Cours Algèbre 2 – III: Anneaux. Théorie Générale

Andrei Teleman

Département de Mathématiques, Aix-Marseille Université

6 avril 2021

Table of Contents

1. Introduction
   - Définition. Exemples. Règles de calcul dans un anneau
     - L'anneau des polynômes à coefficients dans un anneau commutatif
     - Règles de calcul dans un anneau
   - Diviseurs de zéro dans un anneau commutatifs. Anneaux commutatifs intègres
2. Sous-anneaux et idéaux. Anneaux quotients. Morphismes
   - Sous-anneaux et idéaux dans un anneau commutatif. Anneaux quotients
   - Morphismes d'anneaux. Le premier théorème d'isomorphisme
   - La caractéristique d'un anneau

Table of Contents

1 Introduction
- Définition. Exemples. Règles de calcul dans un anneau
  - L'anneau des polynômes à coefficients dans un anneau commutatif
  - Règles de calcul dans un anneau
- Diviseurs de zéro dans un anneau commutatifs. Anneaux commutatifs intègres

2 Sous-anneaux et idéaux. Anneaux quotients. Morphismes
- Sous-anneaux et idéaux dans un anneau commutatif. Anneaux quotients
- Morphismes d'anneaux. Le premier théorème d'isomorphisme
- La caractéristique d'un anneau

1

Définition 1.1

1. Un anneau est un triplet $(A,+,\cdot)$, où A est un ensemble et $+,\cdot$ sont deux lci sur A (appelées addition respectivement multiplication) telles que :

1

Définition 1.1

1. Un anneau est un triplet $(A,+,\cdot)$, où A est un ensemble et $+,\cdot$ sont deux lci sur A (appelées addition respectivement multiplication) telles que :
   - A1 $(A,+)$ est un groupe abélien. Son élément neutre sera appelé l'élément nul de l'anneau et sera noté 0_A ou 0.

1

Définition 1.1

1. Un anneau est un triplet $(A,+,\cdot)$, où A est un ensemble et $+,\cdot$ sont deux lci sur A (appelées addition respectivement multiplication) telles que :
   - A1 $(A,+)$ est un groupe abélien. Son élément neutre sera appelé l'élément nul de l'anneau et sera noté 0_A ou 0.
   - A2 La lci $\cdot$ est associative et admet un élément neutre. Cet élément neutre sera appelé l'élément unité de l'anneau et sera noté 1_A ou 1.

1

Définition 1.1

1. Un anneau est un triplet $(A,+,\cdot)$, où A est un ensemble et $+,\cdot$ sont deux lci sur A (appelées addition respectivement multiplication) telles que :
   - A1 $(A,+)$ est un groupe abélien. Son élément neutre sera appelé l'élément nul de l'anneau et sera noté 0_A ou 0.
   - A2 La lci $\cdot$ est associative et admet un élément neutre. Cet élément neutre sera appelé l'élément unité de l'anneau et sera noté 1_A ou 1.
   - A3 La lci $\cdot$ est distributive à gauche et à droite par rapport à la lci $+$, i.e. pour tout $(x,y,z)\in A\times A\times A$ on a :

$$x\cdot(y+z)=x\cdot y+x\cdot z,$$

$$(y+z)\cdot x=y\cdot x+z\cdot x.$$

1

Définition 1.1

1. Un anneau est un triplet $(A,+,\cdot)$, où A est un ensemble et $+,\cdot$ sont deux lci sur A (appelées addition respectivement multiplication) telles que :
   - A1 $(A,+)$ est un groupe abélien. Son élément neutre sera appelé l'élément nul de l'anneau et sera noté 0_A ou 0.
   - A2 La lci $\cdot$ est associative et admet un élément neutre. Cet élément neutre sera appelé l'élément unité de l'anneau et sera noté 1_A ou 1.
   - A3 La lci $\cdot$ est distributive à gauche et à droite par rapport à la lci $+$, i.e. pour tout $(x,y,z)\in A\times A\times A$ on a :

$$x\cdot(y+z)=x\cdot y+x\cdot z,$$

$$(y+z)\cdot x=y\cdot x+z\cdot x.$$

2. Un anneau $(A,+,\cdot)$ est dit commutatif si $\cdot$ est commutative.

2

Notations simplifiées :

2

Notations simplifiées :

Souvent on va omettre le symbole $\cdot$, donc, pour deux éléments $x, y \in A$ on va écrire xy au lieu de $x \cdot y$.

2

Notations simplifiées :

Souvent on va omettre le symbole $\cdot$, donc, pour deux éléments $x, y \in A$ on va écrire xy au lieu de $x \cdot y$.

Souvent on va désigner un anneau $(A, +, \cdot)$ par A, en sous-entendant qu'on a muni l'ensemble A de deux lci qui définissent une structure d'anneau.

Notations simplifiées :

Souvent on va omettre le symbole $\cdot$, donc, pour deux éléments $x, y \in A$ on va écrire xy au lieu de $x \cdot y$.

Souvent on va désigner un anneau $(A, +, \cdot)$ par A, en sous-entendant qu'on a muni l'ensemble A de deux lci qui définissent une structure d'anneau.

Définition 1.2

Deux éléments $x, y \in A$ sont dit commutables (permutables) si $xy = yx$.

2

Notations simplifiées :

Souvent on va omettre le symbole $\cdot$, donc, pour deux éléments $x, y \in A$ on va écrire xy au lieu de $x \cdot y$.

Souvent on va désigner un anneau $(A, +, \cdot)$ par A, en sous-entendant qu'on a muni l'ensemble A de deux lci qui définissent une structure d'anneau.

Définition 1.2

Deux éléments $x, y \in A$ sont dit commutables (permutables) si $xy = yx$.

Donc un anneau $(A, +, \cdot)$ est commutatif si et seulement si tous deux éléments de A sont permutables.

Exemples 1.1

1. Soit A un singleton dont l'élément sera noté 0. Les lci

$$(0,0) \stackrel{+}{\mapsto} 0,\ (0,0) \stackrel{\cdot}{\mapsto} 0$$

définissent une structure d'anneau sur $A = \{0\}$ avec $0_A = 1_A = 0$. Un tel anneau s'appelle anneau nul.

Exemples 1.1

1. Soit A un singleton dont l'élément sera noté 0. Les lci

$$(0,0) \overset{+}{\mapsto} 0, \ (0,0) \overset{\cdot}{\mapsto} 0$$

définissent une structure d'anneau sur $A = \{0\}$ avec $0_A = 1_A = 0$. Un tel anneau s'appelle anneau nul.

Un anneau A est nul si et seulement si $0_A = 1_A$. Pourquoi ?

Exemples 1.1

1. Soit A un singleton dont l'élément sera noté 0. Les lci

$$(0,0) \overset{+}{\mapsto} 0, \ (0,0) \overset{\cdot}{\mapsto} 0$$

   définissent une structure d'anneau sur $A = \{0\}$ avec $0_A = 1_A = 0$. Un tel anneau s'appelle anneau nul.

   Un anneau A est nul si et seulement si $0_A = 1_A$. Pourquoi ?

2. $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont des anneaux commutatifs.

3

Exemples 1.1

1. Soit A un singleton dont l'élément sera noté 0. Les lci

$$(0,0) \overset{+}{\mapsto} 0,\ (0,0) \overset{\cdot}{\mapsto} 0$$

définissent une structure d'anneau sur $A = \{0\}$ avec $0_A = 1_A = 0$. Un tel anneau s'appelle anneau nul.

Un anneau A est nul si et seulement si $0_A = 1_A$. Pourquoi ?

2. $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont des anneaux commutatifs.
3. Soit $n \in \mathbb{N}^*$. $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ est un anneau commutatif.

4

4. Soit $n \in \mathbb{N}^*$. $(M_{n,n}(\mathbb{Z}),+,\cdot)$, $(M_{n,n}(\mathbb{Q}),+,\cdot)$, $(M_{n,n}(\mathbb{R}),+,\cdot)$, $(M_{n,n}(\mathbb{C}),+,\cdot)$ sont des anneaux. Pour $n \geq 2$ ces anneaux ne sont pas commutatifs.

4

4. Soit $n \in \mathbb{N}^*$. $(M_{n,n}(\mathbb{Z}), +, \cdot)$, $(M_{n,n}(\mathbb{Q}), +, \cdot)$, $(M_{n,n}(\mathbb{R}), +, \cdot)$, $(M_{n,n}(\mathbb{C}), +, \cdot)$ sont des anneaux. Pour $n \geq 2$ ces anneaux ne sont pas commutatifs.
5. Soit E un espace vectoriel réel ou complexe. $(\mathrm{End}(E), +, \circ)$ est un anneau, non-commutatif pour $\dim(E) \geq 2$.

4

4. Soit $n \in \mathbb{N}^*$. $(M_{n,n}(\mathbb{Z}), +, \cdot)$, $(M_{n,n}(\mathbb{Q}), +, \cdot)$, $(M_{n,n}(\mathbb{R}), +, \cdot)$, $(M_{n,n}(\mathbb{C}), +, \cdot)$ sont des anneaux. Pour $n \geq 2$ ces anneaux ne sont pas commutatifs.
5. Soit E un espace vectoriel réel ou complexe. $(\mathrm{End}(E), +, \circ)$ est un anneau, non-commutatif pour $\dim(E) \geq 2$.
6. Soit $(G, +)$ un groupe abélien, 0_G son élément neutre. $(\mathrm{End}(G), +, \circ)$ est un anneau, en général non-commutatif. Son élément nul est l'endomorphisme trivial $x \mapsto 0_G$ et son élément unité est id_G.

