Anneaux et Corps

Frank Wagner

Table des matières

Chapitre 1

Anneaux

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. On note $A^* = A \setminus \{0\}$.

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. □

Convention. A partir de maintenant, tous les anneaux seront commutatifs (sauf mention au contraire).

Définition 1.7. 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 le note $B \leq A$.
Un sous-anneau $B \leq A$ est un *idéal* si $ab \in B$ pour tout $a \in A$ et $b \in B$. On le note $I \trianglelefteq A$.

Remarque 1.8. Si A n'est pas commutatif, pour qu'un sous-anneau B soit un idéal, il faut aussi demander $ba \in B$ pour tout $a \in A$ et $b \in B$.

Exemple 1.9. L'anneau des *entiers de Gauss* est l'anneau $\mathbb{Z}[i] = \{a + ib \in \mathbb{C} : a, b \in \mathbb{Z}\}$. C'est un sous-anneau de $\mathbb{C}$.

Exemple 1.10. Si A est un anneau (commutatif), l'ensemble $X \cdot A[X]$ des polynômes non-constants ou 0 forme un idéal.

Définition 1.11. 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 1.12. Soit A un anneau et $X \subseteq A$ une partie. L'anneau engendré par X est le plus petit sous-anneaux de A qui contient X ; il est noté $\langle X \rangle$. L'idéal engendré par X est le plus petit idéal de A qui contient X ; il est noté (X).

Si $X = \{x_0, \dots, x_n\}$ est fini, on note $\langle X \rangle = \langle x_0, \dots, x_n \rangle$ et $(X) = (x_0, \dots, x_n)$.
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 1.13. *On a $\langle X \rangle = \langle X^n : n \in \mathbb{N}^* \rangle_+$ et $(X) = \langle X, AX \rangle_+$; si $a \in A$ alors $(a) = Aa + \mathbb{Z}a$. Si A est unitaire, $(X) = \langle AX \rangle_+$, et pour $a \in A$ on a $(a) = Aa$.*

Démonstration. Ce sont des sous-groupes additifs par définition, et par distributivité pour $Aa + \mathbb{Z}a$ et Aa. Par associativité et distributivité, $\langle X^n : n \in \mathbb{N}^* \rangle_+$ est clos par produit, et $\langle X, AX \rangle_+$ ainsi que $Aa + \mathbb{Z}a$ sont clos par multiplication par des éléments de A (et donc clos par produit). Ainsi $\langle X^n : n \in \mathbb{N}^* \rangle_+$ est un sous-anneau et $\langle X, AX \rangle_+$ et $Aa + \mathbb{Z}a$ sont des un idéaux. Les deux contiennent X, et tous leurs éléments sont dans tous les sous-anneaux/idéaux qui contiennent X ; si A est unitaire, $X \subseteq AX$ et $\mathbb{Z}a \leq Aa$. □

Exemple 1.14. 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 1.15. Classifier tous les anneaux de cardinal 3.

Exercice 1.16. Classifier tous les anneaux commutatifs unitaires de cardinal 4.

2 Morphismes et anneau quotient

Définition 2.1. Soit A un anneau et $I \trianglelefteq A$ un idéal. Le quotient A/I est l'anneau dont le groupe additif est le groupe quotient A/I, avec multiplication $(a+I)(b+I) = (ab+I)$.

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

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

Remarque 2.2. Si A est commutatif et/ou unitaire, A/I aussi. Si $1 \in A$ est l'unité, $1 + I$ est l'unité de A/I.

Définition 2.3. 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).
Si A et B sont unitaires, f est un homomorphisme (d'anneaux) unitaire(s)s si en plus $f(1_A) = 1_B$.

Remarque 2.4. Il est clair que l'image $\mathrm{im} f$ est un sous-anneau de B.

Exemple 2.5. 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 $f(1) = (1, 0) \neq (1, 1)$. Ainsi f n'est pas un homomorphisme unitaire.

