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 I 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. □

5 Divisibilité, anneaux principaux

Définition 5.1. 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 $ac = b$. On note que $a \mid b$ ssi $b \in (a)$
- Un élément $a \in A^*$ non-inversible est *irréductible* si pour tous $b, c \in A$, si $a = bc$ alors b ou c est inversible.
- Un élément $p \in A^*$ non-inversible 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 5.2. 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 $|a|^2 \in \mathbb{N}$. Si $a \in A$ est inversible, alors $|a|^2\,|a^{-1}|^2 = |aa^{-1}|^2 = |1|^2 = 1$, d'où $|a|^2 = 1$ et $|a| = 1$. Si $z = a + i\sqrt{5}b \in Z[i\sqrt{5}]$ avec $|z|^2 < 5$, on a $b = 0$ et $z \in \mathbb{Z}$. En particulier les seuls éléments z avec $|z|^2 = 1$ sont ± 1, et il n'y a pas d'élément z avec $|z|^2 \in \{2, 3\}$.
On va montrer que $1 \pm i\sqrt{5}$, 2 et 3 sont irréductibles. Si $zz' = 1 \pm i\sqrt{5}$, alors $|z|^2|z'|^2 = 6$; si $zz' = 2$, alors $|z|^2|z'|^2 = 4$, et si $zz' = 3$, alors $|z|^2|z'|^2 = 9$. Dans tous les cas, $|z|^2 \leq 3$ ou $|z'|^2 \leq 3$, donc vaut 1, et $1 \pm i\sqrt{5}$, 2 et 3 sont tous irréductibles. Il n'y a donc pas factorisation unique en irréductibles dans A.

On va montrer que ni $1\pm i\sqrt{5}$ ni 2 ni 3 sont premiers. On a $1\pm i\sqrt{5} \mid 2\cdot 3$, mais $1\pm i\sqrt{5} \nmid 2$ et $1 \pm i\sqrt{5} \nmid 3$ puisque $|1 \pm i\sqrt{5}|^2 = 6 \nmid |2|^2 = 4$ et $|1 \pm i\sqrt{5}|^2 = 6 \nmid |3|^2 = 9$. Donc $1 \pm i\sqrt{5}$ n'est pas premier. De même, $2 \mid (1 + i\sqrt{5})(1 - i\sqrt{5})$ et $3 \mid (1 + i\sqrt{5})(1 - i\sqrt{5})$, mais ni 2 ni 3 divisent $1 \pm i\sqrt{5}$ puisque ni $|2|^2 = 4$ ni $|3|^2 = 9$ divisent $|1 \pm i\sqrt{5}|^2 = 6$. Ainsi ni 2 ni 3 sont premiers.

Proposition 5.3. *Soit A un anneau intègre unitaire. Alors tout élément premier est irréductible.*

Démonstration. Soit $a \in A$ premier, et $b, c \in A$ avec $a = bc$. Alors $a \neq 0$ implique $b \neq 0 \neq c$. 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 4.3. Ainsi c est inversible. Ceci montre que a est irréductible. □

Remarque 5.4. La réciproque est fausse, comme on a vu dans l'exemple 5.2.

Définition 5.5. Soit A un anneau intègre unitaire. Deux éléments $a, b \in A$ sont *associés* s'il y a $c \in A$ inversible avec $a = cb$. On le notera $a \sim b$.

Remarque 5.6. l'association est une relation d'équivalence : On a $a = a \cdot 1$, donc $\sim$ est réflexif. Si $a \sim b$ il y a $c \in A^\times$ avec $a = bc$, et donc $c^{-1} \in A^\times$ avec $b = ac^{-1}$, c'est-à-dire $b \sim a$ et $\sim$ est symétrique. Enfin, si $a \sim b \sim c$, il y a $d, d' \in A^\times$ avec $a = bd$ et $b = cd'$, d'ou $dd' \in A^\times$ et $a = cdd'$, c'est-à-dire $a \sim c$ et $\sim$ est transitif.