5

7. Soient $(A,+,\cdot)$ un anneau, X un ensemble et soit $\mathcal{F}(X,A)$ l'ensemble des applications $X\to A$. Les lci $+,\cdot$ définies par

$$(f+g)(x)=f(x)+g(x),\ (f\cdot g)(x)=f(x)\cdot g(x)$$

définissent un structure d'anneau sur $\mathcal{F}(X,A)$. Cet anneau est commutatif si $(A,+,\cdot)$ est commutatif.

5

7. Soient $(A,+,\cdot)$ un anneau, X un ensemble et soit $\mathcal{F}(X,A)$ l'ensemble des applications $X\to A$. Les lci $+,\cdot$ définies par

$$(f+g)(x)=f(x)+g(x),\ (f\cdot g)(x)=f(x)\cdot g(x)$$

définissent un structure d'anneau sur $\mathcal{F}(X,A)$. Cet anneau est commutatif si $(A,+,\cdot)$ est commutatif.

8. Soient A, B deux anneaux dont les lci sont notées par les mêmes symboles. Alors les lci

$$((x,y),(x',y'))\mapsto(x+x',y+y'),\ ((x,y),(x',y'))\mapsto(xx',yy')$$

définissent un structure d'anneau sur le produit cartésien $A\times B$. Généralisation pour une famille $(A_i)_{i\in I}$ d'anneaux.

6

Soit A un anneau commutatif. On va noter par 0 son élément nul et par 1 son élément unité.

6

Soit A un anneau commutatif. On va noter par 0 son élément nul et par 1 son élément unité.

Définition 1.3

L'ensemble des polynômes à coefficients dans A est défini par

$$A[X] := \{(a_k)_{k\geq 0} |\ (\forall k \in \mathbb{N},\ a_k \in A) \wedge (\exists N \in \mathbb{N}, \forall k \geq N,\ a_k = 0)\}.$$

$(a, 0, 0 \ldots)$ s'appelle le polynôme constant associé à a.

Soit A un anneau commutatif. On va noter par 0 son élément nul et par 1 son élément unité.

Définition 1.3

L'ensemble des polynômes à coefficients dans A est défini par

$$A[X] := \{(a_k)_{k\geq 0} \mid (\forall k \in \mathbb{N},\ a_k \in A) \wedge (\exists N \in \mathbb{N}, \forall k \geq N,\ a_k = 0)\}.$$

$(a, 0, 0\dots)$ s'appelle le polynôme constant associé à a.

Donc un polynôme à coefficients dans A est une suite de A dont tous les termes sont nuls à partir d'un certain indice.

Soit A un anneau commutatif. On va noter par 0 son élément nul et par 1 son élément unité.

Définition 1.3

L'ensemble des polynômes à coefficients dans A est défini par

$$A[X] := \{(a_k)_{k\geq 0} | \, (\forall k \in \mathbb{N}, \, a_k \in A) \wedge (\exists N \in \mathbb{N}, \forall k \geq N, \, a_k = 0)\}.$$

$(a, 0, 0 \dots)$ s'appelle le polynôme constant associé à a.

Donc un polynôme à coefficients dans A est une suite de A dont tous les termes sont nuls à partir d'un certain indice.

$A[X]$ a une structure naturelle de groupe abélien, l'addition étant donnée par

$$((a_k)_{k\geq 0}) + ((b_k)_{k\geq 0}) := (a_k + b_k)_{k\geq 0}.$$

7

Définition 1.4

La multiplication dans $A[X]$: $((a_k)_{k\geq 0})((b_l)_{l\geq 0}) = (c_n)_{n\geq 0}$ où

$$c_n := \sum_{k+l=n} a_k b_l = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{l=0}^{n} a_{n-l} b_l \ .$$

Définition 1.4

La multiplication dans $A[X]$: $((a_k)_{k\geq 0})((b_l)_{l\geq 0}) = (c_n)_{n\geq 0}$ où

$$c_n := \sum_{k+l=n} a_k b_l = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{l=0}^{n} a_{n-l} b_l \; .$$

Cette lci est associative, admet un élément neutre, à savoir le polynôme constant $(1, 0, 0\dots)$, est commutative, et est distributive par rapport à l'addition. Il en résulte :

Définition 1.4

La multiplication dans $A[X]$: $((a_k)_{k\geq 0})((b_l)_{l\geq 0}) = (c_n)_{n\geq 0}$ où

$$c_n := \sum_{k+l=n} a_k b_l = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{l=0}^{n} a_{n-l} b_l \ .$$

Cette lci est associative, admet un élément neutre, à savoir le polynôme constant $(1, 0, 0 \ldots)$, est commutative, et est distributive par rapport à l'addition. Il en résulte :

Proposition 1.5

Les opérations $+, \cdot$ introduites ci-dessus munissent l'ensemble $A[X]$ d'une structure d'anneau commutatif.

8

On identifie $a \in A$ avec le polynôme constant $(a, 0, 0, \dots)$ qui lui correspond. En particulier on va utiliser la notation 1 pour l'élément unité $(1, 0, 0, \dots)$ de $A[X]$.

8

On identifie $a \in A$ avec le polynôme constant $(a, 0, 0, \dots)$ qui lui correspond. En particulier on va utiliser la notation 1 pour l'élément unité $(1, 0, 0, \dots)$ de $A[X]$.

Notation $X := (0, 1, 0, \dots) \in A[X]$. On obtient facilement

$$X^2 = (0, 0, 1, 0, \dots),\ X^3 = (0, 0, 0, 1, 0, \dots) \text{ et ainsi de suite.}$$

$$(a_k)_{k \geq 0} = \sum_{k \geq 0} a_k X^k \text{ (nombre fini de termes non-nuls)},\ X^0 := 1\,.$$

8

On identifie $a \in A$ avec le polynôme constant $(a, 0, 0, \dots)$ qui lui correspond. En particulier on va utiliser la notation 1 pour l'élément unité $(1, 0, 0, \dots)$ de $A[X]$.

Notation $X := (0, 1, 0, \dots) \in A[X]$. On obtient facilement

$$X^2 = (0, 0, 1, 0, \dots),\ X^3 = (0, 0, 0, 1, 0, \dots) \text{ et ainsi de suite.}$$

$$(a_k)_{k \geq 0} = \sum_{k \geq 0} a_k X^k \text{ (nombre fini de termes non-nuls)},\ X^0 := 1\,.$$

Cette égalité fait la liaison entre la définition moderne de la notion de polynôme et la définition élémentaire, comme expression algébrique de la forme $a_0 + a_1 X + \cdots + a_N X^N$.

8

On identifie $a \in A$ avec le polynôme constant $(a, 0, 0, \dots)$ qui lui correspond. En particulier on va utiliser la notation 1 pour l'élément unité $(1, 0, 0, \dots)$ de $A[X]$.

Notation $X := (0, 1, 0, \dots) \in A[X]$. On obtient facilement

$$X^2 = (0, 0, 1, 0, \dots),\ X^3 = (0, 0, 0, 1, 0, \dots) \text{ et ainsi de suite.}$$

$$(a_k)_{k \geq 0} = \sum_{k \geq 0} a_k X^k \text{ (nombre fini de termes non-nuls)},\ X^0 := 1\,.$$

Cette égalité fait la liaison entre la définition moderne de la notion de polynôme et la définition élémentaire, comme expression algébrique de la forme $a_0 + a_1 X + \dots + a_N X^N$.

En appliquant la construction $A \mapsto A[X]$: nouveaux anneaux commutatifs : $\mathbb{Z}[X]$, $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$, $\mathbb{Z}_n[X]$.

9

Soit $(A, +, \cdot)$ un anneau. Puisque $(A, +)$ est un groupe abélien, on va utiliser la notation nx $(\text{pour } n \in \mathbb{Z}, x \in A)$ introduite pour les groupes avec lci en notation additive.

9

Soit $(A, +, \cdot)$ un anneau. Puisque $(A, +)$ est un groupe abélien, on va utiliser la notation nx (pour $n \in \mathbb{Z}$, $x \in A$) introduite pour les groupes avec lci en notation additive.

En particulier l'élément symétrique par rapport à l'addition (l'opposé) d'un élément $x \in A$ sera noté $-x$.

9

Soit $(A, +, \cdot)$ un anneau. Puisque $(A, +)$ est un groupe abélien, on va utiliser la notation nx (pour $n \in \mathbb{Z}$, $x \in A$) introduite pour les groupes avec lci en notation additive.

En particulier l'élément symétrique par rapport à l'addition (l'opposé) d'un élément $x \in A$ sera noté $-x$.

On va aussi utiliser les règles de calcul connues dans un groupe en notation additive.

10

Proposition 1.6 (Règles de calcul dans un anneau)

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

1. Pour tout élément $x \in A$ on a $x \cdot 0 = 0 \cdot x = 0$.

10

Proposition 1.6 (Règles de calcul dans un anneau)

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

1. Pour tout élément $x \in A$ on a $x \cdot 0 = 0 \cdot x = 0$.
2. Pour tout $(x,y) \in A \times A$: $x(-y) = (-x)y = -(xy)$.

