Chapitre 2 : Anneaux

L3-S5. Algèbre générale 1

Licence Mathématiques
Université d'Avignon

Année 2018–2019

I. Les anneaux
1. Structure d'anneaux

Définition : Anneau

Soit A un ensemble muni de deux lois de composition interne $+$ et $*$. On dit que $(A,+,*)$ est un *anneau* si :

1. $(A,+)$ est un groupe abélien ;
2. la loi $*$ est associative et possède un élément neutre ;
3. la loi $*$ est distributive par rapport à $+$.

Si, de plus, la loi $*$ est commutative, on dit que $(A,+,*)$ est un *anneau commutatif*.

Rappel. On dit que $*$ est *distributive* par rapport à $+$ si, pour tout $x,y,z\in A$, on a : $x*(y+z)=x*y+x*z$ (distributivité à gauche), et $(y+z)*x=y*x+z*x$ (distributivité à droite). Pour l'évaluation de $x+y*z$, on donne priorité à $*$ (et les parenthèses deviennent inutiles).

- La loi $+$ (resp. $*$) s'appelle l'*addition* (resp. la *multiplication*) de l'anneau $(A, +, *)$.
- Le neutre de $+$ est noté 0 ; $-x$ désigne l'opposé de x.
- Le neutre de $*$ se note 1, 1_A, e, I etc...selon les cas.

- La loi $+$ (resp. $*$) s'appelle l'*addition* (resp. la *multiplication*) de l'anneau $(A, +, *)$.
- Le neutre de $+$ est noté 0 ; $-x$ désigne l'opposé de x.
- Le neutre de $*$ se note 1, 1_A, e, I etc...selon les cas.

Remarques.

① Le seul anneau A pour lequel $1_A = 0$ est l'anneau nul $\{0\}$ dont les lois sont triviales.

- La loi $+$ (resp. $*$) s'appelle l'*addition* (resp. la *multiplication*) de l'anneau $(A, +, *)$.
- Le neutre de $+$ est noté 0 ; $-x$ désigne l'opposé de x.
- Le neutre de $*$ se note 1, 1_A, e, I etc...selon les cas.

Remarques.

① Le seul anneau A pour lequel $1_A = 0$ est l'anneau nul $\{0\}$ dont les lois sont triviales.

② On considérera souvent des anneaux commutatifs.

- La loi $+$ (resp. $*$) s'appelle l'*addition* (resp. la *multiplication*) de l'anneau $(A, +, *)$.
- Le neutre de $+$ est noté 0 ; $-x$ désigne l'opposé de x.
- Le neutre de $*$ se note 1, 1_A, e, I etc...selon les cas.

Remarques.
① Le seul anneau A pour lequel $1_A = 0$ est l'anneau nul $\{0\}$ dont les lois sont triviales.
② On considérera souvent des anneaux commutatifs.
③ En pratique, on notera $\times$, ou $.$ la deuxième loi "multiplicative", ou même, on l'omettra simplement, notant simplement xy le produit de deux éléments.

Exemples

1. **Anneaux de nombres.** Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis des lois d'addition et multiplication usuelles sont des anneaux commutatifs.

Exemples

1. **Anneaux de nombres.** Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis des lois d'addition et multiplication usuelles sont des anneaux commutatifs.
2. **Matrices.** L'ensemble $\mathcal{M}_n(\mathbb{K})$ des matrices $n \times n$ à coefficients réels ou complexes muni des lois d'addition et multiplication usuelles des matrices est un anneau.

   Le neutre pour $+$ est 0 (matrice nulle) et le neutre pour $\times$ est I_n (matrice identité $n \times n$).

Exemples

1. **Anneaux de nombres.** Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis des lois d'addition et multiplication usuelles sont des anneaux commutatifs.
2. **Matrices.** L'ensemble $\mathcal{M}_n(\mathbb{K})$ des matrices $n \times n$ à coefficients réels ou complexes muni des lois d'addition et multiplication usuelles des matrices est un anneau.

   Le neutre pour $+$ est 0 (matrice nulle) et le neutre pour $\times$ est I_n (matrice identité $n \times n$).
3. **Anneaux arithmétiques.** $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe abélien où $\overline{x} + \overline{y} = \overline{x+y}$. La multiplication étant aussi compatible avec la congruence modulo n, on peut définir le produit $\overline{x} \times \overline{y} = \overline{xy}$ reste modulo n du produit xy. Alors,

$$(\mathbb{Z}/n\mathbb{Z}, +, \times) \textbf{ est un anneau de neutres } \overline{\mathbf{0}} \textbf{ et } \overline{\mathbf{1}}.$$

4. **Endomorphismes.** Notons $\mathrm{End}(G)$ l'ensemble des endomorphismes du groupe commutatif $(G, +)$. Alors $(\mathrm{End}(G), +, \circ)$ est un anneau (non commutatif).

   Le neutre pour $+$ est 0 (fonction nulle) et le neutre pour $\circ$ est l'application identité de G.

4. **Endomorphismes.** Notons $\mathrm{End}(G)$ l'ensemble des endomorphismes du groupe commutatif $(G, +)$. Alors $(\mathrm{End}(G), +, \circ)$ est un anneau (non commutatif).

