non nul de* A.

— *(i)* a *est dit irréductible (ou extrêmal) s'il n'est pas inversible dans* A *et si ses seuls diviseurs sont ses associés et les éléments inversibles de* A. *Autrement dit* a *est irréductible dans* A *si* a *est non inversible et si* $a = xy$ *avec* $x, y \in A$, *alors* $x \in \mathcal{U}(A)$ *ou* $y \in \mathcal{U}(A)$.

— *(ii)* a *est dit premier dans* A *lorsqu'il est non inversible dans* A *et pour tous* $x, y \in A$ *si* a/xy *alors* a/x *ou* a/y.

On notera que dans la définition (i), le "ou" est exclusif, car sinon a sera inversible.

Proposition IV.2.1. *Soit* A *un anneau intègre et* a *un élément non nul de* A. *On a :*
(i)- a *est irréductible dans* $A \Leftrightarrow (a)$ *est maximal parmi les idéaux principaux distincts de* A
(ii)- a *est premier dans* $A \Leftrightarrow (a)$ *est premier de* A.

Preuve. *(i)- Si* a *est irréductible,* $a \notin \mathcal{U}(A)$ *et donc* $(a) \neq A$ *; Par ailleurs, si* $J = (b)$ *est un idéal principal de* A, *distinct de* A *tel que* $(a) \subset J$, *alors* b/a *ou encore, il existe* $c \in A$ *tel que* $a = bc$. *Puisque* (a) *est irréductible et* $b \notin \mathcal{U}(A)$ *(car* $J \neq A$*) ceci implique que* $c \in \mathcal{U}(A)$. *Ainsi,* a *et* b *sont asoociés et donc* $(a) = (b) = J$. *Ceci prouve que* (a) *est maximal parmi les idéaux principaux distincts de* A.

Réciproquement, soit $a \in A$, *tel que* (a) *soit maximal parmi les idéaux principaux distincts de* A. *Comme* $(a) \neq A, a \notin \mathcal{U}(A)$. *De plus, si* $x, y \in A$ *tel que* $a = xy$ *alors* $(a) \subset (x)$ *et d'après la maximalité de* (a) *on a* $(x) = A$ *ou* $(x) = (a)$. *Si* $(x) = A$, $x \in \mathcal{U}(A)$ *; Sinon* x *et* a *sont associés, et donc,* a *est de la forme* λx *pour un certain* $\lambda \in \mathcal{U}(A)$, *on obtient alors* $xy = a = \lambda x$ *et on en déduit par intégrité de* A *que* $y = \lambda \in \mathcal{U}(A)$.

(ii)- a *est premier* $\Leftrightarrow a \notin \mathcal{U}(A)$ *et* $(\forall (x, y) \in A^2, a/xy \Rightarrow a/x$ *ou* $a/y) \Leftrightarrow (a) \neq A$ *et* $(\forall (x, y) \in A^2,\ xy \in (a) \Rightarrow x \in (a)$ *ou* $y \in (a))$ $\Leftrightarrow a$ *est premier de* A. ■

Remarques. — *Tout élément de* A, *associé à un élément irréductible dans* A *est encore irréductible dans* A.

— *Tout élément de* A, *associé à un élément premier dans* A *est aussi un élément premier dans* A.

— *Les éléments irréductibles (et aussi les éléments premiers) dans* $\mathbb{Z}$*, sont les nombres premiers et leurs opposés.*

— *Tout élément d'un corps est réductible (non irréductible).*

Proposition IV.2.2. *Soit* A *un anneau intègre. Tout élément non nul et premier dans* A *est irréductible dans* A*.*

Preuve. *Soit* a *un élément non nul et premier dans* A*, on a alors* $a \notin \mathcal{U}(A)$*. De plus, si* $a = xy$ *avec* $x, y \in A$*, en particulier* a/xy *d'où* a/x *ou* a/y*. Supposons que* a/x*, il existe* $z \in A$ *tel que* $x = az$ *et, par suite,* $a = xy = azy$*. Comme* $a \neq 0$ *et* A *est intègre, on obtient* $zy = 1$*, donc* $y \in \mathcal{U}(A)$*. De même, si* a/y*, on aura alors* $x \in \mathcal{U}(A)$*. Ce qui prouve que* a *est irréductible dans* A*.* ■