10

Proposition 1.6 (Règles de calcul dans un anneau)

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

1. Pour tout élément $x \in A$ on a $x \cdot 0 = 0 \cdot x = 0$.
2. Pour tout $(x,y) \in A \times A$: $x(-y) = (-x)y = -(xy)$.
3. Pour tout $(x,y) \in A \times A$: $(-x)(-y) = -((-x)y) = -(-(xy)) = xy$.

10

Proposition 1.6 (Règles de calcul dans un anneau)

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

1. Pour tout élément $x \in A$ on a $x \cdot 0 = 0 \cdot x = 0$.
2. Pour tout $(x,y) \in A \times A$: $x(-y) = (-x)y = -(xy)$.
3. Pour tout $(x,y) \in A \times A$: $(-x)(-y) = -((-x)y) = -(-(xy)) = xy$.
4. Pour $x \in A$ et $n \in \mathbb{N}$ on définit l'élément $x^n \in A$ par :

$$x^n := \begin{cases} \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ fois}} & \text{si} \quad n > 0, \\ 1 & \text{si} \quad n = 0. \end{cases}$$

Alors on a l'identité $x^m \cdot x^n = x^{m+n}$.

10

Proposition 1.6 (Règles de calcul dans un anneau)

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

1. Pour tout élément $x \in A$ on a $x \cdot 0 = 0 \cdot x = 0$.
2. Pour tout $(x,y) \in A \times A$: $x(-y) = (-x)y = -(xy)$.
3. Pour tout $(x,y) \in A \times A$: $(-x)(-y) = -((-x)y) = -(-(xy)) = xy$.
4. Pour $x \in A$ et $n \in \mathbb{N}$ on définit l'élément $x^n \in A$ par :

$$x^n := \begin{cases} \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ fois}} & \text{si} \quad n > 0, \\ 1 & \text{si} \quad n = 0. \end{cases}$$

   Alors on a l'identité $x^m \cdot x^n = x^{m+n}$.
5. Pour $x \in A$ et $n \in \mathbb{Z}$ on a $nx = (n\, 1_A) \cdot x = x \cdot (n\, 1_A)$.

10

Proposition 1.6 (Règles de calcul dans un anneau)

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

1. Pour tout élément $x \in A$ on a $x\cdot 0 = 0\cdot x = 0$.
2. Pour tout $(x,y) \in A\times A$: $x(-y) = (-x)y = -(xy)$.
3. Pour tout $(x,y) \in A\times A$: $(-x)(-y) = -((-x)y) = -(-(xy)) = xy$.
4. Pour $x \in A$ et $n \in \mathbb{N}$ on définit l'élément $x^n \in A$ par :

$$x^n := \begin{cases} \underbrace{x\cdot x\cdot \ldots \cdot x}_{n \text{ fois}} & \text{si} \quad n > 0, \\ 1 & \text{si} \quad n = 0. \end{cases}$$

   Alors on a l'identité $x^m \cdot x^n = x^{m+n}$.

5. Pour $x \in A$ et $n \in \mathbb{Z}$ on a $nx = (n\,1_A)\cdot x = x\cdot(n\,1_A)$.

Dém: Exercice.

11

Lemme 1.7

Soient $(A,+,\cdot)$ un anneau, $x, y \in A$ deux éléments commutables. Pour tous $k, l \in \mathbb{N}$ les éléments x^k, y^l sont aussi commutables.

11

Lemme 1.7

Soient $(A, +, \cdot)$ un anneau, $x, y \in A$ deux éléments commutables. Pour tous $k, l \in \mathbb{N}$ les éléments x^k, y^l sont aussi commutables.

Dém: Démonstration en deux étapes :

1. En utilisant récurrence par rapport à k on démontre que x^k et y sont commutables pour tout $k \in \mathbb{N}$.

11

Lemme 1.7

Soient $(A,+,\cdot)$ un anneau, $x, y \in A$ deux éléments commutables. Pour tous $k, l \in \mathbb{N}$ les éléments x^k, y^l sont aussi commutables.

Dém: Démonstration en deux étapes :

1. En utilisant récurrence par rapport à k on démontre que x^k et y sont commutables pour tout $k \in \mathbb{N}$.
2. Fixons $k \in \mathbb{N}$. En utilisant la récurrence par rapport à l on démontre que x^k et y^l sont commutables.

∎

11

Lemme 1.7

Soient $(A,+,\cdot)$ un anneau, $x, y \in A$ deux éléments commutables. Pour tous $k, l \in \mathbb{N}$ les éléments x^k, y^l sont aussi commutables.

Dém: Démonstration en deux étapes :

1. En utilisant récurrence par rapport à k on démontre que x^k et y sont commutables pour tout $k \in \mathbb{N}$.
2. Fixons $k \in \mathbb{N}$. En utilisant la récurrence par rapport à l on démontre que x^k et y^l sont commutables.

■

Proposition 1.8 (la formule du binôme dans un anneau)

Soient $(A,+,\cdot)$ un anneau, $x, y \in A$ deux éléments commutables et $n \in \mathbb{N}$. Alors $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.

12

Dém: Exercice. Utiliser le lemme 1.7, la récurrence par rapport à n et les identités :

$$(x+y)^{n+1} = (x+y)^n(x+y),$$

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}.$$

∎

13

Définition 1.9

Soit $(A,+,\cdot)$ un anneau commutatif non-nul. On dit qu'un élément $a \in A \setminus \{0\}$ est un diviseur de zéro si s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$.

13

Définition 1.9

Soit $(A,+,\cdot)$ un anneau commutatif non-nul. On dit qu'un élément $a \in A \setminus \{0\}$ est un diviseur de zéro si s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$.
Un anneau commutatif est dit intègre, ou anneau d'intégrité, s'il est non-nul et ne possède aucun diviseur de zéro.

13

Définition 1.9

Soit $(A,+,\cdot)$ un anneau commutatif non-nul. On dit qu'un élément $a\in A\setminus\{0\}$ est un diviseur de zéro si s'il existe $b\in A\setminus\{0\}$ tel que $ab=0$.
Un anneau commutatif est dit intègre, ou anneau d'intégrité, s'il est non-nul et ne possède aucun diviseur de zéro.

Remarque 1.10

Un anneau commutatif non-nul $(A,+,\cdot)$ est intègre si et seulement si

$$\forall (x,y)\in A\times A\ \big(xy=0\Rightarrow (x=0)\vee(y=0)\big).$$

13

Définition 1.9

Soit $(A,+,\cdot)$ un anneau commutatif non-nul. On dit qu'un élément $a \in A \setminus \{0\}$ est un diviseur de zéro si s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$.
Un anneau commutatif est dit intègre, ou anneau d'intégrité, s'il est non-nul et ne possède aucun diviseur de zéro.

Remarque 1.10

Un anneau commutatif non-nul $(A,+,\cdot)$ est intègre si et seulement si

$$\forall (x,y) \in A \times A \ \Big(xy = 0 \Rightarrow (x = 0) \vee (y = 0)\Big).$$

Exercice 1.1

Préciser les diviseurs de 0 de $(\mathbb{Z}_{12},+,\cdot)$.

14

Exemples 1.2

1. Les anneaux $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont intègres.

Exemples 1.2

1. Les anneaux $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont intègres.
2. Soit $n \in \mathbb{N}^*$. L'anneau $(\mathbb{Z}_n,+,\cdot)$ est intègre si et seulement si n est un nombre premier.

Exemples 1.2

1. Les anneaux $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont intègres.
2. Soit $n \in \mathbb{N}^*$. L'anneau $(\mathbb{Z}_n,+,\cdot)$ est intègre si et seulement si n est un nombre premier.
3. Soient $(A,+,\cdot)$, $(B,+,\cdot)$ deux anneaux commutatifs non-nuls. Alors $A\times B$ (muni de sa structure d'anneau produit) n'est pas intègre.

14

Exemples 1.2

1. Les anneaux $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont intègres.
2. Soit $n \in \mathbb{N}^*$. L'anneau $(\mathbb{Z}_n,+,\cdot)$ est intègre si et seulement si n est un nombre premier.
3. Soient $(A,+,\cdot)$, $(B,+,\cdot)$ deux anneaux commutatifs non-nuls. Alors $A\times B$ (muni de sa structure d'anneau produit) n'est pas intègre.
4. Soient $(A,+,\cdot)$ un anneau commutatif non-nul et X un ensemble. Si $\mathrm{card}(X)\geq 2$ alors $\mathcal{F}(X,A)$ (muni de sa structure naturelle d'anneau) n'est pas intègre. Pourquoi ?

Exemples 1.2

1. Les anneaux $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont intègres.
2. Soit $n\in\mathbb{N}^*$. L'anneau $(\mathbb{Z}_n,+,\cdot)$ est intègre si et seulement si n est un nombre premier.
3. Soient $(A,+,\cdot)$, $(B,+,\cdot)$ deux anneaux commutatifs non-nuls. Alors $A\times B$ (muni de sa structure d'anneau produit) n'est pas intègre.
4. Soient $(A,+,\cdot)$ un anneau commutatif non-nul et X un ensemble. Si $\mathrm{card}(X)\geq 2$ alors $\mathcal{F}(X,A)$ (muni de sa structure naturelle d'anneau) n'est pas intègre. Pourquoi ?