   Le neutre pour $+$ est 0 (fonction nulle) et le neutre pour $\circ$ est l'application identité de G.

5. **Fonctions.** Notons $\mathcal{F}(X, \mathbb{K})$ l'ensemble des fonctions de l'ensemble X à valeurs réelles ou complexes. Alors $(\mathcal{F}(X, \mathbb{K}), +, \times)$ est un anneau commutatif.

   Le neutre pour $+$ est 0 (fonction nulle) et le neutre pour $\times$ est l'application constante 1.

4. **Endomorphismes.** Notons $\mathrm{End}(G)$ l'ensemble des endomorphismes du groupe commutatif $(G,+)$. Alors $(\mathrm{End}(G),+,\circ)$ est un anneau (non commutatif).

   Le neutre pour $+$ est 0 (fonction nulle) et le neutre pour $\circ$ est l'application identité de G.

5. **Fonctions.** Notons $\mathcal{F}(X,\mathbb{K})$ l'ensemble des fonctions de l'ensemble X à valeurs réelles ou complexes. Alors $(\mathcal{F}(X,\mathbb{K}),+,\times)$ est un anneau commutatif.

   Le neutre pour $+$ est 0 (fonction nulle) et le neutre pour $\times$ est l'application constante 1.

   Si $X=\mathbb{N}$, c'est l'anneau des suites réelles ou complexes.

2. Règles de calcul

Proposition

Soit $(A, +, .)$ un anneau. Alors, pour tout x, y, z dans A :

1. $x.0 = 0.x = 0$
2. $x.(-y) = (-x).y = -(x.y)$
3. $x.(y - z) = x.y - x.z$
4. si $x.y = y.x$, alors $(x.y)^n = x^n.y^n$ et
   $$x^n - y^n = (x - y)\sum_{k=0}^{n-1} x^k y^{n-1-k} \text{ pour tout } n \in \mathbb{N},$$

Remarque. $y + (-z)$ s'écrit $y - z$.

Exemple. Pour tout $x \in A$, on a $1_A - x^n = (1_A - x)\sum_{k=0}^{n-1} x^k$.

Théorème : formule du binôme de Newton

Soit $(A, +, \times)$ un anneau. Alors, pour tout x, y dans A tels que $xy = yx$ on a :

$$(x+y)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) x^k y^{n-k}$$

où $\left(\begin{array}{c} n \\ k \end{array} \right) = \dfrac{n!}{k!(n-k)!}$ est le coefficient binômial.

La démonstration est "identique" à celle dans $\mathbb{R}$ (on effectue une récurrence sur n).

Exemple. Pour tout $x \in A$, on a $(1_A + x)^n = \sum_{k=0}^{n} \left(\begin{array}{c} n \\ k \end{array} \right) x^k$.

3. Anneaux intègres

Définition : Unité d'un anneau

Une *unité* d'un anneau $(A, +, \times)$ est un élément de A inversible pour la loi $\times$, c.–à–d. admettant un inverse.

On note $\boldsymbol{U(A)}$ l'ensemble des unités de A ; il contient toujours 1_A.

3. Anneaux intègres

Définition : Unité d'un anneau

Une *unité* d'un anneau $(A, +, \times)$ est un élément de A inversible pour la loi $\times$, c.–à–d. admettant un inverse.

On note $\boldsymbol{U(A)}$ l'ensemble des unités de A ; il contient toujours 1_A. Si A n'est pas l'anneau nul, $U(A) \subset A \backslash \{0\}$.

3. Anneaux intègres

Définition : Unité d'un anneau

Une *unité* d'un anneau $(A, +, \times)$ est un élément de A inversible pour la loi $\times$, c.–à–d. admettant un inverse.

On note $\boldsymbol{U(A)}$ l'ensemble des unités de A ; il contient toujours 1_A. Si A n'est pas l'anneau nul, $U(A) \subset A \backslash \{0\}$.

Théorème

L'ensemble $(U(A), \times)$ est un groupe (multiplicatif).

3. Anneaux intègres

Définition : Unité d'un anneau

Une *unité* d'un anneau $(A, +, \times)$ est un élément de A inversible pour la loi $\times$, c.–à–d. admettant un inverse.

On note $\boldsymbol{U(A)}$ l'ensemble des unités de A ; il contient toujours 1_A. Si A n'est pas l'anneau nul, $U(A) \subset A \backslash \{0\}$.

Théorème

L'ensemble $(U(A), \times)$ est un groupe (multiplicatif).

dém. Tout d'abord, $U(A)$ est stable par $\times$: pour tout $x, y \in U(A)$, $xy \in U(A)$ avec $(xy)^{-1} = y^{-1}x^{-1}$. Donc, $U(A)$ est muni de la loi induite $\times$ par celle de A ; elle est donc associative et possède un élément neutre 1_A. Par définition des unités, tout élément de $U(A)$ est inversible. ∎

Exemples

- Le groupe des unités de $(\mathbb{Z}, +, \times)$ est $\{-1, 1\}$.

Exemples

- Le groupe des unités de $(\mathbb{Z}, +, \times)$ est $\{-1, 1\}$.
- Le groupe des unités de $(\mathbb{K}, +, \times)$ est $\mathbb{K} \backslash \{0\}$.