Remarque. *La réciproque est fausse généralement. En effet, si on considère* $A = \mathbb{Z}[i\sqrt{5}]$*, c'est un anneau intègre. On rappelle que* $N(a + ib\sqrt{5}) = a^2 + 5b^2$ *et que* $N(xy) = N(x)N(y), \forall x, y \in A$*. On vérifie que* 3 *est irréductible,* $3/(1 + i\sqrt{5})(1 - i\sqrt{5})$ *mais* 3 *ne divise ni* $(1 + i\sqrt{5})$ *ni* $(1 - i\sqrt{5})$*. On conclut que* 3 *n'est pas premier dans* A*.*

IV.3 Eléments Premiers entre-eux, PGCD, PPCM

Définition IV.3.1. *Soit* A *un anneau intègre.*

— *(i) Soit* $a, b \in A$*. On dit que* a *et* b *sont premiers entre-eux si les seuls éléments de* A *qui divisent à la fois* a *et* b *sont les éléments de* $\mathcal{U}(A)$*.*

— *(ii) Des éléments* $a_1, a_2, \cdots, a_n \in A$ *sont dits premiers dans leur ensemble si les éléments de* $\mathcal{U}(A)$ *sont les seuls diviseurs communs.*

Remarque. *Si* a *est premier avec* b*, alors* a *est premier avec* $\lambda b, \forall \lambda \in \mathcal{U}(A)$*.*
En termes d'idéaux, la définition de deux éléments premiers entre eux s'exprime comme suit : a *est premier avec* $b \Leftrightarrow \forall x \in A$*,* $(a) \subset (x)$ *et* $(b) \subset (x) \Rightarrow (x) = A$*.*

Proposition IV.3.1. *Soit* A *un anneau intègre. Tout élément irréductible est premier avec tout élément qu'il ne divise pas.*

Preuve. *Soit* a *un élément irréductible dans* A*. Soit* b *un élément de* A *tel que* a *ne divise pas* b*. supposons qu'il existe* $d \in A$ *non inversible tel que* d *divise à la fois* a *et* b*. Il existerait alors* $a', b' \in A$ *tel que* $a = da'$ *et* $b = db'$*. Or,* a *est irréductible et* $d \notin \mathcal{U}(A)$*, par conséquent,* $a' \in \mathcal{U}(A)$ *et par suite,* $b = db' = aa'^{-1}b'$*. Ainsi,* a *divise* b*, ce qui est contradictoire avec l'hypothèse.* ■

Définition IV.3.2. *Soit* A *un anneau intègre. Soit* $n \in \mathbb{N}^*$ *et* $a_1, a_2, \cdots, a_n \in A$*.*

— *(i) On dit que* $(a_i)_{1\leq i\leq n}$ *admet un plus grand commun diviseur dans* A *s'il existe un élément* $d \in A$ *tel que*

  — $\forall i \in \{1, 2, \cdots, n\}$, d/a_i

  — *Si* $d' \in A$ *avec* $d'/a_i, \forall i \in \{1, 2, \cdots, n\}$ *alors* d'/d.

  On écrit alors que $d = pgcd(a_1, a_2, \cdots, a_n)$ *ou* $d = a_1 \wedge a_2, \cdots \wedge a_n$.

— *(ii) On dit que* $(a_i)_{1\leq i\leq n}$ *admet un plus petit commun multiple dans* A *lorsqu'il existe un élément* $\mu \in A$ *tel que*

  — $\forall i \in \{1, 2, \cdots, n\}$, a_i *divise* μ

  — *Si* m *est un élément de* A *qui est divisible par* a_i *pour tout* $i \in \{1, 2, \cdots, n\}$, m *est divisible aussi par* μ.

  On écrit alors $\mu = ppcm(a_1, a_2, \cdots, a_n)$ *ou* $\mu = a_1 \vee a_2 \cdots \vee a_n$.

Proposition IV.3.2. *Soit* A *un anneau intègre et* $a_1, a_2, \cdots, a_n$ *des éléments de* A. *Si* $d = pgcd(a_1, a_2, \cdots, a_n)$ *et* $\mu = ppcm(a_1, a_2, \cdots, a_n)$, *alors*

— *(i)* $\forall \delta \in A$, $\delta = pgcd(a_1, a_2, \cdots, a_n) \Leftrightarrow \delta$ *et* d *sont associés* $(\exists \lambda \in \mathcal{U}(A), \delta = \lambda d)$

— *(ii)* $\forall m \in A, m = ppcm(a_1, a_2, \cdots, a_n) \Leftrightarrow m$ *et* μ *sont associés* $(\exists \lambda \in \mathcal{U}(A), m = \lambda\mu)$

— *(iii)* $a_1, a_2, \cdots, a_n$ *sont premiers dans leur ensemble* $\Leftrightarrow 1 = pgcd(a_1, a_2, \cdots, a_n)$.