On va montrer que, si A un anneau commutatif intègre, alors $A[X]$ est intègre.

15

Proposition 1.11

Soit A un anneau commutatif intègre. Alors $A[X]$ est intègre.

15

Proposition 1.11

Soit A un anneau commutatif intègre. Alors $A[X]$ est intègre.

Dém: La démonstration utilise la notion de degré d'un polynôme :

Définition 1.12

Soit $P(X) = \sum_{k\geq 0} a_k X^k \in A[X]$.

$$\deg(P(X)) := \begin{cases} \max\{k \in \mathbb{N} |\, a_k \neq 0\} & \text{si} \quad P(X) \neq 0 \\ -\infty & \text{si} \quad P(X) = 0 \end{cases} .$$

Proposition 1.11

Soit A un anneau commutatif intègre. Alors $A[X]$ est intègre.

Dém: La démonstration utilise la notion de degré d'un polynôme :

Définition 1.12

Soit $P(X)=\sum_{k\geq 0} a_k X^k \in A[X]$.

$$\deg(P(X)) := \begin{cases} \max\{k\in\mathbb{N} \mid a_k\neq 0\} & \text{si} \quad P(X)\neq 0 \\ -\infty & \text{si} \quad P(X)=0 \end{cases} .$$

La formule connue $\deg(P(X)Q(X))=\deg(P(X))+\deg(Q(X))$ reste vraie pour les polynômes à coefficients dans un anneau intègre (Exercice).

Cette formule montre : $P(X)Q(X) = 0 \Rightarrow (P(X) = 0) \vee (Q(X) = 0)$.

∎

16

Cette formule montre : $P(X)Q(X) = 0 \Rightarrow (P(X) = 0) \vee (Q(X) = 0)$.

■

Exemple 1.1

Calculer $(\hat{2}X + \hat{4})(\hat{3}X + \hat{3}) \in \mathbb{Z}_6[X]$.

17

Définition 1.13

Soit $(A,+,\cdot)$ un anneau commutatif. Un élément $x \in A$ est dit inversible, s'il est inversible par rapport à la multiplication, i.e. s'il existe $y \in A$ tel que $xy = 1$.

Définition 1.13

Soit $(A,+,\cdot)$ un anneau commutatif. Un élément $x \in A$ est dit inversible, s'il est inversible par rapport à la multiplication, i.e. s'il existe $y \in A$ tel que $xy = 1$.
On va désigner par $A^\times \subset A$ le sous-ensemble des éléments inversibles.

Définition 1.13

Soit $(A, +, \cdot)$ un anneau commutatif. Un élément $x \in A$ est dit inversible, s'il est inversible par rapport à la multiplication, i.e. s'il existe $y \in A$ tel que $xy = 1$.
On va désigner par $A^\times \subset A$ le sous-ensemble des éléments inversibles.

Remarque 1.14

Soit $(A, +, \cdot)$ un anneau commutatif. Alors $A^\times$ est stable par rapport à la multiplication et $(A^\times, \cdot)$ est un groupe commutatif.

17

Définition 1.13

Soit $(A,+,\cdot)$ un anneau commutatif. Un élément $x \in A$ est dit inversible, s'il est inversible par rapport à la multiplication, i.e. s'il existe $y \in A$ tel que $xy = 1$.
On va désigner par $A^\times \subset A$ le sous-ensemble des éléments inversibles.

Remarque 1.14

Soit $(A,+,\cdot)$ un anneau commutatif. Alors $A^\times$ est stable par rapport à la multiplication et $(A^\times,\cdot)$ est un groupe commutatif.

Exercice 1.2

Préciser les groupe des éléments inversibles dans les anneaux commutatifs suivants (munis de leurs opérations usuelles) : $\mathbb{Z}$, $\mathbb{Z}_{12}$, $\mathbb{Z}[X]$, $\mathbb{R}[X]$.

18

Définition 1.15

Un anneau commutatif non-nul $(A, +, \cdot)$ s'appelle corps, si tout élément $x \in A \setminus \{0\}$ est inversible.

18

Définition 1.15

Un anneau commutatif non-nul $(A,+,\cdot)$ s'appelle corps, si tout élément $x \in A \setminus \{0\}$ est inversible.

Donc, un anneau commutatif non-nul $(A,+,\cdot)$ est un corps si et seulement si $A^\times = A \setminus \{0\}$.

Exemples 1.3

$(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont des corps.

18

Définition 1.15

Un anneau commutatif non-nul $(A,+,\cdot)$ s'appelle corps, si tout élément $x \in A \setminus \{0\}$ est inversible.

Donc, un anneau commutatif non-nul $(A,+,\cdot)$ est un corps si et seulement si $A^{\times} = A \setminus \{0\}$.

Exemples 1.3

$(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ sont des corps.

Dans un anneau commutatif non-nul un élément inversible n'est jamais diviseur de 0. Pourquoi ? Il en résulte

Remarque 1.16

Tout corps $(K,+,\cdot)$ est un anneau intègre.

Proposition 1.17

Soit $n \in \mathbb{N}^*$. Sont équivalentes

1. $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.
2. $\mathbb{Z}/n\mathbb{Z}$ est un corps.
3. n est un nombre premier.

Proposition 1.17

Soit $n \in \mathbb{N}^*$. Sont équivalentes

1. $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.
2. $\mathbb{Z}/n\mathbb{Z}$ est un corps.
3. n est un nombre premier.

Dém: Exercice. ∎

19

Proposition 1.17

Soit $n \in \mathbb{N}^*$. Sont équivalentes

1. $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.
2. $\mathbb{Z}/n\mathbb{Z}$ est un corps.
3. n est un nombre premier.

Dém: Exercice. ∎

Exercice 1.3

Soit $(A, +, \cdot)$ un anneau commutatif intègre. Identifions A avec le sous ensemble de $A[X]$ formé des polynômes constants.

Proposition 1.17

Soit $n \in \mathbb{N}^*$. Sont équivalentes

1. $\mathbb{Z}/n\mathbb{Z}$ est un anneau intègre.
2. $\mathbb{Z}/n\mathbb{Z}$ est un corps.
3. n est un nombre premier.

Dém: Exercice. ∎

Exercice 1.3

Soit $(A, +, \cdot)$ un anneau commutatif intègre. Identifions A avec le sous ensemble de $A[X]$ formé des polynômes constants. Montrer qu'un polynôme $P(X) \in A[X]$ est inversible si et seulement si $P(X) \in A^\times$. En déduire que $A[X]$ n'est pas un corps.

20

Exemple 1.2

Le sous-ensemble

$$\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \mid a,\, b \in \mathbb{Q}\} \subset \mathbb{R}$$

muni de l'addition et de la multiplication ordinaires est un corps commutatif.

Table of Contents

1 Introduction
- Définition. Exemples. Règles de calcul dans un anneau
  - L'anneau des polynômes à coefficients dans un anneau commutatif
  - Règles de calcul dans un anneau
- Diviseurs de zéro dans un anneau commutatifs. Anneaux commutatifs intègres

2 Sous-anneaux et idéaux. Anneaux quotients. Morphismes
- Sous-anneaux et idéaux dans un anneau commutatif. Anneaux quotients
- Morphismes d'anneaux. Le premier théorème d'isomorphisme
- La caractéristique d'un anneau

21

Dans ce chapitre $(A,+,\cdot)$ désigne un anneau commutatif.

Définition 2.1

Un sous-ensemble $B \subset A$ est dit sous-anneau de $(A,+,\cdot)$ si les conditions suivantes sont vérifiées :

- (i) B est un sous-groupe du groupe abélien $(A,+)$.
- (ii) $\forall (x,y) \in B \times B,\ x \cdot y \in B$.
- (iii) $1_A \in B$.

Dans ce chapitre $(A,+,\cdot)$ désigne un anneau commutatif.

Définition 2.1

Un sous-ensemble $B\subset A$ est dit sous-anneau de $(A,+,\cdot)$ si les conditions suivantes sont vérifiées :

(i) B est un sous-groupe du groupe abélien $(A,+)$.

(ii) $\forall (x,y)\in B\times B,\ x\cdot y\in B$.

(iii) $1_A\in B$.

Remarque 2.2

Si B est un sous-anneau de $(A,+,\cdot)$, alors B est stable par rapport aux lci $+,\cdot$ et les opérations induites sur B définissent une structure d'anneau sur B.

Remarque 2.3

Soit $B \subset A$. Sont équivalentes

(i) B est un sous-anneau de $(A,+,\cdot)$.

(ii) $1_A \in B$ et $\forall (x,y) \in B \times B$, $\Big((x-y \in B) \wedge (x \cdot y \in B)\Big)$.

Dém: Exercice. Utiliser la définition d'un sous-groupe. ■

Remarque 2.3

Soit $B \subset A$. Sont équivalentes

(i) B est un sous-anneau de $(A,+,\cdot)$.

(ii) $1_A \in B$ et $\forall (x,y) \in B \times B$, $\big((x-y \in B) \wedge (x \cdot y \in B)\big)$.

Dém: Exercice. Utiliser la définition d'un sous-groupe. ∎

Remarque 2.4

Tout sous-anneau d'un anneau intègre est un anneau intègre.

