# ANNEAUX

B. Landelle

## Table des matières

Les démonstrations qui ne sont pas détaillées ont été vues dans le chapitre **Structures**. La mention *entier* (sans précision) fait référence à entier naturel.

# I Structure d'anneau

## 1 Définitions, propriétés

**Définition 1.** *On appelle* anneau *un triplet* $(\mathrm{A},+,\times)$ *avec* A *un ensemble (non vide) muni de deux lois de compositions internes* $+$ *et* $\times$ *telles que :*

1. $(\mathrm{A},+)$ *est un groupe abélien de neutre* $0_\mathrm{A}$ *;*
2. $\times$ *est associative ;*
3. $\times$ *possède un neutre* $1_\mathrm{A}$ *;*
4. $\times$ *est distributive sur* $+$*, i.e.*

$$\forall (x,y,z)\in \mathrm{A}^3 \qquad x(y+z)=xy+xz \quad et \quad (x+y)z=xz+yz$$

*Si la loi* $\times$ *est commutative, l'anneau* $(\mathrm{A},+,\times)$ *est dit* commutatif.

**Remarques :** (1) Soit $x\in\mathrm{A}$. On a $0_\mathrm{A}x=0_\mathrm{A}$ (en écrivant $0_\mathrm{A}+0_\mathrm{A}=0_\mathrm{A}$) et $(-1_\mathrm{A})x=-x$ (en écrivant $1_\mathrm{A}-1_\mathrm{A}=0_\mathrm{A}$).
(2) L'anneau nul $\{0_\mathrm{A}\}$ est le seul pour lequel $0_\mathrm{A}=1_\mathrm{A}$. On le rencontre par exemple avec $(\mathscr{L}(\mathrm{E}),+,\circ)$ et $\mathrm{E}=\{0_\mathrm{E}\}$.

**Notations :** Soit $x\in\mathrm{A}$. On pose $0x=0_\mathrm{A}$ puis $(k+1)x=kx+x$ et $-(k+1)x=(-k)x-x$ pour $k$ entier. Puis, on pose $x^0=1_\mathrm{A}$ et $x^{n+1}=x^nx$ pour $n$ entier. On note simplement 0 et 1 les éléments neutres de $(\mathrm{A},+,\times)$ quand il n'y a pas de confusion possible.

**Proposition 1.** *Soit* $(\mathrm{A},+,\times)$ *un anneau. On a*

$$\forall (x,y,k)\in \mathrm{A}^2\times\mathbb{Z} \qquad (kx)y=k(xy)=x(ky)$$

*Démonstration.* Par récurrence pour $k$ entier puis prolongement si $k$ est entier négatif. □

**Proposition 2.** *Soit* $(\mathrm{A},+,\times)$ *un anneau et* $(x,y)\in\mathrm{A}^2$ *avec* $xy=yx$*. On a*

$$\forall (m,n)\in\mathbb{N}^2 \qquad x^my^n=y^nx^m$$

**Remarque :** En particulier, pour $x\in\mathrm{A}$ et $n$ entier, on a $x^{n+1}=xx^n=x^nx$.

**Proposition 3.** *Soit* $(\mathrm{A},+,\times)$ *un anneau et* $(x,y)\in\mathrm{A}^2$ *tel que* $xy=yx$*. On a pour tout* $n$ *entier avec commutation dans le dernier produit*

$$(xy)^n=x^ny^n \qquad (x+y)^n=\sum_{k=0}^{n}\binom{n}{k}x^ky^{n-k} \qquad x^n-y^n=(x-y)\sum_{k=0}^{n-1}x^ky^{n-1-k}$$

**Définition 2.** *Un anneau commutatif* $(\mathrm{A},+,\times)$ *est dit* intègre *s'il est non réduit à* $\{0_\mathrm{A}\}$ *et si*

$$\forall (x,y)\in\mathrm{A}^2 \qquad xy=0_\mathrm{A} \implies x=0_\mathrm{A} \quad ou \quad y=0_\mathrm{A}$$

**Définition 3.** *On appelle* sous-anneau *d'un anneau* $(\mathrm{A},+,\times)$ *une partie* B *de* A *vérifiant :*

1. $1_\mathrm{A}\in\mathrm{B}$ *;*
2. $\forall (x,y)\in\mathrm{B}^2 \qquad x-y\in\mathrm{B}$ *;*
3. $\forall (x,y)\in\mathrm{B}^2 \qquad xy\in\mathrm{B}$.