Preuve. *(i)- Si* $\delta = pgcd(a_1, a_2, \cdots, a_n)$, δ *est alors un diviseur commun des* a_i *et donc puisque* d *est un pgcd des* a_i, *on a* δ/d. *De même* d/δ *et donc* δ *et* d *sont associés. Réciproquement, si* δ *et* d *sont associés, ils ont les mêmes diviseurs, d'où le résultat.*

(iii)- On suppose que $a_1, \cdots, a_n$ *sont premiers dans leur ensemble. Ainsi, si* d *est un diviseur commun des* a_i, $d \in \mathcal{U}(A)$ *et donc* d *divise* 1 *et comme* 1 *divise chaque* a_i, *on conclut alors que* $1 = pgcd(a_1, a_2, \cdots, a_n)$. *Réciproquement, soit* d *un diviseur commun des* a_i, *puisque* $1 = pgcd(a_1, a_2, \cdots, a_n)$ *on a* d *divise* 1 *et donc* $d \in \mathcal{U}(A)$. ■

Remarque. *Soit* $x, y \in A$:
Si $x = 0$ *et* $y = 0$, x *et* y *admettent un pgcd unique qui est* 0.
Si $x = 0$ *et* $y \neq 0$, x *et* y *admettent un pgcd qui est* y *ou tout élément associé à* y.
Si x/y *alors* x *et* y *admettent un pgcd qui est* x *ou tout élément associé à* x. *En particulier pour tout* $u \in \mathcal{U}(A)$, $u \wedge x = x$.
On n'a pas toujours l'existence d'un pgcd de deux éléments quelconques d'un anneau intègre. Par exemple : considérons l'anneau $\mathbb{Z}[i\sqrt{5}]$. *Soit* $x = 6$ *et* $y = 2(1 + i\sqrt{5})$. $x = 2 \times 3 = ((1 + i\sqrt{5})(1 - i\sqrt{5})$, *on a* $2/x$ *et* $2/y$, *de même* $(1 + i\sqrt{5})/x$ *et* $(1 + i\sqrt{5})/y$. *Si le* $pgcd(x, y)$ *existe, soit* $d = pgcd(x, y)$ *alors* $2/d$ *et* $(1 + i\sqrt{5})/d$ *d'où* $N(2)/N(d)$ *et* $N(1 + i\sqrt{5})/N(d)$, *i.e.* $4/N(d)$ *et* $6/N(d)$. *Par ailleurs, comme* d/x *et* d/y *ona alors*

$N(d)/36$ *et* $N(d)/24$. *on en déduit que* $N(d) = 12$ *autrement écrit* $a^2 + 5b^2 = 12$ *où* $a + ib\sqrt{5} = d$ *ceci est impossible.*

Dans la suite, on limite l'étude à une classe particulière d'anneaux dits principaux où l'existence du pgcd (et ppcm) est assurée. Par suite, on pourra généraliser les résultats d'arithmétique connus dans l'anneau $\mathbb{Z}$ à ces anneaux.

IV.4 Arithmétique dans un Anneau Principal

Définition IV.4.1. *On appelle anneau principal tout anneau intègre dans lequel tout idéal est principal (i.e. engendré par un seul élément).*

Exemple. $(\mathbb{Z}, +, \cdot)$ *est un anneau principal.*

Tout corps commutatif est un anneau principal.

Proposition IV.4.1. *Soit* A *un anneau principal. Alors tout élément non nul et irréductible est premier.*

Preuve. *Soit* a *un élément non nul et irréductible dans* A. *D'après la proposition IV.2.1, l'idéal* (a) *est maximal parmi les idéaux principaux et distincts de* A. *Comme* A *est principal, tous ses idéaux sont principaux, donc* (a) *est un idéal maximal de* A. *Puisque tout idéal maximal est premier,* (a) *est premier de* A. *On conclut de la proposition IV.2.1 que* a *est un élément premier dans* A. ■

Remarques. — *Dans un anneau principal, les notions d'élément premier et d'élément irréductible sont identiques.*