Remarque 2.3

Soit $B \subset A$. Sont équivalentes

- (i) B est un sous-anneau de $(A,+,\cdot)$.
- (ii) $1_A \in B$ et $\forall (x,y) \in B \times B$, $\big((x-y \in B) \wedge (x \cdot y \in B)\big)$.

Dém: Exercice. Utiliser la définition d'un sous-groupe. ∎

Remarque 2.4

Tout sous-anneau d'un anneau intègre est un anneau intègre.

Exemples 2.1

1. A est toujours un sous-anneau de $(A,+,\cdot)$ mais, si A est non-nul, $\{0_A\}$ ne sera pas un sous-anneau de $(A,+,\cdot)$.

Remarque 2.3

Soit $B \subset A$. Sont équivalentes

(i) B est un sous-anneau de $(A,+,\cdot)$.

(ii) $1_A \in B$ et $\forall (x,y) \in B \times B$, $\big((x-y \in B) \wedge (x \cdot y \in B)\big)$.

Dém: Exercice. Utiliser la définition d'un sous-groupe. ∎

Remarque 2.4

Tout sous-anneau d'un anneau intègre est un anneau intègre.

Exemples 2.1

1. A est toujours un sous-anneau de $(A,+,\cdot)$ mais, si A est non-nul, $\{0_A\}$ ne sera pas un sous-anneau de $(A,+,\cdot)$.
2. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ sont des inclusions de sous-anneau.

Exemple 2.1

Identifions A avec le sous ensemble de $A[X]$ formé par les polynômes constants. Alors A devient un sous-anneau de $(A[X], +, \cdot)$.

23

Exemple 2.1

Identifions A avec le sous ensemble de $A[X]$ formé par les polynômes constants. Alors A devient un sous-anneau de $(A[X],+,\cdot)$.

Définition 2.5

Soit $I \subset A$. On dit que I est un idéal de A si

- (i) I est un sous-groupe du groupe abélien $(A,+)$.
- (ii) $\forall (a,x) \in A \times I,\ a \cdot x \in I$.

Question : est-ce qu'un idéal $I \subset A$ peut être un sous-anneau ?

Exemple 2.1

Identifions A avec le sous ensemble de $A[X]$ formé par les polynômes constants. Alors A devient un sous-anneau de $(A[X], +, \cdot)$.

Définition 2.5

Soit $I \subset A$. On dit que I est un idéal de A si

(i) I est un sous-groupe du groupe abélien $(A, +)$.

(ii) $\forall (a, x) \in A \times I,\ a \cdot x \in I$.

Question : est-ce qu'un idéal $I \subset A$ peut être un sous-anneau ? La remarque suivante montre que le seul idéal de A qui est un sous-anneau est A lui même.

24

Remarque 2.6

Soit $I \subset A$ un idéal de $(A, +, \cdot)$. Sont équivalentes :

(i) $I = A$.

(ii) I est un sous-anneau.

(iii) $1_A \in I$.

(iv) I contient un élément inversible.

24

Remarque 2.6

Soit $I \subset A$ un idéal de $(A, +, \cdot)$. Sont équivalentes :

(i) $I = A$.
(ii) I est un sous-anneau.
(iii) $1_A \in I$.
(iv) I contient un élément inversible.

Exemple 2.2

Soit $a \in A$. Le sous-ensemble

$$aA := \{a \cdot x | \, x \in A\} \subset A$$

est un idéal de $(A, +, \cdot)$. Cet idéal s'appelle l'idéal principal engendré par a et sera aussi noté (a).

Définition 2.7

Un anneau commutatif $(A,+,\cdot)$ est dit anneau principal s'il est intègre et tout idéal de A est principal.

Définition 2.7

Un anneau commutatif $(A, +, \cdot)$ est dit anneau principal s'il est intègre et tout idéal de A est principal.

Remarque 2.8

L'ensemble des idéaux de $(\mathbb{Z}, +, \cdot)$ est $\{n\mathbb{Z} | \ n \in \mathbb{N}\}$. En particulier $(\mathbb{Z}, +, \cdot)$ est un anneau principal.

Définition 2.7

Un anneau commutatif $(A, +, \cdot)$ est dit anneau principal s'il est intègre et tout idéal de A est principal.

Remarque 2.8

L'ensemble des idéaux de $(\mathbb{Z}, +, \cdot)$ est $\{n\mathbb{Z} \mid n \in \mathbb{N}\}$. En particulier $(\mathbb{Z}, +, \cdot)$ est un anneau principal.

Dém: Soit $I \subset \mathbb{Z}$ un idéal de $(\mathbb{Z}, +, \cdot)$. Puisque I est un idéal, il est un sous-groupe du groupe abélien $(\mathbb{Z}, +)$.

25

Définition 2.7

Un anneau commutatif $(A, +, \cdot)$ est dit anneau principal s'il est intègre et tout idéal de A est principal.

Remarque 2.8

L'ensemble des idéaux de $(\mathbb{Z}, +, \cdot)$ est $\{n\mathbb{Z} | \ n \in \mathbb{N}\}$. En particulier $(\mathbb{Z}, +, \cdot)$ est un anneau principal.

Dém: Soit $I \subset \mathbb{Z}$ un idéal de $(\mathbb{Z}, +, \cdot)$. Puisque I est un idéal, il est un sous-groupe du groupe abélien $(\mathbb{Z}, +)$. Mais tout sous-groupe de $(\mathbb{Z}, +)$ s'écrit sous la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$ (exercice).

Définition 2.7

Un anneau commutatif $(A, +, \cdot)$ est dit anneau principal s'il est intègre et tout idéal de A est principal.

Remarque 2.8

L'ensemble des idéaux de $(\mathbb{Z}, +, \cdot)$ est $\{n\mathbb{Z} | \ n \in \mathbb{N}\}$. En particulier $(\mathbb{Z}, +, \cdot)$ est un anneau principal.

Dém: Soit $I \subset \mathbb{Z}$ un idéal de $(\mathbb{Z}, +, \cdot)$. Puisque I est un idéal, il est un sous-groupe du groupe abélien $(\mathbb{Z}, +)$. Mais tout sous-groupe de $(\mathbb{Z}, +)$ s'écrit sous la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$ (exercice). Réciproquement, tout sous-ensemble de la forme $n\mathbb{Z}$ est un idéal de $(\mathbb{Z}, +, \cdot)$. Pourquoi ? ■

26

Définition 2.9

Un idéal I de $(A,+,\cdot)$ est dit maximal si $I \neq A$ et pour tout idéal J diffèrent de I qui contient I on a $J = A$.

26

Définition 2.9

Un idéal I de $(A,+,\cdot)$ est dit maximal si $I \neq A$ et pour tout idéal J diffèrent de I qui contient I on a $J = A$.

Exemple 2.3

L'idéal $n\mathbb{Z}$ de $(\mathbb{Z},+,\cdot)$ est maximal si et seulement si n est un nombre premier.

26

Définition 2.9

Un idéal I de $(A, +, \cdot)$ est dit maximal si $I \neq A$ et pour tout idéal J diffèrent de I qui contient I on a $J = A$.

Exemple 2.3

L'idéal $n\mathbb{Z}$ de $(\mathbb{Z}, +, \cdot)$ est maximal si et seulement si n est un nombre premier.

En effet, on peut supposer $n \geq 2$. Tout idéal de $\mathbb{Z}$ s'écrit sous la form $m\mathbb{Z}$ avec $m \in \mathbb{N}$. Nous avons les équivalences

$$n\mathbb{Z} \subset m\mathbb{Z} \Leftrightarrow m|n,\ n\mathbb{Z} = m\mathbb{Z} \Leftrightarrow m = n,\ m\mathbb{Z} = \mathbb{Z} \Leftrightarrow m = 1.$$

Définition 2.9

Un idéal I de $(A,+,\cdot)$ est dit maximal si $I \neq A$ et pour tout idéal J diffèrent de I qui contient I on a $J = A$.

Exemple 2.3

L'idéal $n\mathbb{Z}$ de $(\mathbb{Z},+,\cdot)$ est maximal si et seulement si n est un nombre premier.

En effet, on peut supposer $n \geq 2$. Tout idéal de $\mathbb{Z}$ s'écrit sous la form $m\mathbb{Z}$ avec $m \in \mathbb{N}$. Nous avons les équivalences

$$n\mathbb{Z} \subset m\mathbb{Z} \Leftrightarrow m|n,\ n\mathbb{Z} = m\mathbb{Z} \Leftrightarrow m = n,\ m\mathbb{Z} = \mathbb{Z} \Leftrightarrow m = 1.$$

Conclusion : $n\mathbb{Z}$ n'est pas maximal si et seulement s'il existe un diviseur $m \in \mathbb{N}^*$ de n tel que $m \neq 1$ et $m \neq n$, donc si et seulement si n n'est pas un nombre premier.

27

Proposition 2.10

Soit $(I_s)_{s\in S}$ une famille d'idéaux de A. Alors l'intersection $\bigcap_{s\in S} I_s$ est un idéal de A.

Dém: Exercice. ■

Proposition 2.10

Soit $(I_s)_{s\in S}$ une famille d'idéaux de A. Alors l'intersection $\bigcap_{s\in S} I_s$ est un idéal de A.