**Proposition 4.** *Si* $\mathrm{B}$ *est un sous-anneau de* $(\mathrm{A},+,\times)$*, alors* $(\mathrm{B},+,\times)$ *possède une structure d'anneau. Si l'anneau* $(\mathrm{A},+,\times)$ *est commutatif, alors l'anneau* $(\mathrm{B},+,\times)$ *l'est aussi.*

**Exemple :** $\mathbb{Z}[\sqrt{2}] = \left\{a+b\sqrt{2},\ (a,b)\in\mathbb{Z}^2\right\}$ est un sous-anneau de l'anneau commutatif $(\mathbb{R},+,\times)$.

## 2 Groupe des inversibles

**Définition 4.** *Soit* $(\mathrm{A},+,\times)$ *un anneau. Un élément* $x\in\mathrm{A}$ *est dit* inversible *s'il existe* $y\in\mathrm{A}$ *tel que*

$$xy = yx = 1_{\mathrm{A}}$$

*On note* $\mathrm{U}(\mathrm{A})$ *ou* $\mathrm{A}^\times$ *l'ensemble des éléments inversibles de* $\mathrm{A}$.

**Remarque :** Si l'anneau est non nul, alors on a $\mathrm{U}(\mathrm{A})\subset \mathrm{A}\setminus\{0_{\mathrm{A}}\}$ puisque $0_{\mathrm{A}}x = 0_{\mathrm{A}} \neq 1_{\mathrm{A}}$ pour tout $x\in\mathrm{A}$.

**Proposition 5.** *Soit* $(\mathrm{A},+,\times)$ *un anneau. Le couple* $(\mathrm{U}(\mathrm{A}),\times)$ *est un groupe.*

## 3 Anneau produit

**Définition 5.** *Soient* $(\mathrm{A}_1,+,\times)$, ... $(\mathrm{A}_n,+,\times)$ *des anneaux et* $\mathrm{A}=\prod_{i=1}^{n}\mathrm{A}_i$*. On définit les* lois produits $+$ *et* $\times$ *sur* $\mathrm{A}$ *par*

$$\forall (x,y)\in\mathrm{A}^2 \qquad x+y=(x_1+y_1,\dots,x_n+y_n) \quad \text{et} \quad xy=(x_1y_1,\dots,x_ny_n)$$

**Théorème 1.** *Soient* $(\mathrm{A}_1,+,\times)$, ... $(\mathrm{A}_n,+,\times)$ *des anneaux et* $\mathrm{A}=\prod_{i=1}^{n}\mathrm{A}_i$*. L'ensemble* $\mathrm{A}$ *muni des lois produits* $+$ *et* $\times$ *est un anneau dont les neutres sont respectivement* $0_{\mathrm{A}}=(0_{\mathrm{A}_1},\dots,0_{\mathrm{A}_n})$ *et* $1_{\mathrm{A}}=(1_{\mathrm{A}_1},\dots,1_{\mathrm{A}_n})$*. Si les* $(\mathrm{A}_i,+,\times)$ *sont des anneaux commutatif, alors l'anneau produit l'est aussi.*