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 2.6. 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 2.7. *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. $\square$

Remarque 2.8. 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.

Théorème 2.9. *Soient A et B deux anneaux, $f : A \to B$ un morphisme d'anneaux, et $I \trianglelefteq A$ un idéal de A. Soit $\pi : A \to A/I$ la projection canonique. Alors il y a un morphisme $g : A/I \to B$ tel que $f = g \circ \pi$ si et seulement si $I \leq \ker f$.*

Démonstration. S'il y a $g : A/I \to B$ avec $f = g \circ \pi$ et $a \in I$, alors $\pi(a) = 0_I$, et $g(0_I) = 0_B$. Donc $f(a) = (g \circ \pi)(a) = 0_B$ et $a \in \ker f$. Ainsi $I \leq \ker f$.
Réciproquement, soit $I \leq \ker f$. Pour $a + I \in A/I$ on pose $g(a + I) = f(a) \in B$. On vérifie que g est bien défini : Si $a' \in A$ avec $a + I = a' + I$, alors $a - a' \in I \leq \ker f$, et

$$f(a) = f(a - a' + a') = f(a - a') + f(a') = 0 + f(a') = f(a').$$

Donc $g : A/I \to B$ est bien défini, et pour tout $a \in A$ on a bien $(g \circ \pi)(a) = g(a + I) = f(a)$, d'où $f = g \circ \pi$. □

Proposition 2.10. *Soit $I \trianglelefteq A$. Alors $\pi : a \mapsto a + I$ induit une bijection entre les idéaux de A qui contiennent I et les idéaux de A/I.*

Démonstration. Soit $I \leq J \trianglelefteq A$. Alors $f[J] = J/I$ est un sous-groupe additif de A qui est clos par multiplication par des éléments de A/I, puisque $(a + I)J = aJ = J$. Donc $\pi[J]$ est un idéal de A/I.
Réciproquement, si $\bar{J}$ est un idéal de A/I, soit $J = \pi^{-1}[\bar{J}]$ son image réciproque. C'est un groupe additif, et pour tout $a \in A$ on a $\pi[aJ] = \pi(a)\pi[J] = \pi(a)\bar{J} = \bar{J}$, d'où $aJ \leq J$. Ainsi J est un idéal de A.
Enfin, π induit une bijection entre les sous-groupes additifs de A qui contiennent I et les sous-groupes additifs de A/I, qui se restreint en une bijection entre ceux qui sont des idéaux. □

3 Ideaux

Soit X un ensemble. Une famille $(Y_i : i \in I)$ de parties de X est une *chaîne* si pour tout $i, j \in I$ on a $Y_i \subseteq Y_j$ ou $Y_j \subseteq Y_i$.

Proposition 3.1. *Soit A un anneau, et $\{B_i : i \in I\}$ une famille non-vide de sous-anneaux de A.*

1. *L'intersection $\bigcap_{i \in I} B_i$ est un sous-anneau de A.*
2. *Si tous les B_i sont des idéaux, alors $\bigcap_{i \in I} B_i$ est un idéal.*
3. *Si les $\{B_i : i \in I\}$ forment une chaîne, la réunion $\bigcup_{i \in I} B_i$ est un sous-anneau de A.*
4. *Si les $\{B_i : i \in I\}$ forment une chaîne d'idéaux, la réunion $\bigcup_{i \in I} B_i$ est un idéal.*

Démonstration. 1. On a $0 \in B_i$ pour tout $i \in I$, d'où $0 \in \bigcap_{i\in I} B_i$. Si $b, b' \in \bigcap_{i\in I} B_i$, alors $b, b' \in B_i$ pour tout $i \in I$; puisque les B_i sont des sous-anneaux, on a $b - b', bb' \in B_i$ pour tout $i \in I$, et $b - b', bb' \in \bigcap_{i\in I} B_i$. Ainsi $\bigcap_{i\in I} B_i$ est un sous-anneau.

