

ANNEAUX

B. Landelle

Table des matières

I	Structure d'anneau	2
1	Définitions, propriétés	2
2	Groupe des inversibles	3
3	Anneau produit	3
4	Corps, sous-corps	4
II	Morphisme d'anneaux	4
1	Définition, propriétés	4
2	Noyau et image	5
3	Isomorphisme d'anneaux	6
III	Idéaux d'un anneau commutatif	6
1	Définitions, propriétés	6
2	Idéal engendré	7
3	Divisibilité dans un anneau commutatif intègre	8

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 $(A, +, \times)$ avec A un ensemble (non vide) muni de deux lois de compositions internes $+$ et $\times$ telles que :

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

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

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

Remarques : (1) Soit $x \in A$. On a $0_A x = 0_A$ (en écrivant $0_A + 0_A = 0_A$) et $(-1_A)x = -x$ (en écrivant $1_A - 1_A = 0_A$).

(2) L'anneau nul $\{0_A\}$ est le seul pour lequel $0_A = 1_A$. On le rencontre par exemple avec $(\mathcal{L}(E), +, \circ)$ et $E = \{0_E\}$.

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

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

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

Démonstration. Par récurrence pour k entier puis prolongement si k est entier négatif. $\square$

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

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

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

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

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

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

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

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

1. $1_A \in B$;
2. $\forall (x, y) \in B^2 \quad x - y \in B$;
3. $\forall (x, y) \in B^2 \quad xy \in B$.

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

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

2 Groupe des inversibles

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

$$xy = yx = 1_A$$

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

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

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

3 Anneau produit

Définition 5. Soient $(A_1, +, \times), \dots, (A_n, +, \times)$ des anneaux et $A = \prod_{i=1}^n A_i$. On définit les lois produits $+$ et $\times$ sur A par

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

Théorème 1. Soient $(A_1, +, \times), \dots, (A_n, +, \times)$ des anneaux et $A = \prod_{i=1}^n A_i$. L'ensemble A muni des lois produits $+$ et $\times$ est un anneau dont les neutres sont respectivement $0_A = (0_{A_1}, \dots, 0_{A_n})$ et $1_A = (1_{A_1}, \dots, 1_{A_n})$. Si les $(A_i, +, \times)$ sont des anneaux commutatifs, alors l'anneau produit l'est aussi.

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

Théorème 2. Soient $(A_1, +, \times), \dots, (A_n, +, \times)$ des anneaux et $A = \prod_{i=1}^n A_i$ muni des lois produits. On a pour $x = (x_1, \dots, x_n) \in A$

$$x \in U(A) \iff \forall i \in \llbracket 1; n \rrbracket \quad x_i \in U(A_i)$$

et dans ce cas

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

Enfin, on a

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

Démonstration. Immédiate. $\square$

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

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 $\mathbb{K}^* = U(\mathbb{K})$.

Exemples : $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(\mathbb{K}(X), +, \times)$ sont des corps.

Soit $(A, +, \times)$ sous-anneau d'un corps $(\mathbb{K}, +, \times)$. On définit le corps des fractions de A par

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

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

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

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 $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}, (a, b) \in \mathbb{Q}^2\}$. L'ensemble $(\mathbb{Q}[\sqrt{2}], +, \times)$ est un corps.

II Morphisme d'anneaux

1 Définition, propriétés

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

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

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 $(A, +)$ vers le groupe $(A', +)$.

Exemples : 1. L'identité $\text{id} : A \rightarrow A$, l'application $\varphi : \mathbb{Z} \rightarrow A$, $k \mapsto k1_A$.

2. Pour $a \in U(A)$, l'application $\varphi_a : A \rightarrow A$, $x \mapsto axa^{-1}$.

3. L'application $\varphi : \mathbb{C} \rightarrow \mathcal{M}_2(\mathbb{R})$, $a + ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ (utiliser l'écriture trigonométrique).

4. L'application $\varphi : \mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{Z}[\sqrt{2}]$, $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ (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 φ un morphisme de l'anneau $(A, +, \times)$ vers l'anneau $(A', +, \times)$. On a :*

$$1. \forall (x, k) \in A \times \mathbb{Z} \quad \varphi(kx) = k\varphi(x)$$

$$2. \forall (x, n) \in A \times \mathbb{N} \quad \varphi(x^n) = \varphi(x)^n$$

$$3. \forall x \in A \quad x \in U(A) \implies \varphi(x) \in U(A') \quad \text{et} \quad \varphi(x)^{-1} = \varphi(x^{-1})$$

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

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

2 Noyau et image

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

Remarque : Ces notions coïncident avec celles du morphisme φ du groupe $(A, +)$ vers le groupe $(A', +)$.

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

Démonstration. Immédiate. □

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

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

$$\varphi \text{ injective} \iff \text{Ker } \varphi = \{0_A\}$$

Démonstration. L'application est un morphisme de groupes de $(A, +)$ vers $(A', +)$. 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 $(A, +, \times) \simeq (A', +, \times)$ ou plus simplement $A \simeq A'$ 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 $(A, +, \times)$ un isomorphisme de $(A, +, \times)$ dans lui-même.

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

III Idéaux d'un anneau commutatif

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

1 Définitions, propriétés

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

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

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

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

2 Idéal engendré

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

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

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

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

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

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

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

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

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

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

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 . $\square$

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

3 Divisibilité dans un anneau commutatif intègre

Dans cette partie, le triplet $(A, +, \times)$ 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 $c \in A$ tel que $b = ac$. On note $a|b$.

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

$$a|b \iff b \in aA \iff bA \subset aA$$

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

$$a|b \text{ et } b|c \implies a|c$$

$$a|b \text{ et } a|c \implies a|b+c$$

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

$$ab = ac \text{ et } a \neq 0 \implies b = c$$

$$ab|ac \text{ et } a \neq 0 \implies b|c$$

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

$$a, b \text{ associés} \iff aA = bA \iff \exists c \in U(A) \mid b = ac$$

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

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