*Démonstration.* L'ensemble $(\mathrm{A},+)$ est un groupe abélien de neutre $0_{\mathrm{A}}$ en tant que produit de groupes abéliens. La loi $\times$ sur $\mathrm{A}$ est associative, d'élément neutre $1_{\mathrm{A}}$ et distributive par rapport à $+$ par définition des lois $+$ et $\times$ sur $\mathrm{A}$ et propriétés des lois $+$ et $\times$ sur les $\mathrm{A}_i$. La transmission du caractère commutatif est immédiate. □

**Théorème 2.** *Soient* $(\mathrm{A}_1,+,\times)$, ... $(\mathrm{A}_n,+,\times)$ *des anneaux et* $\mathrm{A}=\prod_{i=1}^{n}\mathrm{A}_i$ *muni des lois produits. On a pour* $x=(x_1,\dots,x_n)\in\mathrm{A}$

$$x\in\mathrm{U}(\mathrm{A}) \iff \forall i\in[\![1\,;n]\!] \qquad x_i\in\mathrm{U}(\mathrm{A}_i)$$

*et dans ce cas*

$$x^{-1}=\left(x_1^{-1},\dots,x_n^{-1}\right)$$

*Enfin, on a*

$$\mathrm{U}(\mathrm{A})=\prod_{i=1}^{n}\mathrm{U}(\mathrm{A}_i)$$

*Démonstration.* Immédiate. □

**Exemple :** Soit $n$ entier non nul. On a $\mathrm{U}(\mathbb{Z}^n)=\{-1,1\}^n$.

## 4 Corps, sous-corps

**Définition 6.** *On appelle* corps *un anneau* $(\mathbb{K}, +, \times)$ *commutatif non réduit à* $\{0\}$ *et tel que tous les éléments de* $\mathbb{K} \setminus \{0\}$ *sont inversibles.*

**Remarque :** Une définition plus générale existe, sans l'hypothèse de commutativité mais celle-ci est hors-programme.

**Notations :** On note $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$. On a $\mathbb{K}^* = \mathrm{U}(\mathbb{K})$.

**Exemples :** $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{K}(\mathrm{X}), +, \times)$ sont des corps.
Soit $(\mathrm{A}, +, \times)$ sous-anneau d'un corps $(\mathbb{K}, +, \times)$. On définit le *corps des fractions* de A par

$$\left\{\frac{a}{b}, (a, b) \in \mathrm{A} \times \mathrm{A} \setminus \{0\}\right\}$$

**Proposition 6.** *Tout corps est un anneau intègre.*

*Démonstration.* Soit $(\mathbb{K}, +, \times)$ un corps et $(x, y) \in \mathbb{K}^2$. Si $x \neq 0$, alors

$$xy = 0 \quad \Longrightarrow \quad x^{-1}xy = y = 0$$

Sinon, on a $x = 0$ et le résultat suit. □

**Définition 7.** *On appelle* sous-corps *d'un corps* $(\mathbb{K}, +, \times)$ *une partie* $\mathbb{L}$ *de* $\mathbb{K}$ *vérifiant :*

1. $(\mathbb{L}, +, \times)$ *est un sous-anneau de* $(\mathbb{K}, +, \times)$ *;*
2. *Tout élément non nul de* $\mathbb{L}$ *admet un inverse dans* $\mathbb{L}$*.*

**Proposition 7.** *Si* $\mathbb{L}$ *est un sous-corps de* $(\mathbb{K}, +, \times)$*, alors* $(\mathbb{L}, +, \times)$ *possède une structure de corps et* $\mathbb{K}$ *est un* $\mathbb{L}$*-ev.*

*Démonstration.* On a $(\mathbb{L}, +, \times)$ est un sous-anneau de $(\mathbb{K}, +, \times)$ donc $(\mathbb{L}, +, \times)$ est un anneau commutatif contenant 1 donc non réduit à $\{0\}$. Tout élément de $\mathbb{L} \setminus \{0\}$ est inversible dans $\mathbb{L}$. Enfin, on vérifie sans difficulté que le corps $\mathbb{K}$ est un $\mathbb{L}$-ev (y compris si $\mathbb{K}$ non commutatif mais que $\mathbb{L}$ l'est). □