2. Si les B_i sont des idéaux, alors pour tout $b \in \bigcap_{i\in I} B_i$ et $a \in A$ on a $b \in B_i$ pour tout $i \in I$, d'où $ab \in B_i$, et $ab \in \bigcap_{i\in I} B_i$. Ainsi $\bigcap_{i\in I} B_i$ est un idéal.
3. Puisque la chaîne n'est pas vide, $\bigcup_{i\in I} B_i \neq \emptyset$. Si $b, b' \in \bigcup_{i\in I} B_i$, alors il y a $i, j \in I$ avec $b \in B_i$ et $b' \in B_j$. On peut supposer que $B_i \subseteq B_j$. Alors $b, b' \in B_j$, et donc $b - b', bb' \in B_j \subseteq \bigcup_{i\in I} B_i$. Ainsi $\bigcup_{i\in I} B_i$ est un sous-anneau.
4. Si de plus tous les B_i sont des idéaux, alors pour tout $b \in \bigcup_{i\in I} B_i$ et $a \in A$ il y a $i \in I$ avec $b \in B_i$, d'où $ab \in B_i$ et $ab \in \bigcup_{i\in I} B_i$. Ainsi $\bigcup_{i\in I} B_i$ est un idéal. □

En particulier l'intersection de deux idéaux est un idéal.

Définition 3.2. Soit A un anneau, et I et J deux idéaux.

1. La *somme* de I et J est l'idéal $I + J = \{a + b : a \in I,\ b \in J\}$.
2. Le *produit* de I et J est l'idéal $IJ = \langle ab : a \in I,\, b \in J\rangle_+$.

On note que $I + J = (I, J)$ est le plus petit idéal contenant I et J.

Remarque 3.3. Pour deux *ensembles* $X, Y \subseteq A$ on avait défini XY comme l'*ensemble* $\{xy : x \in X,\, y \in Y\}$. Pour deux *idéaux* $I, J \trianglelefteq A$ on prend l'*idéal* engendré.

Exemple 3.4. Si $A = \mathbb{Z}$ et $n \in \mathbb{N}$, alors $(n) = n\mathbb{Z}$. Si $m \in \mathbb{N}$ on a

$$\begin{aligned}(m, n) &= (m) + (n) = m\mathbb{Z} + n\mathbb{Z} = (m \wedge n)\mathbb{Z},\\ (m)\,(n) &= m\mathbb{Z}\, n\mathbb{Z} = mn\mathbb{Z},\ \text{et}\\ (m) \cap (n) &= (m \vee n)\mathbb{Z}.\end{aligned}$$

Définition 3.5. Soit A un anneau. Deux idéaux I et J sont *étrangers* (ou *premiers entre eux*) si $I + J = A$.

Proposition 3.6. *Soit A un anneau unitaire, et I, J deux idéaux étrangers. Alors $IJ = I \cap J$.*

Démonstration. Puisque I et J sont des idéaux, on a $IJ \leq I$ et $IJ \leq J$, d'où $IJ \leq I \cap J$. Réciproquement, puisque $A = I + J$ il y a $i \in I$ et $j \in J$ avec $i + j = 1$. Soit $a \in I \cap J$. Alors $a = (i + j)a = ia + ja \in IJ$, d'où $I \cap J \leq IJ$ et on a égalité. □

Théorème 3.7 (Théorème des restes chinois)**.** *Soit A un anneau unitaire, et $I_1, \ldots, I_n$ des idéaux deux-à-deux étrangers. Alors le morphisme d'anneaux*

$$\begin{aligned}\varphi : A/(I_1 \cap \cdots \cap I_n) &\to A/I_1 \times \cdots A/I_n\\ x + (I_1 \cap \cdots \cap I_n) &\mapsto (x + I_1, \ldots, x + I_n)\end{aligned}$$

est un isomorphisme.