Lemme 5.7. *Soit A un anneau intègre unitaire, et $a, b \in A$. Deux éléments $a, b \in A$ sont associés si et seulement si $(a) = (b)$.*

Démonstration. S'il y a $c \in A$ inversible avec $ac = b$, alors $bc^{-1} = a$. Donc $b \in (a)$ et $a \in (b)$, d'où $(a) = (b)$.
Réciproquement, supposons $(a) = (b)$. Puisque $b \in (a) = aA$, il y a $c \in A$ avec $ac = b$. De même, il y a $d \in A$ avec $bd = a$. Donc $a = bd = acd$. Alors soit $a = 0$, soit $a \neq 0$ et $cd = 1$. Dans le premier cas $(b) = (0)$ implique $b = 0 = a \cdot 1$; dans le deuxième cas c est inversible avec $ac = b$. □

Proposition 5.8. *Soit A un anneau intègre unitaire, et $a \in A^*$ non-inversible.*

1. *L'élément a est premier si et seulement si l'idéal (a) est premier.*
2. *L'élément a est irréductible si et seulement s'il n'existe pas de $b \in A$ avec $(a) < (b) < A$.*

Démonstration. 1. Soit (a) premier, et $b, c \in A$ avec $a \mid bc$. Donc $bc \in (a)$; puisque (a) est premier, soit $b \in (a)$ et $a \mid b$, soit $c \in (a)$ et $a \mid c$. Ainsi a est premier.

Réciproquement, soit a premier, et soient $b, c \in A$ avec $bc \in (a)$. Puisque (a) est premier, soit $b \in (a)$ et $a \mid b$, soit $c \in (a)$ et $a \mid c$. Ainsi a est premier.

2. Soit a irréductible, et $b \in A$ avec $(a) \leq (b) \trianglelefteq A$. Donc $a \in (b)$ et il y a $c \in A$ avec $a = bc$. Par irréducibilité de a, soit b est inversible et $(b) = A$, soit c est inversible et $(a) = (b)$.

   Réciproquement, supposons qu'il n'existe aucun $b \in A$ avec $(a) < (b) < A$. Soient $c, d \in A$ avec $a = cd$; notons que $a \neq 0$ implique $c \neq 0 \neq d$. Alors $(a) \leq (c) \leq A$. Si $(c) = A$ alors c est inversible ; si $(c) = (a)$ alors a et c sont associés. Il y a donc $d' \in A\times$ avec $a = cd'$, ce qui donne $c(d - d') = a - a = 0$ et $d = d'$ est inversible. Ainsi a est irréductible. □

Définition 5.9. Un idéal I dans un anneau A est *principal* s'il y a $a \in A$ avec $I = (a)$. Un anneau intègre unitaire A est *principal* si tout idéal dans A est principal.

Exemple 5.10. On va voir plus bas des exemples d'anneaux principaux. On note que $\mathbb{Z}[X]$ n'est pas principal : l'idéal $(2, X)$ n'est pas principal (exercice).

Proposition 5.11. *Soit A un anneau principal, et $a \in A^* \setminus A^\times$. Sont équivalents :*

1. *a est premier.*
2. *a est irréductible.*
3. *(a) est premier.*
4. *(a) est maximal.*

Démonstration. On sait déjà que 4.⇒3.⇒1.⇒2 même sans hypothèse de principalité. Enfin, 2.⇒4. découle de la proposition 5.8.2, sachant que tout idéal est principal. □

Définition 5.12. Un anneau intègre unitaire est *euclidien* s'il y a une fonction $N : A \setminus \{0\} \to \mathbb{N}$ telle que

1. On a $N(ab) \geq N(a)$ pour tout $a, b \in A \setminus \{0\}$.
2. Pour tout $a, b \in A$ avec $b \neq 0$ il y a $q, r \in A$ avec $a = bq + r$ et soit $r = 0$, soit $N(r) < N(b)$.

La fonction N est la *norme euclidienne* ; q et r sont le *quotient* et le *reste* de la division euclidienne de a par b. En général ils ne sont pas uniques.

Exemple 5.13.
- — $\mathbb{Z}$ avec la norme $N(z) = |z|$.
- — $K[X]$ avec la norme $N(P) = \deg(P)$.
- — Les entiers de Gauss $\mathbb{Z}[i]$ avec la norme $N(x + iy) = x^2 + y^2$.
  Pour vérifier la condition 2., on considère $a, b \in \mathbb{Z}[i]$ avec $b \neq 0$. Les points de $\mathbb{Z}[i]$ forment un réseau rectangulaire de distance horizontale et verticale 1. Pour tout point $z \in \mathbb{C}$ on trouve donc un point de $\mathbb{Z}[i]$ de distance au plus $\sqrt{2}/2$ de z (avec égalité si z est le milieu d'un carré unitaire dont les coins sont dans $\mathbb{Z}[i]$). En particulier il y a $q \in \mathbb{Z}[i]$ avec $|\frac{a}{b} - q| \leq \frac{\sqrt{2}}{2}$. On pose $r = a - bq$. Alors soit $r = 0$, soit
  $$N(r) = |r|^2 = |a - bq| \leq \frac{1}{2} |b|^2 < |b|^2 = N(b).$$