**Vocabulaire :** On dit aussi que $\mathbb{K}$ est une *extension* du corps $\mathbb{L}$.

**Exemples :** $(\mathbb{Q}, +, \times)$ est un sous-corps de $(\mathbb{R}, +, \times)$ qui est un sous-corps de $(\mathbb{C}, +, \times)$.
Soit $\mathbb{Q}[\sqrt{2}] = \left\{a + b\sqrt{2}, (a, b) \in \mathbb{Q}^2\right\}$. L'ensemble $(\mathbb{Q}[\sqrt{2}], +, \times)$ est un corps.

# II Morphisme d'anneaux

## 1 Définition, propriétés

**Définition 8.** *Soient* $(\mathrm{A}, +, \times)$ *et* $(\mathrm{A}', +\times)$ *des anneaux. Une application* $\varphi : \mathrm{A} \to \mathrm{A}'$ *est un* morphisme d'anneaux *si :*

1. $\varphi(1_{\mathrm{A}}) = 1_{\mathrm{A}'}$ *;*
2. $\forall (x, y) \in \mathrm{A}^2 \qquad \varphi(x + y) = \varphi(x) + \varphi(y)$ *;*
3. $\forall (x, y) \in \mathrm{A}^2 \qquad \varphi(xy) = \varphi(x)\varphi(y)$.

*Si les deux anneaux sont égaux, l'application est un* endomorphisme *d'anneaux.*

**Remarque :** En particulier, le morphisme d'anneaux est un morphisme du groupe $(\mathrm{A}, +)$ vers le groupe $(\mathrm{A}', +)$.

**Exemples :** 1. L'identité $\mathrm{id} : \mathrm{A} \to \mathrm{A}$, l'application $\varphi : \mathbb{Z} \to \mathrm{A},\ k \mapsto k1_{\mathrm{A}}$.
2. Pour $a \in \mathrm{U}(\mathrm{A})$, l'application $\varphi_a : \mathrm{A} \to \mathrm{A},\ x \mapsto axa^{-1}$.
3. L'application $\varphi : \mathbb{C} \to \mathscr{M}_2(\mathbb{R}),\ a + \mathrm{i}b \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ (utiliser l'écriture trigonométrique).
4. L'application $\varphi : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}],\ a + b\sqrt{2} \mapsto a - b\sqrt{2}$ (bien définie, unicité de l'écriture dans $\mathbb{Z}[\sqrt{2}]$).

**Proposition 8.** *La composée de deux morphismes d'anneaux est un morphisme d'anneaux.*

*Démonstration.* Immédiate. □

**Proposition 9.** *Soit $\varphi$ un morphisme de l'anneau $(\mathrm{A}, +, \times)$ vers l'anneau $(\mathrm{A}', +, \times)$. On a :*

1. $\forall (x, k) \in \mathrm{A} \times \mathbb{Z} \qquad \varphi(kx) = k\varphi(x)$
2. $\forall (x, n) \in \mathrm{A} \times \mathbb{N} \qquad \varphi(x^n) = \varphi(x)^n$
3. $\forall x \in \mathrm{A} \qquad x \in \mathrm{U}(\mathrm{A}) \implies \varphi(x) \in \mathrm{U}(\mathrm{A}') \quad \text{et} \quad \varphi(x)^{-1} = \varphi(x^{-1})$

*Démonstration.* La première propriété résulte du fait que $\varphi$ est un morphisme de groupes de $(\mathrm{A}, +)$ vers $(\mathrm{A}', +)$, la deuxième s'obtient par récurrence, et la dernière est immédiate. □

**Remarque :** En particulier, on a $\varphi(0_{\mathrm{A}}) = 0_{\mathrm{A}'}$.

## 2 Noyau et image

**Définition 9.** *Soit $\varphi$ un morphisme de l'anneau $(\mathrm{A}, +, \times)$ vers l'anneau $(\mathrm{A}', +, \times)$. On appelle* image *du morphisme $\varphi$ l'ensemble noté* $\mathrm{Im}\ \varphi$ *défini par* $\mathrm{Im}\ \varphi = \varphi(\mathrm{A})$ *et* noyau *du morphisme $\varphi$ l'ensemble noté* $\mathrm{Ker}\ \varphi$ *défini par* $\mathrm{Ker}\ \varphi = \varphi^{-1}(\{0_{\mathrm{A}'}\})$.