Démonstration. Par récurrence sur n, le cas $n = 1$ étant trivial. On suppose donc que $I_1, \dots, I_n, J$ sont deux-à-deux étrangers, et que $x + I \mapsto (x + I_1, \dots, x + I_n)$ est un isomorphisme, où $I = I_1 \cap \cdots \cap I_n$. Puisque J est étranger à chaque I_k, il y a $i_k \in I_k$ et $j_k \in J$ avec $i_k + j_k = 1$. Alors $1 = \prod_{k=1}^{n}(i_k + j_k) \in i_1 i_2 \cdots i_n + J \subseteq I + J$. Donc I et J sont étrangers. On considère donc

$$A/(I_1 \cap \cdots \cap I_n \cap J) = A/(I \cap J) \to A/I \times A/J \to A/I_1 \times \cdots \times A/I_n \times A/J\,;$$

d'après l'hypothèse de récurrence il suffit de montrer que $\varphi : A/(I \cap J) \to A/I \times A/J$ est un isomorphisme. On est donc réduit au cas $n = 2$.
Il est clair que le morphisme est injectif. On considère $(x + I, y + J) \in A/I \times A/J$. Soient $i \in I$ et $j \in J$ tels que $i + j = 1$. On pose $z = iy + jx$. Alors

$$\begin{aligned} z + I &= iy + jx + I = ix + jx + I = (i + j)x + I = x + I, \quad \text{et} \\ z + J &= iy + jx + J = iy + jy + J = (i + j)y + J = y + J. \end{aligned}$$

Ceci montre la surjectivité. □

On note que si $z_0 \in A$ est une solution particulière du système de congruences $z \in a_k + I_k$ pour $k = 1, \dots, n$, alors l'ensemble des solutions est précisément $z_0 + (I_1 \cap \cdots \cap I_n)$.

Exemple 3.8. Soient $n_1, \dots, n_k \in \mathbb{Z}$ deux-à-deux premiers entre eux. Alors pour tout $a_1, \dots, a_k \in \mathbb{Z}$ il y a $x \in \mathbb{Z}$ tel que $x \equiv a_i \mod n_i$ pour $i = 1, \dots, k$.

Démonstration. Si n_i et n_j sont premiers entre eux, d'après la relation de Bézout il y a $u, v \in \mathbb{Z}$ avec $n_i u + n_j v = 1$. Donc $(n_i) + (n_j) = \mathbb{Z}$, et (n_i) et (n_j) sont étrangers. On conclut avec le théorème des restes chinois. □

4 Inversibilité, anneaux intègres

Définition 4.1. Soit A un anneau (commutatif). Un élément $a \in A^*$ est un *diviseur de zéro* s'il y a $b \in A^*$ avec $ab = 0$. Dans ce cas, b est aussi un diviseur de zéro.
Un anneau 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 $ab = 1$.
L'ensemble des éléments inversibles est noté $A^\times$. C'est un groupe multiplicatif.
Un anneau commutatif non-trivial dont tous les éléments non-nuls sont inversibles est un *corps*. Dans ce cas $A^\times = A^*$.

Remarque 4.2. Ne pas confondre $A^\times$ et $A^* = A \setminus \{0\}$.

Lemme 4.3.
1. *Un élément inversible n'est pas diviseur de zéro. En particulier un corps est intègre.*
2. *Si a n'est pas diviseur de zéro et $ab = ac$, alors $b = c$. En particulier un anneau intègre a simplification multiplicative.*

3. *Un anneau (commutatif) A est un corps ssi A^* est un groupe.*

Démonstration. 1. Si $ab = 0$ et a est inversible, alors $b = a^{-1}ab = a^{-1}0 = 0$.