Exemples

- Le groupe des unités de $(\mathbb{Z}, +, \times)$ est $\{-1, 1\}$.
- Le groupe des unités de $(\mathbb{K}, +, \times)$ est $\mathbb{K} \backslash \{0\}$.
- Le groupe des unités de $(\mathcal{M}_n(\mathbb{K}), +, \times)$ est $GL(n, \mathbb{K})$.

Exemples

- Le groupe des unités de $(\mathbb{Z}, +, \times)$ est $\{-1, 1\}$.
- Le groupe des unités de $(\mathbb{K}, +, \times)$ est $\mathbb{K}\backslash\{0\}$.
- Le groupe des unités de $(\mathcal{M}_n(\mathbb{K}), +, \times)$ est $GL(n, \mathbb{K})$.
- Le groupe des unités de $(\mathbb{Z}/2\mathbb{Z}, +, \times)$ est $\{\overline{1}\}$.

Exemples

- Le groupe des unités de $(\mathbb{Z}, +, \times)$ est $\{-1, 1\}$.
- Le groupe des unités de $(\mathbb{K}, +, \times)$ est $\mathbb{K} \backslash \{0\}$.
- Le groupe des unités de $(\mathcal{M}_n(\mathbb{K}), +, \times)$ est $GL(n, \mathbb{K})$.
- Le groupe des unités de $(\mathbb{Z}/2\mathbb{Z}, +, \times)$ est $\{\overline{1}\}$.

- Le groupe des unités de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est l'ensemble des $\overline{x}$, $x \in [\![1, n-1]\!]$ premier avec n ; c'est donc aussi l'ensemble des générateurs du groupe $(\mathbb{Z}/n\mathbb{Z}, +)$.

En effet,
$$\begin{aligned} \overline{x} \in U(\mathbb{Z}/n\mathbb{Z}) &\iff \exists y \in \mathbb{Z},\ \overline{xy} = \overline{1} \\ &\iff \exists y, k \in \mathbb{Z},\ xy + kn = 1 \\ &\iff x \wedge n = 1 \end{aligned}$$
d'après le théorème de Bezout.

Complément : Fonction indicatrice d'Euler

La fonction indicatrice d'Euler est l'application $\varphi : \mathbb{N}^\star \to \mathbb{N}^\star$ définie par

$$\boldsymbol{\varphi(n) = \mathbf{Card}(U(\mathbb{Z}/n\mathbb{Z}))}$$

autrement dit c'est le nombre d'éléments $\overline{x}$, $x \in [\![1, n-1]\!]$ premier avec n.

Complément : Fonction indicatrice d'Euler

La fonction indicatrice d'Euler est l'application $\varphi : \mathbb{N}^\star \to \mathbb{N}^\star$ définie par

$$\boldsymbol{\varphi(n) = \mathbf{Card}(U(\mathbb{Z}/n\mathbb{Z}))}$$

autrement dit c'est le nombre d'éléments $\overline{x}$, $x \in [\![1, n-1]\!]$ premier avec n.

Exemples. $\varphi(1) = 1$, $\varphi(12) = \mathrm{Card}(\{1, 5, 7, 11\}) = 4$.

Complément : Fonction indicatrice d'Euler

La fonction indicatrice d'Euler est l'application $\varphi : \mathbb{N}^\star \to \mathbb{N}^\star$ définie par

$$\boldsymbol{\varphi(n) = \mathbf{Card}(U(\mathbb{Z}/n\mathbb{Z}))}$$

autrement dit c'est le nombre d'éléments $\overline{x}$, $x \in [\![1, n-1]\!]$ premier avec n.

Exemples. $\varphi(1) = 1$, $\varphi(12) = \text{Card}(\{1, 5, 7, 11\}) = 4$.

Si p est un nombre premier, $\varphi(p) = p - 1$.

Complément : Fonction indicatrice d'Euler

La fonction indicatrice d'Euler est l'application $\varphi : \mathbb{N}^\star \to \mathbb{N}^\star$ définie par

$$\boldsymbol{\varphi(n) = \mathbf{Card}(U(\mathbb{Z}/n\mathbb{Z}))}$$

autrement dit c'est le nombre d'éléments $\overline{x}$, $x \in [\![1, n-1]\!]$ premier avec n.

Exemples. $\varphi(1) = 1$, $\varphi(12) = \mathrm{Card}(\{1, 5, 7, 11\}) = 4$.
Si p est un nombre premier, $\varphi(p) = p - 1$.

Théorème d'Euler

Soit $n \in \mathbb{N}^\star$. Si a est un entier premier avec n alors $a^{\varphi(n)} \equiv 1[n]$.

En particulier, si n est premier, et a n'est pas divisible par n, alors $a^{n-1} \equiv 1[n]$, ce qui équivaut à :

Petit théorème de Fermat

Soit n un nombre premier. Pour tout entier a, on a : $a^n \equiv a[n]$.

Définition : Diviseurs de zéro

Soit $(A, +, \times)$ un anneau (commutatif). Un *diviseur de zéro* est un élément x de A tel que :

- x est non nul : $x \neq 0$,
- il existe un élément non-nul y de A tel que $xy = yx = 0$.