— $\mathbb{Z}[i\sqrt{5}]$ *n'est pas principal.*

Théorème IV.1. *soit* A *un anneau principal et* $a_1, a_2, \cdots, a_n \in A$. *Alors* $a_1, a_2, \cdots, a_n$ *admettent un pgcd et un ppcm dans* A.
Plus précisément, tout générateur de $\sum_{i=1}^{n}(a_i)$ *est un pgcd de* $a_1, a_2, \cdots, a_n$,
$(d = pgcd(a_1, a_2, \cdots, a_n) \Leftrightarrow \sum_{i=1}^{n}(a_i) = (d))$;
et tout générateur de $\bigcap_{1\leq i\leq n}(a_i)$ *est un ppcm de* $a_1, a_2, \cdots, a_n$,
$(\mu = ppcm(a_1, a_2, \cdots, a_n) \Leftrightarrow \bigcap_{1\leq i\leq n}(a_i) = (\mu))$.

Preuve. *Soit* I *l'idéal engendré par les éléments* $a_1, a_2, \cdots, a_n$, *(ou encore* $I = (a_1) + (a_2) + \cdots + (a_n)$*). Comme* A *est principal,* I *est principal et donc il existe* $d \in A$ *tel que* $I = (d)$. *Montrons que* $d = pgcd(a_1, a_2, \cdots, a_n)$.
On a pour tout $i \in \{1, 2, \cdots, n\}$, $(a_i) \subset (d)$ *donc* d/a_i *pour tout* i. *Soit* $d' \in A$ *tel que* $d'/a_i, \forall i \in \{1, 2, \cdots, n\}$, *donc* $(a_i) \subset (d')$ *pour tout* i, *ce qui implique* $\sum_{i=1}^{n}(a_i) \subset (d')$, *i.e.* $(d) \subset (d')$ *et donc* d'/d. *Ceci prouve que* $d = pgcd(a_1, a_2, \cdots, n)$.

Soit maintenant $d' = pgcd(a_1, a_2, \cdots, a_n)$ *et* d *tel que* $(d) = \sum_{i=1}^{n}(a_i)$. *D'après ce qui précède* $d = pgcd(a_1, a_2, \cdots, a_n)$ *et par conséquent* d *et* d' *sont associés, donc* $(d) = (d')$, *i.e.* $\sum_{i=1}^{n}(a_i) = (d')$.

Soit $J = \bigcap_{i=1}^{n}(a_i)$, $\exists \mu \in A$ *tel que* $J = (\mu)$. *Montrons que* $\mu = ppcm(a_1, a_2, \cdots, a_n)$. $\forall i \in \{1, 2, \cdots, n\}$, $(\mu) \subset (a_i)$, *donc* a_i *divise* μ *pour tout* i, *et si* $m \in A$ *tel que* $\forall i, a_i/m$ *alors* $(m) \subset (a_i)$ *pour tout* i *d'où*$(m) \subset \bigcap_{i=1}^{n}(a_i)$, *donc* μ/m *et* $\mu = ppcm(a_1, a_2, \cdots, a_n)$.

Réciproquenement, si $\mu' = ppcm(a_1, a_2, \cdots, a_n)$ *alors* μ *et* μ' *sont associés d'où* $(\mu') = (\mu) = \bigcap_{i=1}^{n}(a_i)$. ■

Théorème IV.2. *(Théorème de Bézout) Soit* A *un anneau principal et* $a_1, a_2, \cdots, a_n$ *des éléments de* A.

$a_1, a_2, \cdots, a_n$ *sont premiers dans leur ensemble si et seulement si il existe* $u_1, u_2, \cdots, u_n \in A$ *tel que* $u_1a_1 + u_2a_2 + \cdots + u_na_n = 1$ *(Identité de Bézout).*

Preuve. $a_1, a_2, \cdots, a_n$ *sont premiers dans leur ensemble* $\Leftrightarrow 1 = pgcd(a_1, a_2, \cdots, a_n)$ *(d'après la proposition IV.3.2)*

$\Leftrightarrow A = (a_1) + (a_2) + \cdots + (a_n)$ *(d'après le Théorème précédent)*

$\Leftrightarrow 1 \in (a_1) + (a_2) + \cdots + (a_n)$

$\Leftrightarrow \exists u_1, u_2, \cdots, u_n \in A$ *tel que* $1 = u_1a_1 + u_2a_2 + \cdots + u_na_n$. ■

Remarques. — *On n'a pas l'unicité des* u_i *qui vérifient l'identité de Bézout.*