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

Lemme 4.4. *Soit A un anneau intègre. Alors un ideal I est propre (c'est-à-dire $I \neq A$) ssi A ne contient pas d'élément inversible. En particulier un corps n'a pas d'idéal propre non-trivial.*

Démonstration. Si $I = A$ alors $1 \in I$ et I contient un élément inversible.
Réciproquement, si $a \in I$ est inversible, alors $1 = a^{-1}a \in I$ et $A = A\,1 \subseteq I$. □

Définition 4.5. Soit A un anneau, et $I \trianglelefteq A$ un idéal.
— I est *premier* si pour tous $a, b \in A$, si $ab \in I$ alors $a \in I$ ou $b \in I$.
— I est *maximal* si I est propre et il n'y a pas d'idéal J avec $I < J < A$.

Théorème 4.6. *Soit A un anneau, et $I \trianglelefteq A$ un idéal.*

1. *I est premier si et seulement si A/I est intègre.*
2. *Si A/I est un corps, alors I est maximal.*
3. *Si A est unitaire et I maximal, alors A/I est un corps.*

Démonstration. 1. Soit I premier, et $a, a' \in A$ avec $(a + I)(a' + I) = 0 + I$. Alors $aa' + I = (a + I)(a' + I) = I$ et $aa' \in I$. Puisque I est premier, soit $a \in I$ et $a + I = 0 + I$, soit $a' \in I$ et $a' + I = 0 + I$. Donc A/I est intègre.
Réciproquement, soit A/I intègre et $a, a' \in A$ avec $aa' \in I$. Donc $(a+I)(a'+I) = 0 + I$; puisque A/I est intègre, soit $a + I = 0 + I$ et $a \in I$, soit $a' + I = 0 + I$ et $a' \in I$. Ainsi I est premier.

2. Soit A/I un corps. Alors A/I n'a pas d'idéal non-trivial propre. D'après la proposition 2.10 il n'y a pas d'idéal strictement entre I et A. Donc I est maximal. De plus A/I contient au moins deux éléments, et I est propre.
3. Soit A unitaire et I maximal. Soit $a + I \in (A/I)^*$, donc $a \notin I$. Par maximalité, $I < (a, I) = Aa + I = A$. Il y a donc $a' \in A$ et $c \in I$ avec $a'a + c = 1$. Donc $(a' + I)(a + I) = 1 + I$ et $a + I$ est inversible dans A/I. □

Remarque 4.7 (Hors programme)**.** En fait, pour le dernier point il suffit de supposer que A/I est non-nul : Soit I maximal et A/I non-nul. Soit $a+I \in (A/I)^*$. Alors $a \notin I$, et $I < (a, I)$ d'où $A = (a, I) = (a) + I = Aa + \mathbb{Z}a + I$ par maximalité.
Si $Aa \leq I$, alors $\mathbb{Z}a + I = A$. Or, $(za + I)(z'a + I) = zz'aa + I \subseteq Aa + I = I$ pour tout $z, z' \in \mathbb{Z}$, et A/I est un anneau nul, une contradiction. Donc $Aa \not\leq I$ et $Aa + I = A$. Alors il y a $c \in I$ et $e \in A$ avec $ea + c = a$. Ainsi

$$(e + I)(a + I) = ea + I = a - c + I = a + I.$$

De même, pour tout $a' \in A$ il y a $c' \in I$ et $b' \in A$ avec $b'a+c' = a'$, d'où $(b'+I)(a+I) = b'a + I = a' - c' + I = a' + I$. Donc

$$(e + I)(a' + I) = (e + I)(b' + I)(a + I) = (b' + I)(a + I) = a' + I.$$

Ainsi A/I est unitaire, avec unité $e+I$. Alors il y a $c'' \in I$ et $a'' \in A$ avec $a''a+c'' = e$, et $(a'' + I)(a + I) = a''a + I = e - c'' + I = e + I$. Donc $a + I$ est inversible dans A/I, et A/I est un corps.

Remarque 4.8. Le groupe additif $\mathbb{Z}/p\mathbb{Z}$ pour p premier considéré comme anneau nul n'est pas un corps, mais $I = (0)$ est le seul sous-groupe propre et donc un ideal maximal, ce qui montre que la condition A/I non-nul est nécessaire.

