Anneaux et Corps

Frank Wagner

Table des matières

Chapitre 1

Anneaux

1.1 Anneaux, sous-anneaux et idéaux

Définition 1.1. Un *anneau* est une structure de domaine un ensemble A avec une constante 0 et deux lois binaires $+$ et $\times$ satisfaisant

- $(A, 0, +)$ est un groupe abélien.
- $(A, \times)$ est un semi-groupe, c'est-à-dire $\times$ est associatif : $(a \times b) \times c = a \times (b \times c)$ pour tout $a, b, c \in A$.
- On a les lois distributives : Pour tout $a, b, c \in A$ on a

$$a \times (b + c) = a \times b + a \times c \qquad \text{et} \qquad (b + c) \times a = b \times a + c \times a.$$

Si A possède un élément 1 tel que $a \times 1 = 1 \times a = a$ pour tout $a \in A$, alors $(A, 0, 1, +, \times)$ est un anneau *unitaire*, ou *unifère*.
Si $\times$ est commutatif, alors A est un *anneau commutatif*.

Pour une notation plus compacte, on supprime généralement la multiplication $\times$, et la multiplication est prioritaire sur l'addition.

Remarque 1.2. Dans un anneau unitaire l'addition est automatiquement commutative : On a

$$a+b+a+b = (a+b)\times 1+(a+b)\times 1 = (a+b)\times(1+1) = a\times(1+1)+b\times(1+1) = a+a+b+b,$$

ce qui implique $b + a = a + b$.

Remarque 1.3. Dans un anneau on a $0 \times a = a \times 0 = 0$ pour tout $a \in A$. En fait,

$$a \times 0 = a \times (0 + 0) = a \times 0 + a \times 0,$$

d'où $a \times 0 = 0$. L'égalité $0 \times a = 0$ se montre de manière analogue.

Exemple 1.4.
- Les corps rationnels $\mathbb{Q}$, réels $\mathbb{R}$ et complexes $\mathbb{C}$.
- Les anneaux de polynômes sur ces corps $\mathbb{Q}[X]$, $\mathbb{R}[X]$ et $\mathbb{C}[X]$.

— Les entiers relatifs $\mathbb{Z}$, ou l'anneau des polynômes avec coefficients entiers $\mathbb{Z}[X]$.
— Les entiers relatifs multiples de k, pour un entier $k > 1$, noté $k\mathbb{Z}$.
— L'anneau des matrices carrées sur un corps $\mathcal{M}_n(\mathbb{Q})$, $\mathcal{M}_n(\mathbb{R})$ et $\mathcal{M}_n(\mathbb{C})$.
— L'anneau des matrices carrées sur les entiers relatifs $\mathcal{M}_n(\mathbb{Z})$.
— L'anneau des matrices carrées sur $k\mathbb{Z}$, soit $\mathcal{M}_n(k\mathbb{Z})$, pour des entiers $n, k > 1$.

Ils sont tous unitaires sauf les $k\mathbb{Z}$ et $\mathcal{M}_n(k\mathbb{Z})$ (pour $k > 1$), et commutatifs sauf les $\mathcal{M}_n$ (pour $n > 1$).

Définition 1.5. Un anneau est *nul* si $ab = 0$ pour tout $a, b \in A$.

Ainsi tout groupe abélien peut être considéré comme groupe additif d'un anneau nul.

Exemple 1.6. Si A est un anneau, l'ensemble $A[X]$ des polynômes avec coefficients dans A est encore un anneau ; si A est commutatif et/ou unitaire, $A[X]$ l'est aussi.

Démonstration. Si $P = \sum_i a_i X^i$ et $Q = \sum_i b_i X^i$ (ou presque tous les coefficients sont 0) sont deux polynômes dans $A[X]$, on pose $P + Q = \sum_i (a_i + b_i) X^i$ et $PQ = \sum_i c_i X^i$, avec $c_i = \sum_{k=0}^{i} a_k b_{i-k}$ (et on note que presque tous les c_i sont 0). On vérifié comme pour les polynômes avec coefficients réels que c'est un anneau dont le zéro est celui de A. Si A est unitaire, alors l'unité 1 de A est aussi unité pour $A[X]$; si A est commutatif, on voit facilement que $A[X]$ est commutatif. □

Exemple 1.7. L'anneau des *entiers de Gauss* est l'anneau $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Z}\}$.