— *Soit* A *un anneau principal et* $a_1, a_2, \cdots, a_n \in A$

(i) $d = pgcd(a_1, a_2, \cdots, a_n) \Rightarrow \exists u_1, u_2, \cdots, u_n \in A$, $\sum_{i=1}^{n} u_ia_i = d$. *(Attention ! la réciproque n'est pas vraie).*

(ii) $\exists u_1, u_2, \cdots, u_n \in A, \sum_{i=1}^{n} u_ia_i = d \Rightarrow d/pgcd(a_1, a_2, \cdots, a_n)$

(iii) $(\forall i \in \{1, 2, \cdots, n\}, d/a_i)$ *et* $(\exists u_1, u_2, \cdots, u_n \in A, \sum_{i)=1}^{n} u_ia_i = d) \Rightarrow d = pgcd(a_1, a_2, \cdots, a_n)$

Théorème IV.3. *(Théorème de Gauss) Soit* A *un anneau principal et* $a, b, c \in A$. *Alors :* a/bc *et* $pgcd(a, b) = 1 \Rightarrow a/c$.

Preuve. a/bc *et* $pgcd(a, b) = 1 \Leftrightarrow (\exists a' \in A, bc = aa')$ *et* $(\exists u, v \in A, ua + vb = 1)$ *(d'après le Théorème de Bézout)*

$\Rightarrow c = acu + bcv = acu + aa'v = a(cu + a'v)$ *avec* $u, v, c, a' \in A$

$\Leftrightarrow a/c$.■

Proposition IV.4.2. *Soit* A *un anneau principal et* $a, b, c \in A$. *Alors*

— *(i)* $(a \wedge b = 1, a/c$ *et* $b/c) \Rightarrow ab/c$.

— *(ii)* $(a \wedge b = 1$ *et* $a \wedge c = 1) \Rightarrow a \wedge bc = 1$.

— *(iii)* $a \wedge b = d \Rightarrow \exists a', b' \in A,\ a = da',\ b = db'$ *et* $a' \wedge b' = 1$.

— *(iv)* $(a \wedge b)(a \vee b) = ab$.

Preuve. *Exercice.*

Nous allons achever ce paragraphe par l'une des propriétés fondamentales des anneaux principaux qui est la décomposition des éléments de A en produit de facteurs irréductibles.

Proposition IV.4.3. *Soit A un anneau principal. Soit a un élément de A. Si a est non nul et non inversible dans A alors il existe un élément irréductible dans A qui divise a.*

Preuve. *Soit $a \in A$ tel que a est non nul et $a \notin \mathcal{U}(A)$. D'après le corollaire II.2, (a) est contenu dans un idéal maximal I. Comme A est principal, $I = (p)$ pour un certain $p \in A$, or, $I = (p)$ est maximal, d'après la proposition IV.2.1, p est alors irréductible. Donc, il existe un élément p irréductible dans A tel que $(a) \subset (p)$, ce qui équivaut à p divise a avec p un élément irréductible dans A.* ■

Proposition IV.4.4. *Soit A un anneau principal et $a, b, p \in A$. Alors :*

$(p$ *irréductible et* $p/ab) \Rightarrow (p/a$ *ou* $p/b)$

Preuve. *Soit $a, b, p \in A$ tel que p est irréductible et p/ab. Supposons que p ne divise pas a, d'après la proposition IV.3.1, p et a sont premiers entre-eux et, en utilisant le théorème de Gauss, on aura nécessairement p/b.* ■

Théorème IV.4. *Soit A un anneau principal. Tout élément non nul et non inversible de A a une décomposition $a = p_1, p_2, \cdots, p_m$ comme produit d'éléments irréducctibles. Cette décomposition est unique à un multiplicatif d'associés près.*

Preuve. *Démontrons d'abord l'existence de la décomposition. On utilise la proposition IV.4.3 et le lemme suivant :*

Lemme 2. *Soit A un anneau principal. Toute suite croissante $I_0 \subset I_1 \subset \cdots I_i \subset I_{i+1} \subset \cdots$ d'idéaux est stationnaire, i.e. il existe $k \in \mathbb{N}$ tel que si $i \geq k$, $I_i = I_k$.*

Preuve. *En effet, comme (I_j) est totalement ordonnée, $\bigcup I_j$ est un idéal de A et donc $\bigcup I_j = (a)$ pour un certain $a \in A$ puisque A est principal. Par suite, il existe $k \in \mathbb{N}$ tel que $a \in I_k$ d'où $(a) \subset I_k$ et donc $(a) = I_k$; ainsi $\forall l \geq k$, $I_l = (a) = I_k$.* □

Revenons à la démonstration du théorème. Soit $a \in A$ tel que $a \neq 0$, i.e. $a \notin \mathcal{U}(A)$. D'après la proposition IV.4.3, $a = p_1 a_1$ avec p_1 irréductible.