Corollaire 4.9. Si A est unitaire, tout idéal maximal est premier.

Démonstration. Si I est maximal, A/I est un corps, donc intègre, et I est premier. □

Théorème 4.10. *Soit A un anneau unitaire et $I \lhd A$ un idéal propre. Alors I est contenu dans un idéal maximal.*

Avant la démonstration il nous faut introduire un peu de terminologie.

Définition 4.11. Soit X un ensemble. Une partie $\mathcal{F} \subseteq \mathcal{P}(X)$ est *inductive* si toute chaine $(Y_i : i \in I)$ dans $\mathcal{F}$ a un *majorant* dans $\mathcal{F}$, c'est à dire un élément $Y \in \mathcal{F}$ tel que $Y_i \subseteq Y$ pour tout $i \in I$.

Fait 4.12 (Lemme de Zorn)**.** *Si $\mathcal{F}$ est inductive, alors $\mathcal{F}$ à des éléments maximaux.*

Ce fait est une des 1001 versions équivalentes de l'axiome du choix. Sauf dans des cas particuliers (où l'on n'en a pas vraiment besoin), il est donc impossible d'obtenir un tel élément maximal explicitement.

Démonstration du Théorème 4.10. Soit $X = A$ et $\mathcal{F} = \{J \lhd A : I \leq J\}$ l'ensemble des idéaux propres de A contenant I.
Soit $(J_s : s \in S)$ une chaîne non-vide dans $\mathcal{F}$. Alors $\bigcup_{s\in S} J_s$ est un idéal dans A contenant I majorant la chaîne ; puisque $1 \notin J_s$ pour tout $s \in S$ on a $1 \notin \bigcup_{s\in S} J_s$ et $\bigcup_{s\in S} J_s \in \mathcal{F}$. Ainsi $\mathcal{F}$ est inductif et possède un élément M maximal d'après le lemme de Zorn. Alors M es un idéal maximal contenant I. □

L'exemple suivant montre que la condition que A soit unitaire est nécessaire.

Exemple 4.13. Soit A l'anneau des polynômes sur $\mathbb{Z}$ sans terme constant en variables $X, X^{1/2}, X^{1/4} \ldots, X^{1/2^n}, \ldots$, augmenté de 0, avec bien sur $\left(X^{1/2^{n+1}}\right)^2 = X^{1/2^n}$ pour tout $n \in \mathbb{N}$. On note que pour tout $P \in A$ et $n \in \mathbb{N}$ suffisamment grand il y a $Q \in A$ avec $P = QX^{1/2^n}$.
Soit $I_n = (X^{1/2^n})$. Puisque $X^{1/2^k}$ divise $X^{1/2^n}$ pour $k > n$, on a $(X^{1/2^n}) \leq (X^{1/2^k})$ et les $(I_n : n \in \mathbb{N})$ forment une chaîne croissante. Or, $A = \bigcup_{n\in\mathbb{N}} I_n$. Si $I_0 \leq I \lhd A$ avec I maximal, alors A/I est non-nul, puisque tout $P \in A \setminus I$ s'écrit comme $P = QX^{1/2^n}$.

Ainsi A/I est un corps d'après le théorème 4.6. Puisque $I < A$ et $\bigcup_{n\in\mathbb{N}} I_n = A$ il y a $n \in \mathbb{N}$ minimal tel que $I_n \not\leq I$; on note que $n > 0$. Soit $P \in I_n \setminus I$. Alors $P^2 \in I_{n-1} \leq I$. Comme I est maximal, il est premier, et $P \in I$, une contradiction. Donc I_0 n'est pas contenu dans un idéal maximal.