**Remarque :** Ces notions coïncident avec celles du morphisme $\varphi$ du groupe $(\mathrm{A}, +)$ vers le groupe $(\mathrm{A}', +)$.

**Proposition 10.** *Soit $\varphi$ un morphisme de l'anneau $(\mathrm{A}, +, \times)$ vers l'anneau $(\mathrm{A}', +, \times)$. L'image du morphisme $\varphi$ est un sous-anneau de $(\mathrm{A}', +, \times)$.*

*Démonstration.* Immédiate. □

**Remarque :** Excepté le cas où $\mathrm{A}' = \{0_{\mathrm{A}'}\}$, le noyau d'un morphisme d'anneaux n'est pas un sous-anneau de $(\mathrm{A}, +, \times)$. En effet, on a $\varphi(1_{\mathrm{A}}) = 1_{\mathrm{A}'} \neq 0_{\mathrm{A}'}$ d'où $1_{\mathrm{A}} \notin \mathrm{Ker}\ \varphi$.

**Proposition 11.** *Soit $\varphi$ un morphisme de l'anneau $(\mathrm{A}, +, \times)$ vers l'anneau $(\mathrm{A}', +, \times)$. On a*

$$\varphi \text{ injective} \iff \mathrm{Ker}\ \varphi = \{0_{\mathrm{A}}\}$$

*Démonstration.* L'application est un morphisme de groupes de $(\mathrm{A}, +)$ vers $(\mathrm{A}', +)$. Le résultat suit. □

## 3 Isomorphisme d'anneaux

**Définition 10.** *On appelle* isomorphisme d'anneaux *un morphisme d'anneaux bijectif.*

**Définition 11.** *Deux anneaux sont dits* isomorphes *s'il existe un isomorphisme entre eux.*

**Notation :** On note $(\mathrm{A},+,\times) \simeq (\mathrm{A}',+,\times)$ ou plus simplement $\mathrm{A} \simeq \mathrm{A}'$ s'il n'y a aucune confusion sur les structures.

**Proposition 12.** *Une composée de deux isomorphismes d'anneaux est un isomorphisme d'anneaux.*

*Démonstration.* Immédiate. □

**Proposition 13.** *L'application réciproque d'un isomorphisme d'anneaux est un isomorphisme d'anneaux.*

*Démonstration.* Immédiate. □

**Définition 12.** *On appelle* automorphisme *d'un anneau* $(\mathrm{A},+,\times)$ *un isomorphisme de* $(\mathrm{A},+,\times)$ *dans lui-même.*

**Exemple :** Pour $a \in \mathrm{U}(\mathrm{A})$, l'application $\varphi_a : \mathrm{A} \to \mathrm{A}, x \mapsto axa^{-1}$ est un automorphisme de l'anneau $(\mathrm{A},+,\times)$.

# III Idéaux d'un anneau commutatif

Dans cette partie, le triplet $(\mathrm{A},+,\times)$ désigne un anneau commutatif.