Définition : Diviseurs de zéro

Soit $(A, +, \times)$ un anneau (commutatif). Un *diviseur de zéro* est un élément x de A tel que :

- x est non nul : $x \neq 0$,
- il existe un élément non-nul y de A tel que $xy = yx = 0$.

Le neutre 0 n'est pas un diviseur de zéro.
Les unités ne sont pas des diviseurs de zéro.

Définition : Diviseurs de zéro

Soit $(A, +, \times)$ un anneau (commutatif). Un *diviseur de zéro* est un élément x de A tel que :

- x est non nul : $x \neq 0$,
- il existe un élément non-nul y de A tel que $xy = yx = 0$.

Le neutre 0 n'est pas un diviseur de zéro.
Les unités ne sont pas des diviseurs de zéro.

Exemples

- Dans $(\mathcal{M}_2(\mathbb{R}), +, \times)$, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ et $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ sont des diviseurs de zéros.
- Dans $(\mathbb{Z}^2, +, \times)$, $(1, 0)$ et $(0, 1)$ sont des diviseurs de zéro.
- Dans $(\mathbb{Z}/6\mathbb{Z}, +, \times)$, $\overline{2}$ et $\overline{3}$ sont des diviseurs de zéro.

Définition : Anneau intègre

Un anneau $(A, +, \times)$ (commutatif) est *intègre* si

- A n'est pas l'anneau nul
- A n'admet aucun diviseur de zéro, c.–à–d.

$$\forall x, y \in A,\ xy = 0 \Rightarrow x = 0 \text{ ou } y = 0$$

Ainsi, un anneau intègre est "sans diviseur de zéro".

Définition : Anneau intègre

Un anneau $(A, +, \times)$ (commutatif) est *intègre* si

- A n'est pas l'anneau nul
- A n'admet aucun diviseur de zéro, c.–à–d.

$$\forall x, y \in A,\ xy = 0 \Rightarrow x = 0 \text{ ou } y = 0$$

Ainsi, un anneau intègre est “sans diviseur de zéro”.

Exemples

- Les anneaux $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$ sont tous intègres.
- Les anneaux $(\mathbb{Z}^2, +, \times)$ et $(\mathbb{Z}/6\mathbb{Z}, +, \times)$ ne sont pas intègres.
- $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si $n = 0$ ou n premier.

Dans un anneau intègre A, l'équation $x^2 = 1_A$ a pour solution solutions 1_A et -1_A, ce qui n'est pas le cas lorsque A n'est pas intègre.

Exemples. Dans $(\mathbb{R}^2, +, \times)$, $(x, y)^2 = (1, 1)$ a pour solutions $(1, 1)$, $(-1, 1)$, $(1, -1)$ et $(-1, -1)$.

Dans un anneau intègre A, l'équation $x^2 = 1_A$ a pour solution solutions 1_A et -1_A, ce qui n'est pas le cas lorsque A n'est pas intègre.

Exemples. Dans $(\mathbb{R}^2, +, \times)$, $(x, y)^2 = (1, 1)$ a pour solutions $(1, 1)$, $(-1, 1)$, $(1, -1)$ et $(-1, -1)$.

Dans $(\mathcal{M}_2(\mathbb{R}), +, \times)$, $A^2 = I$ a pour solutions $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 2 & -3 \\ 1 & -2 \end{pmatrix}$, $\begin{pmatrix} 2 & -1 \\ 3 & -2 \end{pmatrix}$, $\begin{pmatrix} 3 & 4 \\ -2 & -3 \end{pmatrix}$, etc ....

4. Sous-anneaux

Définition : Sous-anneaux

Soit $(A, +, \times)$ un anneau (commutatif). Un sous-ensemble B de A est un sous-anneau de A si :

- B est un sous-groupe de $(A, +)$,
- B est stable pour la loi $\times$,
- B contient 1_A.

4. Sous-anneaux

Définition : Sous-anneaux

Soit $(A, +, \times)$ un anneau (commutatif). Un sous-ensemble B de A est un sous-anneau de A si :

- B est un sous-groupe de $(A, +)$,
- B est stable pour la loi $\times$,
- B contient 1_A.

Bien vérifier $1_A \in B$ et non $0 \in B$ ou seulement $B \neq \emptyset$.

Par exemple $B = \{\overline{0}, \overline{2}, \overline{4}\}$ n'est pas un sous-anneau de $\mathbb{Z}/6\mathbb{Z}$.
Pourtant c'est un anneau de neutre $\overline{4}$.

Exemples

- A est un sous-anneau de l'anneau $(A, +, \times)$.
- $\mathbb{Z}$ est un sous-anneau de $(\mathbb{R}, +, \times)$, mais $2\mathbb{Z}$ n'est pas un sous-anneau de $(\mathbb{R}, +, \times)$.
- Soit I un intervalle de $\mathbb{R}$ non réduit à un point. L'ensemble $\mathcal{C}^k(I, \mathbb{K})$, $k \in \mathbb{N} \cup \{+\infty\}$, est un sous-anneau de $(\mathcal{F}(I, \mathbb{K}), +, \times)$.