Dém: Exercice. ■

Définition 2.11

Soit $S \subset A$ un sous-ensemble. L'idéal engendré par S est l'intersection de tous les idéaux de $(A,+,\cdot)$ qui contiennent S :

$$(S) := \bigcap_{\substack{I \text{ idéal de } A \\ S\subset I}} I$$

27

Proposition 2.10

Soit $(I_s)_{s\in S}$ une famille d'idéaux de A. Alors l'intersection $\bigcap_{s\in S} I_s$ est un idéal de A.

Dém: Exercice. ∎

Définition 2.11

Soit $S\subset A$ un sous-ensemble. L'idéal engendré par S est l'intersection de tous les idéaux de $(A,+,\cdot)$ qui contiennent S :

$$(S):=\bigcap_{\substack{I \text{ idéal de } A\\ S\subset I}} I$$

Donc l'idéal engendré par S est le plus petit idéal (au sens de l'inclusion) de A qui contient S.

Remarque 2.12

Soit $S \subset A$ un sous-ensemble. Alors

$$(S) = \left\{ \sum_{i=1}^{k} s_i \cdot x_i \,\middle|\, k \in \mathbb{N},\ (s_1, \dots, s_k) \in S^k,\ (x_1, \dots, x_k) \in A^k \right\}.$$

Remarque 2.12

Soit $S \subset A$ un sous-ensemble. Alors

$$(S) = \left\{ \sum_{i=1}^{k} s_i \cdot x_i \,\middle|\, k \in \mathbb{N},\ (s_1, \dots, s_k) \in S^k,\ (x_1, \dots, x_k) \in A^k \right\}.$$

Dém: Démonstration en deux étapes :

1. Le sous-ensemble

$$I := \left\{ \sum_{i=1}^{k} s_i \cdot x_i \,\middle|\, k \in \mathbb{N},\ (s_1, \dots, s_k) \in S^k,\ (x_1, \dots, x_k) \in A^k \right\}$$

   est un idéal de $(A, +, \cdot)$ qui contient S. Ceci implique l'inclusion $(S) \subset I$.

28

Remarque 2.12

Soit $S \subset A$ un sous-ensemble. Alors

$$(S) = \left\{ \sum_{i=1}^{k} s_i \cdot x_i \,\middle|\, k \in \mathbb{N},\ (s_1, \ldots, s_k) \in S^k,\ (x_1, \ldots, x_k) \in A^k \right\}.$$

Dém: Démonstration en deux étapes :

1. Le sous-ensemble

$$I := \left\{ \sum_{i=1}^{k} s_i \cdot x_i \,\middle|\, k \in \mathbb{N},\ (s_1, \ldots, s_k) \in S^k,\ (x_1, \ldots, x_k) \in A^k \right\}$$

est un idéal de $(A, +, \cdot)$ qui contient S. Ceci implique l'inclusion $(S) \subset I$.

2. Tout idéal de $(A, +, \cdot)$ qui contient S doit contenir I. Ceci implique $I \subset (S)$.

29

Définition 2.13

Un idéal I de A est dit idéal de type fini s'il est engendré par un ensemble fini, donc s'il existe $k \in \mathbb{N}$ et $s_1, \ldots, s_k \in A$ tels que

$$I = \left\{ \sum_{i=1}^{k} s_i \cdot x_i \,\middle|\, (x_1, \ldots, x_k) \in A^k \right\}.$$

Définition 2.13

Un idéal I de A est dit idéal de type fini s'il est engendré par un ensemble fini, donc s'il existe $k \in \mathbb{N}$ et $s_1, \ldots, s_k \in A$ tels que

$$I = \left\{ \sum_{i=1}^{k} s_i \cdot x_i \,\middle|\, (x_1, \ldots, x_k) \in A^k \right\}.$$

Soient I, J deux idéaux de A. La somme $I + J$ est l'idéal :

$$I + J := (I \cup J) = \{x + y \,|\, x \in I,\ y \in J\}.$$

Définition 2.13

Un idéal I de A est dit idéal de type fini s'il est engendré par un ensemble fini, donc s'il existe $k\in\mathbb{N}$ et $s_1,\dots,s_k\in A$ tels que

$$I=\Big\{\sum_{i=1}^k s_i\cdot x_i \,\big|\, (x_1,\dots,x_k)\in A^k\Big\}.$$

Soient I, J deux idéaux de A. La somme $I+J$ est l'idéal :

$$I+J:=(I\cup J)=\{x+y \,|\, x\in I,\ y\in J\}.$$

Pour une famille finie $(I_i)_{1\leq i\leq k}$ d'idéaux de A on pose

$$I_1+\ldots+I_k:=(I_1\cup\ldots\cup I_k)=\Big\{\sum_{i=1}^k x_i \,\big|\, x_i\in I_i \text{ pour } 1\leq i\leq k\Big\}.$$

Exercice 2.1

Un idéal $I \subset A$ est maximal si et seulement si $I \neq A$ et pour tout $a \in A \setminus I$ on a $aA + I = A$.

30

Exercice 2.1

Un idéal $I \subset A$ est maximal si et seulement si $I \neq A$ et pour tout $a \in A \setminus I$ on a $aA + I = A$.

Définition 2.14

Un idéal I de A est dit premier si $I \neq A$ et l'implication suivante est vraie : $(a \cdot b \in I) \Rightarrow (a \in I) \vee (b \in I)$.

Exercice 2.1

Un idéal $I \subset A$ est maximal si et seulement si $I \neq A$ et pour tout $a \in A \setminus I$ on a $aA + I = A$.

Définition 2.14

Un idéal I de A est dit premier si $I \neq A$ et l'implication suivante est vraie : $(a \cdot b \in I) \Rightarrow (a \in I) \vee (b \in I)$.

Proposition 2.15

1. L'idéal nul $\{0\}$ est premier si et seulement si A est intègre.
2. Tout idéal maximal $I \subset A$ de A est un idéal premier.

Exercice 2.1

Un idéal $I \subset A$ est maximal si et seulement si $I \neq A$ et pour tout $a \in A \setminus I$ on a $aA + I = A$.

Définition 2.14

Un idéal I de A est dit premier si $I \neq A$ et l'implication suivante est vraie : $(a \cdot b \in I) \Rightarrow (a \in I) \vee (b \in I)$.

Proposition 2.15

1. L'idéal nul $\{0\}$ est premier si et seulement si A est intègre.
2. Tout idéal maximal $I \subset A$ de A est un idéal premier.

Dém: 1. Evident.

Exercice 2.1

Un idéal $I \subset A$ est maximal si et seulement si $I \neq A$ et pour tout $a \in A \setminus I$ on a $aA + I = A$.

Définition 2.14

Un idéal I de A est dit premier si $I \neq A$ et l'implication suivante est vraie : $(a \cdot b \in I) \Rightarrow (a \in I) \vee (b \in I)$.

Proposition 2.15

1. L'idéal nul $\{0\}$ est premier si et seulement si A est intègre.
2. Tout idéal maximal $I \subset A$ de A est un idéal premier.

Dém: 1. Evident. 2. Soient I maximal et $a, b \in A$ tels que $ab \in I$. Si $a \notin I$, alors $aA + I = A$, donc $\exists x \in A$ $\exists z \in I$ tels que $ax + z = 1$.

30

Exercice 2.1

Un idéal $I \subset A$ est maximal si et seulement si $I \neq A$ et pour tout $a \in A \setminus I$ on a $aA + I = A$.

Définition 2.14

Un idéal I de A est dit premier si $I \neq A$ et l'implication suivante est vraie : $(a \cdot b \in I) \Rightarrow (a \in I) \vee (b \in I)$.

Proposition 2.15

1. L'idéal nul $\{0\}$ est premier si et seulement si A est intègre.
2. Tout idéal maximal $I \subset A$ de A est un idéal premier.

Dém: 1. Evident. 2. Soient I maximal et $a, b \in A$ tels que $ab \in I$. Si $a \notin I$, alors $aA + I = A$, donc $\exists x \in A$ $\exists z \in I$ tels que $ax + z = 1$. On a donc $b = abx + bz \in I$ (parce que $ab \in I$ et $z \in I$). ∎

Exemple 2.4

L'idéal principal $X\mathbb{Z}[X]$ engendré par le polynôme X dans l'anneau $\mathbb{Z}[X]$ (muni des opérations usuelles) est premier, mais n'est pas maximal.

Exemple 2.4

L'idéal principal $X\mathbb{Z}[X]$ engendré par le polynôme X dans l'anneau $\mathbb{Z}[X]$ (muni des opérations usuelles) est premier, mais n'est pas maximal.

$X\mathbb{Z}[X]$ est premier : $P(X) = \sum_k a_k X^k \in X\mathbb{Z}[X]$ si et seulement si $a_0 = 0$. Il en résulte facilement :

$$P(X)Q(X) \in X\mathbb{Z}[X] \Rightarrow (P(X) \in X\mathbb{Z}[X]) \vee (Q(X) \in X\mathbb{Z}[X]))$$

Exemple 2.4

L'idéal principal $X\mathbb{Z}[X]$ engendré par le polynôme X dans l'anneau $\mathbb{Z}[X]$ (muni des opérations usuelles) est premier, mais n'est pas maximal.