## 1 Définitions, propriétés

**Définition 13.** *Soit* $(\mathrm{A},+,\times)$ *un anneau commutatif. On appelle* idéal *de cet anneau une partie* I *de* A *vérifiant :*

1. *l'ensemble* I *est un sous-groupe de* $(\mathrm{A},+)$ *;*
2. *propriété d'absorption :* $\forall (a,x) \in \mathrm{A}\times\mathrm{I} \qquad ax \in \mathrm{I}$

**Exemple :** Les parties $\{0_\mathrm{A}\}$ et A sont des idéaux dits *triviaux* de A.

**Proposition 14.** *Le noyau d'un morphisme d'un anneau commutatif vers un anneau est un idéal.*

*Démonstration.* Soit $\varphi$ un morphisme de l'anneau $(\mathrm{A},+,\times)$ commutatif vers l'anneau $(\mathrm{A}',+,\times)$ pas nécessairement commutatif. Le noyau $\mathrm{Ker}\,\varphi$ est un sous-groupe de $(\mathrm{A},+)$ puisqu'on peut voir $\varphi$ comme morphisme de groupes. Puis, soit $(a,x) \in \mathrm{A}\times\mathrm{Ker}\,\varphi$. On a $\varphi(ax) = \varphi(a)\varphi(x) = 0_{\mathrm{A}'}$ d'où $ax \in \mathrm{Ker}\,\varphi$. □

**Proposition 15.** *Une somme finie d'idéaux est un idéal contenant chacun des idéaux de la somme.*

**Proposition 16.** *Une intersection (quelconque) d'idéaux est un idéal.*

*Démonstration.* Soit $(\mathrm{I}_s)_{s\in\mathrm{S}}$ une famille d'idéaux avec S non vide et $\mathrm{I} = \bigcap_{s\in\mathrm{S}} \mathrm{I}_s$. L'ensemble I est un sous-groupe de $(\mathrm{A},+)$ comme intersection de sous-groupes. Soit $(a,x) \in \mathrm{A}\times\mathrm{I}$. On a $ax \in \mathrm{I}_s$ pour tout $s \in \mathrm{S}$ d'où $ax \in \mathrm{I}$. □

## 2 Idéal engendré

**Définition 14.** *Soit* $(\mathrm{A},+,\times)$ *un anneau commutatif et* $\mathrm{X}\subset\mathrm{A}$. *On appelle* idéal engendré *par* X *noté* $(\mathrm{X})$ *(notation non conventionnelle, à rappeler) l'intersection de tous les idéaux de* $(\mathrm{A},+,\times)$ *contenant* X *:*

$$(\mathrm{X})=\bigcap_{\mathrm{I}\in\mathscr{S}}\mathrm{I}\quad avec\quad \mathscr{S}=\{\mathrm{I}\ idéal\ de\ \mathrm{A}\mid \mathrm{X}\subset\mathrm{I}\}$$

**Remarque :** L'intersection porte sur un ensemble non vide puisque $\mathrm{A}\in\mathscr{S}$.

**Notation :** Pour $x\in\mathrm{A}$, on note simplement $(\{x\})=(x)$.

**Théorème 3.** *Soit* $(\mathrm{A},+,\times)$ *un anneau commutatif et* $\mathrm{X}\subset\mathrm{A}$. *L'ensemble* $(\mathrm{X})$ *est le plus petit idéal de* A *contenant* X.

*Démonstration.* L'ensemble $(\mathrm{X})$ est un idéal comme intersection d'idéaux, contient X et est contenu dans tout idéal contenant X par construction. □

**Proposition 17.** *Soit* $(\mathrm{A},+,\times)$ *un anneau commutatif et* $x\in\mathrm{A}$. *On a*

$$(x)=x\mathrm{A}\quad avec\quad x\mathrm{A}=\{xa,\ a\in\mathrm{A}\}$$

*Démonstration.* On a $x\in(x)$ d'où $xa\in(x)$ pour tout $a\in\mathrm{A}$ par absorption, autrement dit $x\mathrm{A}\subset(x)$ puis on vérifie sans difficulté que $x\mathrm{A}$ est un idéal contenant $x$ d'où le résultat. □