Exemples

- A est un sous-anneau de l'anneau $(A, +, \times)$.
- $\mathbb{Z}$ est un sous-anneau de $(\mathbb{R}, +, \times)$, mais $2\mathbb{Z}$ n'est pas un sous-anneau de $(\mathbb{R}, +, \times)$.
- Soit I un intervalle de $\mathbb{R}$ non réduit à un point. L'ensemble $\mathcal{C}^k(I, \mathbb{K})$, $k \in \mathbb{N} \cup \{+\infty\}$, est un sous-anneau de $(\mathcal{F}(I, \mathbb{K}), +, \times)$.

Propriété

Un sous-ensemble $B \subset A$ est un sous-anneau si et seulement si :

- $1_A \in B$,
- $\forall x, y \in B,\ x - y \in B$,
- $\forall x, y \in B,\ xy \in B$.

Théorème

Si B est un sous-anneau de $(A, +, \times)$, B peut être muni des lois $+$ et $\times$ définies par restriction des lois sur A et alors $(B, +, \times)$ est un anneau de même neutres que A.

Théorème

Si B est un sous-anneau de $(A, +, \times)$, B peut être muni des lois $+$ et $\times$ définies par restriction des lois sur A et alors $(B, +, \times)$ est un anneau de même neutres que A.

Propriétés

Si B_1 et B_2 sont des sous-anneaux de $(A, +, \times)$, alors $B_1 \cap B_2$ est aussi un sous-anneau de A.

Ce résultat se généralise à : l'intersection d'une famille quelconque de sous-anneaux est encore un sous-anneau.

5. Anneau produit

Théorème

Soit $(A_i)_{i\in I}$ une famille d'anneaux. Alors, le produit $\prod_{i\in I} A_i$ muni des lois produits est un anneau.

Les lois produits :

$$(x_i)_{\in I} + (y_i)_{i\in I} \overset{\text{déf.}}{=} (x_i + y_i)_{i\in I}$$

$$(x_i)_{\in I} \times (y_i)_{i\in I} \overset{\text{déf.}}{=} (x_i \times y_i)_{i\in I}$$

5. Anneau produit

Théorème

Soit $(A_i)_{i\in I}$ une famille d'anneaux. Alors, le produit $\prod_{i\in I} A_i$ muni des lois produits est un anneau.

Les lois produits :

$$(x_i)_{\in I} + (y_i)_{i\in I} \stackrel{\text{déf.}}{=} (x_i + y_i)_{i\in I}$$

$$(x_i)_{\in I} \times (y_i)_{i\in I} \stackrel{\text{déf.}}{=} (x_i \times y_i)_{i\in I}$$

Cas particulier : si les A_i sont tous égaux, alors $\prod_{i\in I} A_i$ est l'ensemble A^I des applications de I vers A.

$$\forall f, g \in A^I, \quad \forall i \in I, \quad (f+g)(i) \stackrel{\text{déf.}}{=} f(i) + g(i)$$

$$\forall f, g \in A^I, \quad \forall i \in I, \quad f.g(i) \stackrel{\text{déf.}}{=} f(i) \times g(i)$$

II. Idéaux

1. Idéaux d'un anneau commutatif

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

Définition : Idéal

Un sous-ensemble I de A est un *idéal* si :

- $(I, +)$ est un sous-groupe de $(A, +)$,
- $\forall a \in A,\ \forall x \in I,\ xa \in I$.

II. Idéaux

1. Idéaux d'un anneau commutatif

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

Définition : Idéal

Un sous-ensemble I de A est un *idéal* si :

- $(I, +)$ est un sous-groupe de $(A, +)$,
- $\forall a \in A,\ \forall x \in I,\ xa \in I$.

Proposition

Une partie $I \subset A$ est un idéal de A si et seulement si :

- $0 \in I$,
- $\forall x, y \in I,\ x + y \in I$,
- $\forall a \in A,\ \forall x \in I,\ xa \in I$.

Remarques.

1. Soit I un idéal de $(A, +, \times)$. Alors :

$$I = A \iff 1_A \in I \iff I \cap U(A) \neq \emptyset.$$

Remarques.

1. Soit I un idéal de $(A, +, \times)$. Alors :

$$I = A \iff 1_A \in I \iff I \cap U(A) \neq \emptyset.$$

2. Les idéaux triviaux de A sont $\{0\}$ et A.

Remarques.

1. Soit I un idéal de $(A, +, \times)$. Alors :

$$I = A \iff 1_A \in I \iff I \cap U(A) \neq \emptyset.$$

2. Les idéaux triviaux de A sont $\{0\}$ et A.

3. **Idéal $\neq$ sous-anneau**.

   Par exemple, $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$ mais pas un idéal.
   $\{\overline{0}, \overline{2}, \overline{4}\}$ est un idéal de $\mathbb{Z}/6\mathbb{Z}$ mais pas un sous-anneau.

Remarques.

1. Soit I un idéal de $(A, +, \times)$. Alors :

$$I = A \iff 1_A \in I \iff I \cap U(A) \neq \emptyset.$$

2. Les idéaux triviaux de A sont $\{0\}$ et A.

3. **Idéal $\neq$ sous-anneau.**

   Par exemple, $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$ mais pas un idéal.