Exemple 4.14. 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 4.15. *$\mathbb{Z}/n\mathbb{Z}$ 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 $sk + tn = \mathrm{pgcd}(k, n) = 1$. Alors

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

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

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

Proposition 4.16. *Un anneau intègre fini est un corps.*

Démonstration. Soit $a \in A^*$. Alors l'application $\lambda_a : x \mapsto ax$ est injective : Si $ax = ax'$, alors d'après lemme 4.3.2 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 4.3.2. 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. □

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.

On va maintenant généraliser la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$ à un anneau intègre quelconque.

Théorème 4.17 (Corps des fractions)**.** *Soit A un anneau intègre. Alors il y a un unique (à isomorphisme près) plus petit corps K contenant A. Tout élément de K s'écrit de la forme ab^{-1} avec $a, b \in A$ (inverse et produit calculé dans K). C'est le* corps des fractions *de A. Si $f : A \to L$ est un morphisme d'anneaux injectif avec L un corps, il se prolonge en morphisme $\bar{f} : K \to L$.*

Démonstration. On imagine que A se plonge dans un corps K. Alors K contient tous les éléments de la forme ab^{-1} avec $a \in A$ et $b \in A^*$. On note que la collection de tels quotients est clos par addition, soustraction, multiplication et réciproque, c'est donc un sous-corps. Par minimalité $K = \{ab^{-1} : a \in A,\, b \in A^*\}$. On va coder l'élément ab^{-1} par la paire (a, b). Or, ce codage n'est pas unique ; on appellera paires qui donnent le même quotient $\sim$-équivalents : $(a, b) \sim (a'b') \Leftrightarrow ab^{-1} = a'b'^{-1} \Leftrightarrow ab' = a'b$.
Pour ce faire, on n'a pas besoin de l'existence *à priori* de K — on le construira. Sur $A \times A^*$ on définit une relation d'équivalence par $(a, b) \sim (a', b')$ si et seulement si $ab' = a'b$. On note que $(a, b) \sim (ac, bc)$ pour $c \neq 0$, et que $\sim$ est réflexif et symétrique. On vérifie la transitivité : si $(a, b) \sim (a', b') \sim (a'', b'')$, alors $ab' = a'b$ et $a'b'' = a''b'$, d'où $ab'b'' = a'bb'' = a''bb'$ et $ab'' = a''b$ par simplification, ce qui donne $(a, b) \sim (a'', b'')$. Ainsi $\sim$ est une relation d'équivalence, dont on note la classe de (a, b) par $[a, b]$.
On *pose* $K = (A \times A^*)/\sim$, et définit une addition $\oplus$ et une multiplication $\otimes$ sur K par les formules qu'on connaît des quotients ab^{-1} :

$$[a, b] \oplus [a', b'] = [ab' + a'b, bb'] \qquad \text{et} \qquad [a, b] \otimes [a', b'] = [aa', bb'].$$

Il faut vérifier que la somme et le produit ne dépendent pas du choix des représentants. Par symétrie il suffit de vérifier sur la gauche. Soit donc $[a, b] = [a'', b'']$, et donc $ab'' = a''b$. Alors $[a'', b''] \oplus [a', b'] = [a''b' + a'b'', b''b']$ et $[a'', b''] \otimes [a', b'] = [a''a', b''b']$. Or,

$$\begin{aligned}[ab' + a'b, bb'] = [ab'b'' + a'bb'', bb'b''] = [a''b'b + a'bb'', bb'b''] = [a''b' + a'b'', b''b'] \text{ et} \\ [aa', bb'] = [aa'b'', bb'b''] = [a''a'b, bb'b''] = [a''a', b''b'].\end{aligned}$$