$X\mathbb{Z}[X]$ est premier : $P(X)=\sum_k a_k X^k \in X\mathbb{Z}[X]$ si et seulement si $a_0=0$. Il en résulte facilement :

$$P(X)Q(X)\in X\mathbb{Z}[X] \Rightarrow (P(X)\in X\mathbb{Z}[X]) \vee (Q(X)\in X\mathbb{Z}[X]))$$

$X\mathbb{Z}[X]$ n'est pas maximal : $X\mathbb{Z}[X]$ est contenu dans l'idéal $2\mathbb{Z}[X]+X\mathbb{Z}[X]$ et les deux inclusions

$$X\mathbb{Z}[X]\subset 2\mathbb{Z}[X]+X\mathbb{Z}[X],\ 2\mathbb{Z}[X]+X\mathbb{Z}[X]\subset \mathbb{Z}[X]$$

sont strictes. Pourquoi ?

Remarque 2.16

Soient $I \subset A$ un idéal de A et $(A/I, +)$ le groupe quotient du groupe abélien $(A, +)$ par le sous-groupe I. La formule

$$([x]_I, [y]_I) \mapsto [x \cdot y]_I$$

définit une lci sur A/I (notée par le même symbole $\cdot$) et $(A/I, +, \cdot)$ est un anneau commutatif dont l'élément unité est la classe $[1]_I$.

Dém: Exercice.

Remarque 2.16

Soient $I \subset A$ un idéal de A et $(A/I, +)$ le groupe quotient du groupe abélien $(A, +)$ par le sous-groupe I. La formule

$$([x]_I, [y]_I) \mapsto [x \cdot y]_I$$

définit une lci sur A/I (notée par le même symbole $\cdot$) et $(A/I, +, \cdot)$ est un anneau commutatif dont l'élément unité est la classe $[1]_I$.

Dém: Exercice.

Définition 2.17 (Anneau quotient)

L'anneau $(A/I, +, \cdot)$ défini dans la remarque 2.16 s'appelle l'anneau quotient de $(A, +, \cdot)$ par l'idéal I.

Exemple 2.5

L'anneau quotient de $(\mathbb{Z},+,\cdot)$ par l'idéal $n\mathbb{Z}$ est précisément l'anneau $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ des entiers modulo n.

Proposition 2.18

Soient $(A,+,\cdot)$ un anneau commutatif et $I\subset A$ un idéal. Alors

1. I est un idéal maximal si et seulement si A/I est un corps.
2. I est un idéal premier si et seulement si A/I est intègre.

Dém: Exercice. ■

Définition 2.19

Soient A et B deux anneaux. Une application $f : A \to B$ est dite morphisme d'anneaux si :

(i) $f(1_A) = 1_B$.

(ii) $\forall (x, y) \in A \times A,\ f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$.

34

Définition 2.19

Soient A et B deux anneaux. Une application $f : A \to B$ est dite morphisme d'anneaux si :

(i) $f(1_A) = 1_B$.

(ii) $\forall (x, y) \in A \times A$, $f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$.

Un morphisme $f : A \to B$ est dit monom. (épim., isom.) si f est injective (resp. surjective, bijective).

Définition 2.19

Soient A et B deux anneaux. Une application $f : A \to B$ est dite morphisme d'anneaux si :

(i) $f(1_A) = 1_B$.

(ii) $\forall (x,y) \in A \times A,\ f(x+y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$.

Un morphisme $f : A \to B$ est dit monom. (épim., isom.) si f est injective (resp. surjective, bijective).

Un endomorphisme de A est un morphisme $A \to A$.

34

Définition 2.19

Soient A et B deux anneaux. Une application $f : A \to B$ est dite morphisme d'anneaux si :

(i) $f(1_A) = 1_B$.

(ii) $\forall (x, y) \in A \times A,\ f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$.

Un morphisme $f : A \to B$ est dit monom. (épim., isom.) si f est injective (resp. surjective, bijective).

Un endomorphisme de A est un morphisme $A \to A$.

Un automorphisme de A est un isomorphisme $A \to A$.

Définition 2.19

Soient A et B deux anneaux. Une application $f : A \to B$ est dite morphisme d'anneaux si :

(i) $f(1_A) = 1_B$.

(ii) $\forall (x,y) \in A \times A,\ f(x+y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$.

Un morphisme $f : A \to B$ est dit monom. (épim., isom.) si f est injective (resp. surjective, bijective).

Un endomorphisme de A est un morphisme $A \to A$.

Un automorphisme de A est un isomorphisme $A \to A$.

Le noyau d'un morphisme $f : A \to B$ est l'idéal de A défini par :

$$\ker(f) := \{x \in A \mid f(x) = 0_B\}.$$

Exemple 2.6

Soient A un anneau commutatif et $I \subset A$ un idéal. La surjection canonique $p : A \to A/I$ est un épimorphisme d'anneaux, qui s'appelle l'épimorphisme canonique.

35

Exemple 2.6

Soient A un anneau commutatif et $I \subset A$ un idéal. La surjection canonique $p : A \to A/I$ est un épimorphisme d'anneaux, qui s'appelle l'épimorphisme canonique.

Remarque 2.20

Soient $f : A \to B$, $g : B \to C$ morphismes d'anneaux. Alors :

(i) $g \circ f : A \to C$ est un morphisme d'anneaux.

Exemple 2.6

Soient A un anneau commutatif et $I \subset A$ un idéal. La surjection canonique $p : A \to A/I$ est un épimorphisme d'anneaux, qui s'appelle l'épimorphisme canonique.

Remarque 2.20

Soient $f : A \to B$, $g : B \to C$ morphismes d'anneaux. Alors :

(i) $g \circ f : A \to C$ est un morphisme d'anneaux.

(ii) Si f est un isomorphisme, alors l'application réciproque $f^{-1} : B \to A$ est un isomorphisme.

35

Exemple 2.6

Soient A un anneau commutatif et $I \subset A$ un idéal. La surjection canonique $p : A \to A/I$ est un épimorphisme d'anneaux, qui s'appelle l'épimorphisme canonique.

Remarque 2.20

Soient $f : A \to B$, $g : B \to C$ morphismes d'anneaux. Alors :

(i) $g \circ f : A \to C$ est un morphisme d'anneaux.

(ii) Si f est un isomorphisme, alors l'application réciproque $f^{-1} : B \to A$ est un isomorphisme.

Dém: Exercice. ∎

Proposition 2.21

Soit $f : A \to B$ un morphisme d'anneaux. Alors :

(i) $f(0_A) = 0_B$.

36

Proposition 2.21

Soit $f : A \to B$ un morphisme d'anneaux. Alors :

(i) $f(0_A) = 0_B$.

(ii) Pour tout $x \in A$ on a $f(-x) = -f(x)$.

Proposition 2.21

Soit $f : A \to B$ un morphisme d'anneaux. Alors :

(i) $f(0_A) = 0_B$.

(ii) Pour tout $x \in A$ on a $f(-x) = -f(x)$.

(iii) Si $x \in A^\times$, alors $f(x) \in B^\times$ et $f(x^{-1}) = (f(x))^{-1}$.

36

Proposition 2.21

Soit $f : A \to B$ un morphisme d'anneaux. Alors :

1. (i) $f(0_A) = 0_B$.
2. (ii) Pour tout $x \in A$ on a $f(-x) = -f(x)$.
3. (iii) Si $x \in A^\times$, alors $f(x) \in B^\times$ et $f(x^{-1}) = (f(x))^{-1}$.
4. (iv) Soit $A' \subset A$ un sous-anneau de A. Alors l'image $f(A')$ est un sous-anneau de B.

Proposition 2.21

Soit $f : A \to B$ un morphisme d'anneaux. Alors :

1. (i) $f(0_A) = 0_B$.
2. (ii) Pour tout $x \in A$ on a $f(-x) = -f(x)$.
3. (iii) Si $x \in A^\times$, alors $f(x) \in B^\times$ et $f(x^{-1}) = (f(x))^{-1}$.
4. (iv) Soit $A' \subset A$ un sous-anneau de A. Alors l'image $f(A')$ est un sous-anneau de B.
5. (v) Soit $I \subset A$ un idéal de A. Si f est surjective, alors l'image $f(I)$ est un idéal de B.

Proposition 2.21

Soit $f : A \to B$ un morphisme d'anneaux. Alors :

1. (i) $f(0_A) = 0_B$.
2. (ii) Pour tout $x \in A$ on a $f(-x) = -f(x)$.
3. (iii) Si $x \in A^\times$, alors $f(x) \in B^\times$ et $f(x^{-1}) = (f(x))^{-1}$.
4. (iv) Soit $A' \subset A$ un sous-anneau de A. Alors l'image $f(A')$ est un sous-anneau de B.
5. (v) Soit $I \subset A$ un idéal de A. Si f est surjective, alors l'image $f(I)$ est un idéal de B.
6. (vi) Soit $B' \subset B$ est un sous-anneau de B. Alors l'image réciproque $f^{-1}(B')$ est un sous-anneau de A.

Proposition 2.21

Soit $f : A \to B$ un morphisme d'anneaux. Alors :

1. (i) $f(0_A) = 0_B$.
2. (ii) Pour tout $x \in A$ on a $f(-x) = -f(x)$.
3. (iii) Si $x \in A^\times$, alors $f(x) \in B^\times$ et $f(x^{-1}) = (f(x))^{-1}$.
4. (iv) Soit $A' \subset A$ un sous-anneau de A. Alors l'image $f(A')$ est un sous-anneau de B.
5. (v) Soit $I \subset A$ un idéal de A. Si f est surjective, alors l'image $f(I)$ est un idéal de B.
6. (vi) Soit $B' \subset B$ est un sous-anneau de B. Alors l'image réciproque $f^{-1}(B')$ est un sous-anneau de A.
7. (vii) Soit $I \subset B$ est un idéal de B. Alors $f^{-1}(I)$ est un idéal de A.