   $\{\overline{0}, \overline{2}, \overline{4}\}$ est un idéal de $\mathbb{Z}/6\mathbb{Z}$ mais pas un sous-anneau.

Théorème

Les idéaux de $(\mathbb{Z}, +, \times)$ sont de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$.

2. Opérations

Théorème : intersection

Si I et J sont deux idéaux de $(A, +, \times)$, alors $I \cap J$ est un idéal de A.

$I \cap J$ est le plus grand idéal inclus dans I et J. Le résultat se généralise à une intersection d'une famille d'idéaux.

2. Opérations

Théorème : intersection

Si I et J sont deux idéaux de $(A,+,\times)$, alors $I \cap J$ est un idéal de A.

$I \cap J$ est le plus grand idéal inclus dans I et J. Le résultat se généralise à une intersection d'une famille d'idéaux.

Théorème : somme

Si I et J sont deux idéaux de $(A,+,\times)$, alors
$I + J \stackrel{\text{déf.}}{=} \{x + y / x \in I, y \in J\}$ est un idéal de A.

$I + J$ est le plus petit idéal contenant I et J.

3. Idéal engendré par un élément

Définition : Idéal engendré par un élément

On appelle *idéal engendré* par $x \in A$ l'ensemble

$$xA \overset{\text{déf.}}{=} \{xu/u \in A\}.$$

3. Idéal engendré par un élément

Définition : Idéal engendré par un élément

On appelle *idéal engendré* par $x \in A$ l'ensemble

$$xA \overset{\text{déf.}}{=} \{xu / u \in A\}.$$

Théorème

xA est un idéal contenant l'élément x et inclus dans tout idéal contenant x.

Autrement dit c'est le plus petit (pour l'inclusion) idéal de A contenant x.

3. Idéal engendré par un élément

Définition : Idéal engendré par un élément

On appelle *idéal engendré* par $x \in A$ l'ensemble

$$xA \overset{\text{déf.}}{=} \{xu / u \in A\}.$$

Théorème

xA est un idéal contenant l'élément x et inclus dans tout idéal contenant x.

Autrement dit c'est le plus petit (pour l'inclusion) idéal de A contenant x.

Exemple

L'idéal de $\mathbb{Z}$ engendré par n est $n\mathbb{Z}$.

III. Morphismes d'anneaux

1. Morphismes d'anneaux

Définition

Soit $(A, +, \times)$ et $(A', +, \times)$ deux anneaux. On appelle *morphisme* d'anneaux toute application $f : A \to A'$ vérifiant

1. $\forall x, y \in A,\ f(x + y) = f(x) + f(y)$,
2. $\forall x, y \in A,\ f(xy) = f(x)f(y)$,
3. $f(1_A) = 1_{A'}$.

En particulier, $f : A \to A'$ est un morphisme de groupes additifs.

III. Morphismes d'anneaux

1. Morphismes d'anneaux

Définition

Soit $(A, +, \times)$ et $(A', +, \times)$ deux anneaux. On appelle *morphisme* d'anneaux toute application $f : A \to A'$ vérifiant

1. $\forall x, y \in A,\ f(x+y) = f(x) + f(y)$,
2. $\forall x, y \in A,\ f(xy) = f(x)f(y)$,
3. $f(1_A) = 1_{A'}$.

En particulier, $f : A \to A'$ est un morphisme de groupes additifs. Aussi,

- Un morphisme de A vers A est un *endomorphisme* de A.
- Un morphisme bijectif de A vers A' est un *isomorphisme* de A vers A'.
- Un endomorphisme bijectif de A vers A est un *automorphisme* de A.

Exemples

1. L'application identité $\mathrm{Id}_A : A \to A$ est un automorphisme de $(A, +, \times)$.
2. L'application $\varphi_A : \mathbb{Z} \to A$ définie par $\varphi_A(k) = k.1_A$ est un morphisme de $(\mathbb{Z}, +, \times)$ vers $(A, +, \times)$.
3. Soit $a \in U(A)$. L'application $\tau_a : A \to A$ définie par $\tau_a(x) = axa^{-1}$ est un automorphisme de $(A, +, \times)$

Exemples

1. L'application identité $\mathrm{Id}_A : A \to A$ est un automorphisme de $(A, +, \times)$.
2. L'application $\varphi_A : \mathbb{Z} \to A$ définie par $\varphi_A(k) = k.1_A$ est un morphisme de $(\mathbb{Z}, +, \times)$ vers $(A, +, \times)$.
3. Soit $a \in U(A)$. L'application $\tau_a : A \to A$ définie par $\tau_a(x) = axa^{-1}$ est un automorphisme de $(A, +, \times)$

Propriétés

Si $f : A \to A'$ est un morphisme d'anneaux,

1. $f(0) = 0$,
2. $\forall x \in A,\ f(-x) = -f(x)$,
3. $\forall x \in U(A),\ f(x^{-1}) = (f(x))^{-1}$.

2. Image et noyau d'un morphisme

Théorème

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

1. Si B est un sous-anneau de A, alors $f(B)$ est un sous-anneau de A'.
2. Si B' est un sous-anneau de A', alors $f^{-1}(B')$ est un sous-anneau de A.
3. Si I est un idéal de A', alors $f^{-1}(I)$ est un idéal de A.