**Remarque :** Ainsi, pour $x\in\mathrm{A}$, on note simplement $x\mathrm{A}$ l'idéal engendré par $x$.

**Proposition 18 (À savoir refaire).** *Un anneau commutatif non nul est un corps si et seulement si ses seuls idéaux sont les idéaux triviaux.*

*Démonstration.* Soit $(\mathbb{K},+,\times)$ un corps et I un idéal non réduit à $\{0\}$ de $\mathbb{K}$. Soit $a\in\mathrm{I}\setminus\{0\}$. Par suite, pour tout $x\in\mathbb{K}$, on a $x=(xa^{-1})a\in\mathrm{I}$ d'où $\mathbb{K}\subset\mathrm{I}$ et l'autre inclusion est triviale. Réciproquement, supposons que $(\mathrm{A},+,\times)$ soit un anneau non nul avec pour seuls idéaux les idéaux triviaux. Soit $x\in\mathrm{A}\setminus\{0\}$. L'idéal engendré $x\mathrm{A}$ n'est pas réduit à $\{0\}$ donc est A lui même d'où $1_\mathrm{A}\in x\mathrm{A}$ et par suite, il existe $y\in\mathrm{A}$ tel que $xy=1$ ce qui prouve l'inversibilité de $x$. □

**Théorème 4.** *Les idéaux de* $(\mathbb{Z},+,\times)$ *sont les* $n\mathbb{Z}$ *avec* $n$ *entier.*

*Démonstration.* Les idéaux de $(\mathbb{Z},+,\times)$ sont sous-groupes de $(\mathbb{Z},+)$ donc de la forme $n\mathbb{Z}$ avec $n$ entier et il s'agit de l'idéal engendré par $n$. □

**Remarque :** On dit que $(\mathbb{Z},+,\times)$ est un *anneau principal* (on avait rencontré cette notion avec $\mathbb{K}[\mathrm{X}]$ dans le chapitre **Structures**).

## 3 Divisibilité dans un anneau commutatif intègre

Dans cette partie, le triplet $(\mathrm{A}, +, \times)$ désigne un anneau commutatif intègre (il y a redondance puisqu'un anneau intègre est commutatif).

**Définition 15.** *Soient $a, b$ dans* A. *On dit que $a$* divise *$b$ s'il existe $c \in \mathrm{A}$ tel que $b = ac$. On note $a|b$.*

**Proposition 19.** *Soient $a, b$ dans* A. *On a*

$$a|b \iff b \in a\mathrm{A} \iff b\mathrm{A} \subset a\mathrm{A}$$

**Proposition 20.** *Soient $a, b, c$ dans* A. *On a*

$$a|b \quad et \quad b|c \quad \Longrightarrow \quad a|c$$

$$a|b \quad et \quad a|c \quad \Longrightarrow \quad a|b+c$$

**Proposition 21.** *Soient $a, b, c$ dans* A. *On a*

$$ab = ac \quad et \quad a \neq 0 \quad \Longrightarrow \quad b = c$$

$$ab|ac \quad et \quad a \neq 0 \quad \Longrightarrow \quad b|c$$

**Définition 16.** *Soient $a, b$ dans* A. *On dit que $a$ et $b$ sont* associés *si $a$ divise $b$ et $b$ divise $a$.*

**Proposition 22.** *Soient $a, b$ dans* A. *On a*

$$a, b \text{ associés} \iff a\mathrm{A} = b\mathrm{A} \iff \exists c \in \mathrm{U(A)} \quad | \quad b = ac$$

**Corollaire 1.** *Soit* I *un idéal de $(\mathbb{Z}, +, \times)$. Il existe un unique entier $n$ tel que* $\mathrm{I} = n\mathbb{Z}$.

*Démonstration.* D'après le théorème 4, on dispose d'un entier $n$ tel que $\mathrm{I} = n\mathbb{Z}$. Soit $m$ entier tel que $n\mathbb{Z} = m\mathbb{Z}$. Ainsi, les entiers $n$ et $m$ sont associés donc égaux. □