Définition 1.8. Une partie non-vide $B \subseteq A$ est un *sous-anneau* si B est un sous-groupe additif, et clos par multiplication. C'est-à-dire, si $a, b \in B$ alors $a - b \in B$ et $ab \in B$. On note $B \leq A$.
Un sous-anneau $B \leq A$ est un *idéal à gauche* si $ab \in B$ pour tout $a \in A$ et $b \in B$. C'est un *idéal à droite* si $ba \in B$ pour tout $a \in A$ et $b \in B$, et un idéal (bilatère) si c'est à la fois un idéal à gauche et à droite. On le note $I \trianglelefteq A$.

Définition 1.9. Soient A et B deux anneaux. L'*anneau produit* $A \times B$ est l'anneau dont le groupe additif est la somme directe $A \oplus B$ des groupes additifs de A et de B, c'est-à-dire avec zéro $(0, 0)$ et addition $(a, b) + (a', b') = (a + a', b + b')$, et dont la multiplication est donnée par $(a, b)\,(a', b') = (aa', bb')$.

Définition 1.10. Soit A un anneau et $X \subseteq A$ une partie. L'anneau engendré par X est le plus petit sous-anneau de A contenant X ; il est noté $\langle X \rangle$. L'idéal engendré par X est le plus petit idéal de A contenant X ; il est noté (X).

Soient X et Y deux parties de A.
— On pose $XY = \{xy : x \in X,\, y \in Y\}$, l'ensemble des produit d'un élément de X avec un élément d'Y.
— On définit récursivement $X^1 = X$, et $X^{n+1} = XX^n$.
— $\langle X \rangle_+$ est le sous-groupe additif engendré par X.

Proposition 1.11. *On a* $\langle X \rangle = \langle X^n : n \in \mathbb{N}^* \rangle_+$ *et* $(X) = \langle X, AX, XA, AXA \rangle_+$.

Démonstration. Ce sont des sous-groupes additifs par définition. Par associativité et distributivité, $\langle X^n : n \in \mathbb{N}^* \rangle_+$ est clos par produit, et $\langle X, AX, XA, AXA \rangle_+$ est clos par multiplication à gauche et à droite par des éléments de A (et donc est clos par produit). Ainsi $\langle X^n : n \in \mathbb{N}^* \rangle_+$ est un sous-anneau et $\langle X, AX, XA, AXA \rangle_+$ est un idéal. Les deux contiennent X, et tous leurs éléments sont dans tous les sous-anneaux/idéaux qui contiennent X, d'où les égalités. □

Remarque 1.12. Si A est commutatif et unitaire, cela se simplifie en $(X) = \langle AX \rangle_+$.

Exemple 1.13. On va étudier les petits anneau de cardinalité n.

1. Le seul anneau de cardinal 1 est l'anneau trivial $\{0\}$.
2. Soit $A = \{0, a\}$ un anneau de cardinal 2. Alors le groupe additif est isomorphe à $\mathbb{Z}/2\mathbb{Z}$, donc $a + a = 0$. Pour le groupe multiplicatif, il y a deux options : Soit $a^2 = 0$ et A est nul, soit $a^2 = 1$ et $A \cong \mathbb{Z}/2\mathbb{Z}$ en tant qu'anneau.
3. Soit A un anneau de cardinal 3. Son groupe additif est isomorphe à $\mathbb{Z}/3\mathbb{Z}$, le seul groupe de cardinal 3. Si A est unitaire, on a $A = \{0, 1, a\}$ avec $1 + 1 = a$, d'où $a^2 = (1 + 1)(1 + 1) = 1 + 1 + 1 + 1 = 1$.

Exercice 1.14. Classifier tous les anneaux de cardinal 3.

Exercice 1.15. Classifier tous les anneaux commutatifs unitaires de cardinal 4.

1.2 Morphismes et anneau quotient

Définition 1.16. Soit A un anneau et $I \trianglelefteq A$ un idéal (bilatère). Le quotient A/I est l'anneau dont le groupe additif est le groupe quotient A/I, avec multiplication $(a + I)(b + I) = (ab + I)$. Si A est commutatif et/ou unitaire, A/I aussi.