2. Image et noyau d'un morphisme

Théorème

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

1. Si B est un sous-anneau de A, alors $f(B)$ est un sous-anneau de A'.
2. Si B' est un sous-anneau de A', alors $f^{-1}(B')$ est un sous-anneau de A.
3. Si I est un idéal de A', alors $f^{-1}(I)$ est un idéal de A.

En particulier,

- $\operatorname{Im} f \overset{\text{déf.}}{=} f(A)$ est un sous-anneau de A'.
- $\operatorname{Ker} f \overset{\text{déf.}}{=} f^{-1}(0)$ est un idéal de A (et ce n'est pas un sous-anneau sauf si A' est l'anneau nul).

3. Anneaux isomorphismes

Définition : anneaux isomorphes

On dit que deux anneaux A et A' sont *isomorphes* s'il existe un isomorphisme d'anneaux de l'un vers l'autre : ces deux anneaux possèdent alors les mêmes propriétés calculatoires.

3. Anneaux isomorphismes

Définition : anneaux isomorphes

On dit que deux anneaux A et A' sont *isomorphes* s'il existe un isomorphisme d'anneaux de l'un vers l'autre : ces deux anneaux possèdent alors les mêmes propriétés calculatoires.

Exemple

$(\mathbb{Z}, +, \times)$ et $(\mathrm{End}(\mathbb{Z}), +, \circ)$ sont isomorphes.

3. Anneaux isomorphismes

Définition : anneaux isomorphes

On dit que deux anneaux A et A' sont *isomorphes* s'il existe un isomorphisme d'anneaux de l'un vers l'autre : ces deux anneaux possèdent alors les mêmes propriétés calculatoires.

Exemple

$(\mathbb{Z}, +, \times)$ et $(\mathrm{End}(\mathbb{Z}), +, \circ)$ sont isomorphes.

Théorème des restes chinois

Si m et n sont deux entiers premiers entre eux, les anneaux $\mathbb{Z}/mn\mathbb{Z}$ et $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ sont isomorphes.

4. Quotient par un idéal

Soit $(A, +, \times)$ un aneau commutatif et I un idéal de A. On définit la relation d'équivalence sur A suivante

$$x\mathcal{R}y \overset{\text{déf.}}{\Longleftrightarrow} y - x \in I.$$

On dit que x *est congru à* y *modulo* I. La relation $\mathcal{R}$ est une congruence à gauche.

4. Quotient par un idéal

Soit $(A, +, \times)$ un aneau commutatif et I un idéal de A. On définit la relation d'équivalence sur A suivante

$$x\mathcal{R}y \overset{\text{déf.}}{\iff} y - x \in I.$$

On dit que x *est congru à* y *modulo* I. La relation $\mathcal{R}$ est une congruence à gauche.
La classe d'équivalence de x modulo I est

$$\bar{x} = \{y \in A : y - x \in I\} = I + x.$$

On note $A/I = \{I + x : x \in A\}$ l'espace quotient et $p_I : A \to A/I$ la surjection canonique ($p_I(x) = I + x$).

Théorème

Il existe une unique structure d'anneau sur A/I telle que $p_I : A \to A/I$ soit un morphisme d'anneaux.

Le noyau de p_I est I.

Théorème

Il existe une unique structure d'anneau sur A/I telle que $p_I : A \to A/I$ soit un morphisme d'anneaux.

Le noyau de p_I est I.

Exemples

Pour $I = A$, A/A est l'anneau trivial $\{A\}$.
Pour $A = \mathbb{Z}$ et $I = n\mathbb{Z}$, A/I est l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$.

Théorème

Il existe une unique structure d'anneau sur A/I telle que $p_I : A \to A/I$ soit un morphisme d'anneaux.

Le noyau de p_I est I.

Exemples

Pour $I = A$, A/A est l'anneau trivial $\{A\}$.
Pour $A = \mathbb{Z}$ et $I = n\mathbb{Z}$, A/I est l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$.

Théorème

Soit $f : A \to B$ un morphisme d'anneaux. Alors $f(A)$ est isomorphe à $A/\operatorname{Ker} f$.

5. Caractéristique d'un anneau

Soit $(A, +, \times)$ un anneau non réduit à $\{0\}$ et $\varphi_A : \mathbb{Z} \to A$ le morphisme d'anneaux défini par

$$\boldsymbol{\varphi_A(n) = n.1_A}$$

où $\quad n.1_A \overset{\text{déf.}}{=} \underbrace{1_A + \cdots + 1_A}_{n \text{ fois}}$ si $n \in \mathbb{N}$,

et $n.1_A = -(|n|.1_A)$ si $-n \in \mathbb{N}$.

φ_A est le seul morphisme d'anneaux de $\mathbb{Z}$ dans A.
Le noyau de φ_A est un idéal de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$, $p \in \mathbb{N}$.