Lemme 5.14. *Soit A un anneau euclidien. Alors $N(1) = \min \mathrm{im}(N)$ est la valeur minimale de la norme. Un élément $a \in A$ est inversible si et seulement si $N(a) = N(1)$.*

Démonstration. Pour $b \in A^*$ on a $N(b) = N(1 \cdot b) \geq N(1)$.
Si a est inversible, disons $c \in A$ satisfait $ac = 1$, alors $N(1) = N(ac) \geq N(a) \geq N(1)$ et on a égalité. Réciproquement, si $N(a) = N(1)$, alors $a \neq 0$ et il y a $q, r \in A$ avec $1 = aq + r$ et soit $N(r) < N(1)$ ou $r = 0$. Le premier cas est impossible. Donc $r = 0$ et $aq = 1$, ce qui veut dire que a est inversible. □

Théorème 5.15. *Un anneau euclidien est principal.*

Démonstration. Soit $(0) \neq I \trianglelefteq A$. On choisit $0 \neq a \in I$ avec $N(a)$ minimal possible. Alors pour tout $b \in I$ il y a $q, r \in A$ avec $b = aq + r$, et soit $r = 0$, soit $N(r) < N(a)$. Or, $r = b - aq \in I$, d'où $N(r) \geq N(a)$ par minimalité. Donc $r = 0$ et $b = aq \in (a)$. Ainsi $I = (a)$ est principal. □

Exemple 5.16. L'anneau $\mathbb{Z}[\frac{1+\sqrt{19}}{2}]$ est principal, mais pas euclidien.

Si on peut deviner la norme, il est généralement facile de montrer qu'un anneau est euclidien. Sinon, il est souvent plus facile de montrer qu'un anneau est principal.

Définition 5.17. Soit A un anneau principal, et $a_1, \ldots, a_n \in A^*$.
- Un élément $\delta \in A$ tel que $(\delta) = (a_1, \ldots, a_n)$ est un pgcd de $a_1, \ldots, a_n$. On le note $\delta = \mathrm{pgcd}(a_1, \ldots, a_n) = a_1 \wedge \cdots \wedge a_n$. D'après le lemme 5.7 un pgcd est déterminé à association près.
- Un élément $\Delta \in A$ tel que $(\Delta) = (a_1) \cap \cdots \cap (a_n)$ est un ppcm de $_1, \ldots, a_n$. Il est noté $\delta = \mathrm{ppcm}(a_1, \ldots, a_n) = a_1 \vee \cdots \vee a_n$, et déterminé à association près.

Remarque 5.18. Dans $\mathbb{Z}$ et $K[X]$ on peut éliminer l'ambiguïté dans le définition du pgcd et du ppcm en demandant qu'il soit positif (dans $\mathbb{Z}$) ou unitaire (dans $K[X]$). En général il n'y a pas de choix canonique.

Théorème 5.19 (Relation de Bézout)**.** *Soit $\delta = a_1 \wedge \cdots \wedge a_n$. Alors il y a $c_1, \ldots, c_n \in A$ avec $\delta = c_1 a_1 + \cdots + c_n a_n$.*

Démonstration. On a $\delta \in (a_1, \ldots, a_n) = a_1 A + \cdots + a_n A$. □

Remarque 5.20. Les éléments $c_1, \ldots, c_n$ sont des *coefficients de Bézout.*

Définition 5.21. Les éléments $a_1, \ldots, a_n$ sont *premiers entre eux* si $a_1 \wedge \cdots \wedge a_n = 1$.

Corollaire 5.22 (Théorème de Bézout)**.** Soit A principal. Les éléments $a_1, \ldots, a_n$ sont premiers entre eux si et seulement s'il y a $c_1, \ldots, c_n \in A$ avec $a_1 c_1 + \cdots + a_n c_n = 1$.

Démonstration. L'existence est la relation de Bézout. Réciproquement, $a_1 \wedge \cdots \wedge a_n$ doit diviser $a_1 c_1 + \cdots + a_n c_n$ et est donc associé à 1. □

Théorème 5.23 (Lemme de Gauss)**.** *Soient a, b, c non-nuls. Si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.*

Démonstration. Puisque $a \wedge b = 1$ il y a $u, v \in A$ avec $au + bv = 1$. Alors $c = acu + bcv$. Or, $a \mid acu$ et $a \mid bcv$, donc $a \mid acu + bcv = c$. □

Théorème 5.24. *Soit $\delta = a_1 \wedge \cdots \wedge a_n$ et $\Delta = a_1 \vee \cdots \vee a_n$.*

1. *Pour un élément $b \in A$ on a $b \mid \delta$ si et seulement si $b \mid a_i$ pour $i = 1, \ldots, n$.*
2. *Pour un élément $b \in A$ on a $\Delta \mid b$ si et seulement si $a_i \mid b$ pour $i = 1, \ldots, n$.*

Démonstration.