Démonstration. Il faut montrer que la multiplication est bien définie. On considère donc $a, a', b, b' \in A$ avec $a + I = a' + I$ et $b + I = b' + I$. Alors $a - a' \in I$ et $b - b' \in I$, ce qui donne

$$ab - a'b' = a(b - b') + ab' - a'b' = a(b - b') + (a - a')b' \in aI + Ib' \subseteq I.$$

Ainsi $ab + I = a'b' + I$ et la multiplication ne dépend pas du choix de représentant. L'associativité en découle, puisque

$$\big((a+I)(b+I)\big)(c+I) = (ab+I)(c+I) = abc+I = (a+I)(bc+I) = (a+I)\big((b+I)(c+I)\big).$$

Il est clair que la commutativité de A implique celle de A/I, et si $1 \in A$ est unité, alors $1 + I$ est unité dans A/I. □

Définition 1.17. Soient A et B deux anneaux. Un homomorphisme de groupes additifs $f : A \to B$ est un *morphisme d'anneau* si $f(aa') = f(a)\,f(a')$ pour tout $a, a' \in A$.
Si f est bijectif, alors f est un isomorphisme (d'anneaux). Si de plus $A = B$, alors f est un automorphisme (d'anneaux).

Remarque 1.18. Il est clair que l'image $\mathrm{im} f$ est un sous-anneau de B.

Exemple 1.19. Les applications suivantes sont des morphismes d'anneau.

1. Si A est commutatif et $a \in A$, l'application
$$f_a : A[X] \to A, \qquad P \mapsto P(a).$$
2. Si A et B sont deux anneaux, l'application
$$\pi : A \times B \to A, \qquad (a, b) \mapsto a.$$
3. Si A et B sont deux anneaux, l'application
$$\iota : A \to A \times B, \qquad a \mapsto (a, 0).$$
Cependant, si A et B sont unitaires, $A \times B$ l'est aussi avec unité $(1, 1)$, mais $f(1) = (1, 0) \neq (1, 1)$.

L'application $\mathbb{R} \times \mathbb{R} \to \mathbb{C}$ donné par $(x, y) \mapsto x + iy$ ne préserve pas la multiplication. Ce n'est donc pas un morphisme d'anneau.

Définition 1.20. Soit $f : A \to B$ un morphisme d'anneau. Son noyau est $\ker f = \{a \in A : f(a) = 0\}$, c'est-à-dire son noyau en tant que homomorphisme additif.

Proposition 1.21. *Soit $f : A \to B$ un morphisme d'anneau. Alors* $\ker f$ *est un idéal dans A, et* $\mathrm{im} f \cong A/\ker f$.

Démonstration. C'est un sous-groupe additif. Si $a \in \ker f$ ou $a' \in \ker f$, alors $f(a) = 0$ ou $f(b) = 0$, d'où $f(ab) = f(a)f(b) = 0$. Ainsi $\ker f$ est clos par multiplication à gauche et à droit par des éléments de A, et en particulier clos par multiplication. Ainsi $\ker f$ est un idéal.
L'application $a + \ker f \mapsto f(a)$ est une bijection de groupes additifs entre $A/\ker f$ et $\mathrm{im} f$. Elle préserve la multiplication. C'est donc un isomorphisme d'anneaux. □

Remarque 1.22. Si A est unitaire, alors $\mathrm{im} f$ est un sous-anneau unitaire de B, mais son unité $f(1_A)$ n'est pas forcément unité de B.

1.2.1 Inversibilité, divisibilité, anneaux intègres

Définition 1.23. Soit A un anneau. Un élément $0 \neq a \in A$ est un *diviseur de zéro à gauche* s'il y a $0 \neq b \in A$ avec $ab = 0$. Dans ce cas, b est un *diviseur de zéro à droite.*
Un anneau commutatif sans diviseur de zéro est un anneau *intègre.* Attention : Parfois on demande en plus que l'anneau soit unitaire !
Si A est unitaire, un élément $a \in A$ est *inversible* s'il y a $b \in A$ avec $ab = ba = 1$.
L'ensemble des éléments inversibles est noté $A^\times$.
Un anneau commutatif dont tous les éléments non-nuls sont inversibles est un *corps.*
Donc $A^\times = A \setminus \{0\}$ est un groupe abélien multiplicatif.

Remarque 1.24. $A^\times$ forme un sous-groupe multiplicatif de A.

Lemme 1.25. *1. Un élément inversible n'est pas diviseur de zéro.*

2. Si a n'est pas diviseur de zéro à gauche et $ab = ac$, alors $b = c$ (et similairement à droite).

Démonstration. 1. Si $ab = 0$ et a est inversible, alors $b = a^{-1}ab = a^{-1}0 = 0$. Le raisonnement de l'autre coté est analogue.

2. Si $ab = ac$ alors $a(b - c) = 0$. Comme a n'est pas diviseur de zéro à gauche, $b - c = 0$ et $b = c$. □

Exemple 1.26. Soit $n \in \mathbb{N}$. Alors $n\mathbb{Z}$ est un idéal dans $\mathbb{Z}$, et $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif unitaire. Si $n = 0$ on a $n\mathbb{Z} = \{0\}$ et $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}$. Si $n = 1$ on a $n\mathbb{Z} = \mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \cong \{0\}$, l'anneau trivial. On supposera donc $n \geq 2$.