Si $a_1 \in \mathcal{U}(A)$ alors $p_1 a_1$ est irréductible (i.e. a est irréductible).

Si $a_1 \notin \mathcal{U}(A)$, on aura une inclusion stricte $(a) \subset (a_1)$. De même, $a_1 = p_2 a_2$ avec p_2 irréductible.

On continue ainsi par récurrence. Si le processus se poursuit indéfiniment, on obtiendrait une suite infinie d'idéaux $(a) \subset (a_1) \subset (a_2) \cdots$ strictement croissante, ce qui est contradictoire avec le lemme. Donc $a = p_1 p_2 \cdots p_k u$ avec $p_1, p_2, \cdots, p_k$ des éléments irréductibles et $u \in \mathcal{U}(A)$, et donc $p_k u$ est irréductible d'où l'existence de la décomposition.

Montrons l'unicité par récurrence sur le nombre minimum k de facteurs irréductibles dans les diverses décompositions $a = p_1 p_2 \cdots p_k$ de a en produit d'éléments irréductibles.

Pour $k = 1$, on a $a = p_1$ et $a = q_1 q_2 \cdots q_m$ une autre décomposition de a en produit d'éléments irréductibles, supposons que $m > 1$, alors q_1 divise p_1 et comme p_1 est irréductible $q_1 = u p_1$ pour un certain $u \in \mathcal{U}(A)$ d'où $a = p_1 = u p_1 q_2 \cdots q_m$. Par intégrité de A on obtient $1 = u q_2 q_3 \cdots q_m$ d'où q_2 est inversible. Ceci est absurde, donc $m = 1$ et $p_1 = a = q_1$. Soit $k \geq 2$, supposons l'unicité pour les éléments de A qui sont en produit d'au plus $k-1$ facteurs irréductibles. Soit $a = p_1 p_2 \cdots p_k$ un produit de k facteurs irréductibles. Si $a = q_1 q_2 \cdots q_m$ est une autre décomposition de a en facteurs irréductibles, d'après la proposition IV.4.4, il existe $1 \leq i \leq m$ tel que p_1 divise q_i. Quitte à permuter les q_i, on peut supposer que p_1 divise q_1, on en déduit que $q_1 = u p_1$ pour un certain $u \in \mathcal{U}(A)$ et donc $a = p_1 p_2 \cdots p_k = u p_1 q_2 \cdots q_m$ et par intégrité de A, on obtient $b = p_2 p_3 \cdots p_k = u q_2 \cdots q_m$. L'élément $b \in A$ est produit de $k-1$ facteurs irréductibles ; d'après l'hypothèse de récurrence $m - 1 = k - 1$, donc $k = m$ et il existe une permutation de $\{2, \cdots, k\}$ tel que p_i et $q_{\sigma(i)}$ sont associés. Donc, si $a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$ alors $k = m$ et il existe $\sigma \in S_k$ tel que $\forall i \in \{1, 2, \cdots, k\}$, p_i et $q_{\sigma(i)}$ sont associés. La décomposition est ainsi unique. ■

Remarque. *Dans un anneau principal A, on n'a pas toujours (comme dans $\mathbb{Z}$) un choix canonique de représentants dans chaque classe d'éléments irréductibles associés.*

Définition IV.4.2. *On appelle système d'irréductibles (ou de représentants) dans l'anneau principal A, une famille $\mathcal{P} = (x_i)_{i \in I}$ d'éléments irréductibles de A tel que*

(i) tout élément irréductible de A est associé à un x_i pour un certain $i \in I$,

(ii) si $i \neq j$, $\overline{x_i} \neq \overline{x_j}$, i.e. x_i et x_j ne sont pas associés.

Donc, pour tout élément $a \in A \setminus \{0\}$ tel que $a \notin \mathcal{U}(A)$, a s'écrit sous la forme $a = u p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ avec $u \in \mathcal{U}(A), p_1, p_2, \cdots, p_m \in \mathcal{P}$ distincts et $\alpha_1, \cdots, \alpha_m \in \mathbb{N}^*$.