36

Proposition 2.21

Soit $f : A \to B$ un morphisme d'anneaux. Alors :

(i) $f(0_A) = 0_B$.

(ii) Pour tout $x \in A$ on a $f(-x) = -f(x)$.

(iii) Si $x \in A^\times$, alors $f(x) \in B^\times$ et $f(x^{-1}) = (f(x))^{-1}$.

(iv) Soit $A' \subset A$ un sous-anneau de A. Alors l'image $f(A')$ est un sous-anneau de B.

(v) Soit $I \subset A$ un idéal de A. Si f est surjective, alors l'image $f(I)$ est un idéal de B.

(vi) Soit $B' \subset B$ est un sous-anneau de B. Alors l'image réciproque $f^{-1}(B')$ est un sous-anneau de A.

(vii) Soit $I \subset B$ est un idéal de B. Alors $f^{-1}(I)$ est un idéal de A.

(viii) f est injectif si et seulement $\ker(f) = \{0_A\}$.

Dém: Exercice. ■

37

Dém: Exercice. ■

En général l'image directe d'un idéal par un morphisme d'anneaux n'est pas nécessairement un idéal. Par exemple l'image de $\mathbb{Z}$ par le morphisme d'inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ n'est pas un idéal de $\mathbb{Q}$.

Dém: Exercice. ∎

En général l'image directe d'un idéal par un morphisme d'anneaux n'est pas nécessairement un idéal. Par exemple l'image de $\mathbb{Z}$ par le morphisme d'inclusion $\mathbb{Z} \hookrightarrow \mathbb{Q}$ n'est pas un idéal de $\mathbb{Q}$.

L'anneau quotient est caractérisé par une propriété universelle. Sa démonstration utilise la méthode utilisée pour la propriété universelle du groupe quotient.

Théorème 2.22 (la propriété universelle de l'anneau quotient)

Soient A, B anneaux commutatifs, I un idéal de A, $p : A \to A/I$ l'épimorphisme canonique et $f : A \to B$ un morphisme.

1. Il existe un morphisme $\bar{f} : A/I \to B$ tel que $\bar{f} \circ p = f$ si et seulement si $I \subset \ker(f)$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p"'] & B \\ A/I \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Théorème 2.22 (la propriété universelle de l'anneau quotient)

Soient A, B anneaux commutatifs, I un idéal de A, $p : A \to A/I$ l'épimorphisme canonique et $f : A \to B$ un morphisme.

1. Il existe un morphisme $\bar{f} : A/I \to B$ tel que $\bar{f} \circ p = f$ si et seulement si $I \subset \ker(f)$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p"'] & B \\ A/I \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

2. Si cette condition est vérifiée, alors
   1. $\bar{f}$ est unique, $\ker(\bar{f}) = \ker(f)/I$ et $\mathrm{im}(\bar{f}) = \mathrm{im}(f)$.

Théorème 2.22 (la propriété universelle de l'anneau quotient)

Soient A, B anneaux commutatifs, I un idéal de A, $p : A \to A/I$ l'épimorphisme canonique et $f : A \to B$ un morphisme.

1. Il existe un morphisme $\bar{f} : A/I \to B$ tel que $\bar{f} \circ p = f$ si et seulement si $I \subset \ker(f)$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p"'] & B \\ A/I \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

2. Si cette condition est vérifiée, alors
   1. $\bar{f}$ est unique, $\ker(\bar{f}) = \ker(f)/I$ et $\mathrm{im}(\bar{f}) = \mathrm{im}(f)$.
   2. $\bar{f}$ est un monomorphisme si et seulement si $I = \ker(f)$.

Théorème 2.22 (la propriété universelle de l'anneau quotient)

Soient A, B anneaux commutatifs, I un idéal de A, $p : A \to A/I$ l'épimorphisme canonique et $f : A \to B$ un morphisme.

1. Il existe un morphisme $\bar{f} : A/I \to B$ tel que $\bar{f} \circ p = f$ si et seulement si $I \subset \ker(f)$.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "p"'] & B \\ A/I \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

2. Si cette condition est vérifiée, alors
   1. $\bar{f}$ est unique, $\ker(\bar{f}) = \ker(f)/I$ et $\mathrm{im}(\bar{f}) = \mathrm{im}(f)$.
   2. $\bar{f}$ est un monomorphisme si et seulement si $I = \ker(f)$.
   3. $\bar{f}$ est un épimorphisme si et seulement si f est un épimorphisme.

Comme dans la théorie des groupes on obtient un théorème d'isomorphisme pour les morphismes d'anneaux :

Théorème 2.23 (le 1er th. d'isomorphisme pour les anneaux)

Soient A, B anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux. Alors la formule $\varphi([x]_I) := f(x)$ définit un isomorphisme

$$\varphi : A/\ker(f) \xrightarrow{\simeq} \mathrm{im}(f)\,.$$

39

Comme dans la théorie des groupes on obtient un théorème d'isomorphisme pour les morphismes d'anneaux :

Théorème 2.23 (le 1er th. d'isomorphisme pour les anneaux)

Soient A, B anneaux commutatifs et $f : A \to B$ un morphisme d'anneaux. Alors la formule $\varphi([x]_I) := f(x)$ définit un isomorphisme

$$\varphi : A/\ker(f) \xrightarrow{\simeq} \mathrm{im}(f)\,.$$

Exemple 2.7

Soient $K[X]$ l'anneau des polynômes a coefficients dans un corps K et $f : K[X] \to K$ le morphisme défini par $f(P(X)) := P(0)$. Nous avons $\ker(f) = (X)$, donc $K[X]/(X) \simeq K$.

40

Soit A un anneau. L'application

$$\gamma_A : \mathbb{Z} \to A,\ \gamma_A(n) := n 1_A$$

est un morphisme d'anneaux.

40

Soit A un anneau. L'application

$$\gamma_A : \mathbb{Z} \to A,\ \gamma_A(n) := n1_A$$

est un morphisme d'anneaux.
C'est l'unique morphisme d'anneaux de $\mathbb{Z}$ vers A.

40

Soit A un anneau. L'application

$$\gamma_A : \mathbb{Z} \to A,\ \gamma_A(n) := n1_A$$

est un morphisme d'anneaux.
C'est l'unique morphisme d'anneaux de $\mathbb{Z}$ vers A.
Son noyau est un idéal de $\mathbb{Z}$, donc s'écrit sous la forme $c_A\mathbb{Z}$ pour un nombre $c_A \in \mathbb{N}$ qui dépend seulement de l'anneau A.

40

Soit A un anneau. L'application

$$\gamma_A : \mathbb{Z} \to A,\ \gamma_A(n) := n 1_A$$

est un morphisme d'anneaux.
C'est l'unique morphisme d'anneaux de $\mathbb{Z}$ vers A.
Son noyau est un idéal de $\mathbb{Z}$, donc s'écrit sous la forme $c_A\mathbb{Z}$ pour un nombre $c_A \in \mathbb{N}$ qui dépend seulement de l'anneau A.
On a donc

$$c_A = \begin{cases} 0 & \text{si} \quad \ker(\gamma_A) = \{0\}, \\ \min\{k \in \mathbb{N}^* |\ k 1_A = 0_A\} = \mathrm{ord}(1_A) & \text{si} \quad \ker(\gamma_A) \neq \{0\}. \end{cases}$$

40

Soit A un anneau. L'application

$$\gamma_A : \mathbb{Z} \to A,\ \gamma_A(n) := n1_A$$

est un morphisme d'anneaux.
C'est l'unique morphisme d'anneaux de $\mathbb{Z}$ vers A.
Son noyau est un idéal de $\mathbb{Z}$, donc s'écrit sous la forme $c_A\mathbb{Z}$ pour un nombre $c_A \in \mathbb{N}$ qui dépend seulement de l'anneau A.
On a donc

$$c_A = \begin{cases} 0 & \text{si} \quad \ker(\gamma_A) = \{0\}, \\ \min\{k \in \mathbb{N}^* |\, k1_A = 0_A\} = \mathrm{ord}(1_A) & \text{si} \quad \ker(\gamma_A) \neq \{0\}. \end{cases}$$

Définition 2.24

Le nombre naturel c_A défini par l'égalité $\ker(\gamma_A) = c_A\mathbb{Z}$ s'appelle la caractéristique de l'anneau A.

Le 1er théorème d'isomorphisme donne un isomorphisme

$$\bar{\gamma}_A : \mathbb{Z}/c_A\mathbb{Z} \to \mathrm{im}(\gamma_A) := \{k 1_A \mid k \in \mathbb{Z}\}.$$

Remarque 2.25

Si A est un anneau intègre (en particulier un corps) alors c_A est soit 0, soit un nombre premier.

Dém: Exercice. Pour la 2ème affirmation utiliser la remarque 2.4 et la proposition 1.17.

Exemples 2.2

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des anneaux de caractéristique 0.
2. $\mathbb{Z}_n$ et $\mathbb{Z}_n[X]$ sont des anneaux de caractéristique n.