5. Caractéristique d'un anneau

Soit $(A,+,\times)$ un anneau non réduit à $\{0\}$ et $\varphi_A : \mathbb{Z} \to A$ le morphisme d'anneaux défini par

$$\boldsymbol{\varphi_A(n) = n.1_A}$$

où $\quad n.1_A \overset{\text{déf.}}{=} \underbrace{1_A + \cdots + 1_A}_{n \text{ fois}}$ si $n \in \mathbb{N}$,

et $n.1_A = -(|n|.1_A)$ si $-n \in \mathbb{N}$.

φ_A est le seul morphisme d'anneaux de $\mathbb{Z}$ dans A.
Le noyau de φ_A est un idéal de $\mathbb{Z}$, donc de la forme $p\mathbb{Z}$, $p \in \mathbb{N}$.

Définition : caractéristique d'un anneau

L'entier positif (ou nul) p tel que $\operatorname{Ker} \varphi_A = p\mathbb{Z}$ est appelé la *caractéristique* de $(A,+,\times)$.

Autrement dit, la caractéristique de A est le plus petit entier > 0, s'il existe, tel que $p.1_A = 0$; et 0 sinon.
Soit encore, si l'ordre de 1_A (élément neutre pour la loi multiplicative) est fini, la caractéristique de A est l'ordre de 1_A pour la loi additive ; si l'ordre de 1_A est infini, la caractéristique de A est 0.

Exemples

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont de caractéristique 0.
2. Si $p \neq 1$, $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.

Autrement dit, la caractéristique de A est le plus petit entier > 0, s'il existe, tel que $p.1_A = 0$; et 0 sinon.
Soit encore, si l'ordre de 1_A (élément neutre pour la loi multiplicative) est fini, la caractéristique de A est l'ordre de 1_A pour la loi additive ; si l'ordre de 1_A est infini, la caractéristique de A est 0.

Exemples

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont de caractéristique 0.
2. Si $p \neq 1$, $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.

Proposition

Si A est intègre, sa caractéristique est nulle ou un nombre premier.

IV. Corps
1. Structure de corps

Définition : Corps

On appelle *corps* tout anneau $(K, +, \times)$ vérifiant

1. $(K, +, \times)$ est commutatif
2. K n'est pas réduit à $\{0\}$
3. tous les éléments non nuls de K sont des unités.

IV. Corps
1. Structure de corps

Définition : Corps

On appelle *corps* tout anneau $(K, +, \times)$ vérifiant

1. $(K, +, \times)$ est commutatif
2. K n'est pas réduit à $\{0\}$
3. tous les éléments non nuls de K sont des unités.

Les corps usuels sont $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$.
$(\mathbb{Z}, +, \times)$ n'est pas un corps.

IV. Corps
1. Structure de corps

Définition : Corps

On appelle *corps* tout anneau $(K, +, \times)$ vérifiant

1. $(K, +, \times)$ est commutatif
2. K n'est pas réduit à $\{0\}$
3. tous les éléments non nuls de K sont des unités.

Les corps usuels sont $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$.
$(\mathbb{Z}, +, \times)$ n'est pas un corps.

Proposition

❶ Tout corps est intègre, c.–à–d. "sans diviseur de zéro".

IV. Corps
1. Structure de corps

Définition : Corps

On appelle *corps* tout anneau $(K, +, \times)$ vérifiant

1. $(K, +, \times)$ est commutatif
2. K n'est pas réduit à $\{0\}$
3. tous les éléments non nuls de K sont des unités.

Les corps usuels sont $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$.
$(\mathbb{Z}, +, \times)$ n'est pas un corps.

Proposition

❶ Tout corps est intègre, c.–à–d. "sans diviseur de zéro".
❷ Les seuls idéaux d'un corps sont $\{0\}$ et lui-même.

IV. Corps
1. Structure de corps

Définition : Corps

On appelle *corps* tout anneau $(K, +, \times)$ vérifiant

1. $(K, +, \times)$ est commutatif
2. K n'est pas réduit à $\{0\}$
3. tous les éléments non nuls de K sont des unités.

Les corps usuels sont $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$.
$(\mathbb{Z}, +, \times)$ n'est pas un corps.

Proposition

1. Tout corps est intègre, c.–à–d. "sans diviseur de zéro".
2. Les seuls idéaux d'un corps sont $\{0\}$ et lui-même.
3. $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.

2. Sous-corps

Définition : Sous-corps

On appelle *sous-corps* d'un corps $(K, +, \times)$ toute partie L de K vérifiant

1. L est un sous-anneau de $(K, +, \times)$
2. pour tout $x \in L \backslash \{0\}$, $x^{-1} \in L$.

2. Sous-corps

Définition : Sous-corps

On appelle *sous-corps* d'un corps $(K, +, \times)$ toute partie L de K vérifiant

1. L est un sous-anneau de $(K, +, \times)$
2. pour tout $x \in L \backslash \{0\}$, $x^{-1} \in L$.

Exemple

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

2. Sous-corps

Définition : Sous-corps

On appelle *sous-corps* d'un corps $(K, +, \times)$ toute partie L de K vérifiant

1. L est un sous-anneau de $(K, +, \times)$
2. pour tout $x \in L\backslash\{0\}$, $x^{-1} \in L$.

Exemple

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

Théorème

Si L est un sous-corps de $(K, +, \times)$, alors $(L, +, \times)$ est un corps.