Donc $\oplus$ et $\otimes$ sont bien définis.
On fixe $c \in A^*$ et pose $0 = [0, c]$ et $1 = [c, c]$. Ces classes ne dépendent pas du choix de c. Pour $[a, b] \in K$ on pose $-[a, b] = [-a, b]$, et si $a \neq 0$ on pose $[a, b]^{-1} = [b, a]$. On vérifie facilement que ceci ne dépend pas du choix des représentants. Alors

$$[a, b] \oplus [0, c] = [ac + 0b, bc] = [a, b] \qquad \text{et} \qquad [a, b] \otimes [c, c] = [ac, bc] = [a, b],$$

et donc

$$\begin{aligned}[a, b] \oplus (-[a, b]) = [a, b] \oplus [-a, b] = [ab - ab, bb] = [0, bb] = 0, \text{ et} \\ [a, b] \otimes [a, b]^{-1} = [a, b] \otimes [b, a] = [ab, ab] = 1.\end{aligned}$$

Il est évident de la définition que $\oplus$ et $\otimes$ sont commutatifs. On vérifie l'associativité :

$$\begin{aligned}([a, b] \oplus [a', b']) \oplus [a'', b''] &= [ab' + a'b, bb'] \oplus [a'', b''] = [ab'b'' + a'bb'' + a''bb', bb'b''] \\ &= [a, b] \oplus [a'b'' + a''b', b'b''] = [a, b] \oplus ([a', b'] \oplus [a'', b'']), \text{ et} \\ ([a, b] \otimes [a', b']) \otimes [a'', b''] &= [aa', bb'] \otimes [[a'', b''] = [aa'a'', bb'b''] = [a, b] \otimes [a'a'', b'b''] \\ &= [a, b] \otimes ([a', b'] \otimes [a'', b''])\end{aligned}$$

et la distributivité :

$$\begin{aligned}([a, b] + [a', b']) \otimes [a'', b''] &= [ab' + a'b, bb'] \otimes [a'', b''] = [aa''b' + a'a''b, bb'b''] \\ &= [aa''b'b'' + a'a''bb'', bb'b''b''] = [aa'', bb''] \oplus [a'a'', b'b''] \\ &= [a, b] \otimes [a'', b''] \oplus [a', b'] \otimes [a'', b''].\end{aligned}$$

Ainsi $(K, 0, 1, \oplus, \otimes)$ est bien un corps.
On considère $f : A \to K$ défini par $a \mapsto [ac, c]$ (on note que $f(a)$ ne dépend pas de c). Si $f(a) = f(a')$ alors $[ac, c] = [a'c, c]$, soit $ac^2 = a'c^2$ et $a = a'$; ainsi f est injectif. On a $f(0) = [0c, c] = 0$, $f(1) = [1c, c] = 1$ (si A est unitaire), et f préserve l'addition et la multiplication :

$$f(a+b) = [(a+b)c, c] = [acc + bcc, cc] = [ac, c] + [bc, c] = f(a) \oplus f(b), \text{ et}$$
$$f(ab) = [abc, c] = [acbc, cc] = [ac, c] \otimes [bc, c] = f(a) \otimes f(b).$$

Ainsi f plonge A dans K, et tout élément $[a, b] \in K$ est de la forme

$$f(a) \otimes f(b)^{-1} = [ac, c] \otimes [bc, c]^{-1} = [ac, c][c, bc] = [ac^2, bc^2] = [a, b].$$

On identifie donc A avec son image dans K.
Si L est un autre corps et $g : A \to L$ est un plongement, on prolonge g sur K par $g : [a, b] \mapsto g(a)g(b)^{-1}$; on vérifie que $\bar{g}$ ne dépend pas des choix des représentants, que $\bar{g}(0) = 0$ et que $\bar{g}$ prolonge g et préserve l'addition et la multiplication. Ainsi $\bar{g}$ est un homomorphisme de K dans L. Or, $\ker \bar{g}$ est un idéal de K qui ne peut pas être K entier puisque $\ker \bar{g} \cap A = \{0\}$. Mais un idéal d'un corps est soit (0) soit le corps entier. Ainsi $\ker \bar{g} = (0)$ et $\bar{g}$ est injectif, ce qui montre que K est minimal et unique. □