Lemme 1.27. *$\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier, pour $n \geq 2$.*

Démonstration. Supposons d'abord $n = k\ell$ composé, avec $1 < k, \ell < n$. Alors $k + n\mathbb{Z} \neq 0 + n\mathbb{Z}$, et $\ell + n\mathbb{Z} \neq 0 + n\mathbb{Z}$, mais

$$(k + n\mathbb{Z})(\ell + n\mathbb{Z}) = kl + n\mathbb{Z} = n + n\mathbb{Z} = 0 + n\mathbb{Z}.$$

Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.
Réciproquement, supposons n premier. Alors pour tout $k \in \mathbb{Z}$ soit n divise k et $k + n\mathbb{Z} = 0 + n\mathbb{Z}$, soit k et n sont premiers entre eux. Dans ce cas, d'après le théorème de Bézout il y a des entiers relatifs $s, t \in \mathbb{Z}$ tels que $sk + tn = \text{pgcd}(k, n) = 1$. Alors

$$(s + n\mathbb{Z})(k + n\mathbb{Z}) = (sk + n\mathbb{Z}) = 1 - kn + n\mathbb{Z} = 1 + n\mathbb{Z}.$$

Ainsi tout $k + \mathbb{Z}$ non-nul est inversible, et $\mathbb{Z}/n\mathbb{Z}$ est un corps. □

C'est un cas particulier d'un théorème plus général.

Proposition 1.28. *Un anneau intègre fini est un corps.*

En fait, le Théorème de Wedderburn asserte qu'on a pas besoin de supposer la commutativité : Tout anneau fini sans diviseur de zéro est un corps.

Démonstration. Soit $0 \neq a \in A$. Alors l'application $\lambda_a : x \mapsto ax$ est injective : Si $ax = ax'$, alors d'après lemme 1.25.2 on a $x = x'$. Or, A est fini, et toute application $A \to A$ injective est surjective. Par surjectivité de λ_a il y a un élément $e \in A$ avec $ae = a$. Si $b \in A$ est quelconque, alors $ab = aeb$, d'où $b = eb$ encore par lemme 1.25.2. Ainsi e est une unité multiplicative.
Encore par surjectivité de λ_a il y a $a' \in A$ avec $aa' = e$. Donc a possède un inverse multiplicatif $a^{-1} = a'$, et A est un corps. □

Définition 1.29. Soit A un anneau intègre unitaire.
- Soient $a, b \in A$. On dit que a *divise* b, noté $a \mid b$, s'il y a $c \in A$ avec $ac = b$.
- Un élément a est *irréductible* si pour tous $b, c \in A$, si $a = bc$ alors b ou c est inversible.
- Un élément $a \in A$ est premier si pour tous $b, c \in A$, si $p \mid bc$ alors $p \mid b$ ou $p \mid c$.

Ceci généralise les notions bien connues de $\mathbb{Z}$ et $\mathbb{R}[X]$.

Exemple 1.30. Soit $A = \mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} : a, b \in \mathbb{Z}\}$, un sous-anneau de $\mathbb{C}$. On a

$$6 = 2 \times 3 = (1 + i\sqrt{5})\,(1 - i\sqrt{5}).$$

Pour tout $a \in A$ on a $|a|^2 \in \mathbb{N}$. On en déduit que $|a| = 1$ pour tout $a \in A$ inversible, et que 2, 3, $1 + i\sqrt{5}$ et $1 - i\sqrt{5}$ sont irréductibles. Il n'y a donc pas factorisation unique en irréductibles dans A.

Proposition 1.31. *Soit A un anneau intègre unitaire. Alors tout élément premier est irréductible.*

Démonstration. Soit $a \in A$ premier, et $b, c \in A$ avec $a = bc$. Puisque A est unitaire, $a \mid bc$; comme a est premier, on a $a \mid b$ ou $a \mid c$. Par symétrie on peut supposer $a \mid b$, et il y a $d \in A$ avec $ad = b$. Donc $bcd = ad = b$ et $cd = 1$ d'après le lemme 1.25. Ainsi c est inversible. Ceci montre que a est irréductible. □

Remarque 1.32. La réciproque est fausse : Dans l'exemple 1.30 on a que 2 est irréductible et divise $6 = (1 + i\sqrt{5})\,(1 - i\sqrt{5})$, mais ne divise aucun des deux facteurs.