1. D'après Bézout il y a $c_1, \ldots, c_n \in A$ avec $\delta = c_1 a_1 + \cdots + c_n a_n$. Donc si $b \mid a_i$ pour $i = 1, \ldots, n$ alors $b \mid c_1 a_1 + \cdots + c_n a_n = \delta$.
   Réciproquement, $a_i \in (\delta)$ pour $i = 1, \ldots, n$, donc il y a $d_i \in A$ avec $a_i = \delta d_i$. Donc si $b \mid \delta$, alors $b \mid \delta d_i = a_i$.
2. On a $\Delta \in (a_i)$ pour $i = 1, \ldots, n$, et il y a $c_i \in A$ avec $\Delta = a_i c_i$. Donc si $\Delta \mid b$, alors $a_i \mid b$ pour $i = 1, \ldots, n$.
   Réciproquement, si $a_i \mid b$ alors $b \in (a_i)$ pour $i = 1, \ldots, n$, et donc $b \in (a_1) \cap \cdots \cap (a_n) = (\Delta)$. Ainsi $\Delta \mid b$. □

Remarque 5.25. Puisque $a \mid b$ si et seulement $ca \mid cb$, on a $ca_1 \wedge \cdots \wedge ca_n = c\,(a_1 \wedge \cdots \wedge a_n)$ et $ca_1 \vee \cdots \vee ca_n = c\,(a_1 \vee \cdots \vee a_n)$.

Théorème 5.26. *Soit A un anneau principal, $a, b \in A^*$, $\delta = A \wedge b$ et $\Delta = a \vee b$. Alors $(\delta)\,(\Delta) = (ab)$, c'est-à-dire $\delta\Delta \sim ab$.*

Remarque 5.27. Notons que $(\delta)\,(\Delta) = A\delta A\Delta = AA\delta\Delta = A\delta\Delta = (\delta\Delta)$: Dans un anneau unitaire le produit de deux idéaux principaux est un idéal principal.

Démonstration. Soient $a', b' \in A$ avec $a = a'\delta$ et $b = b'\delta$. Alors $a' \wedge b' = 1$, et il suffit de montrer que $(a' \vee b') = (a'b')$, puisque cela implique

$$(\delta\Delta) = \delta(a \vee b) = \delta(a'\delta \vee b'\delta) = \delta^2(a' \vee b') = \delta^2(a'b') = (a'\delta b'\delta) = (ab).$$

Puisque $a' \mid \Delta$ il y a $c \in A$ avec $a'c = \Delta$. Or, $b' \mid \Delta = a'c$ et $b' \wedge a' = 1$ d'où $b' \mid c$ d'après Gauss et il y a $c' \in A$ avec $b'c' = c$. Alors $\Delta = a'c = a'b'c'$ et $(\Delta) \leq (a'b')$. Réciproquement, $a'b' \in (a') \cap (b') = (\Delta)$, d'où $(a'b') \leq (\Delta)$. Ainsi on a égalité. □

Dans un anneau euclidien, on calcule le pgcd à l'aide de l'*algorithme d'Euclide*. Soient $a_0, a_1 \in A^*$. Alors on trouve $q_1, a_2 \in A$ avec $a_0 = a_1 q_1 + a_2$ et $a_2 = 0$ ou $N(a_2) < N(b)$. Puisque $(a_0, a_1) = (a_1, a_2)$, on a $a_0 \wedge a_1 = a_1 \wedge a_2$. Si $a_2 = 0$ on a $a_1 \mid a_0$ et $(a_0, a_1) = (a_1)$, d'où $a_0 \wedge a_1 = a_1$. Si $a_2 \neq 0$ on itère avec a_1, a_2. Puisque la suite d'entiers $(N(a_i))_{i>0}$ décroît strictement, l'algorithme s'arrête. Pour calculer des coefficents de Bézout, on calcule $u_n, v_n \in A$ tel que $a_n = u_n a_0 + v_n a_1$. On pose $u_0 = v_1 = 1$ et $u_1 = v_0 = 0$. Si $a_{n-1} = u_{n-1} a_0 + v_{n-1} a_1$ et $a_n = u_n a_0 + v_n a_1$, on obtient

$$\begin{aligned} a_{n+1} &= a_{n-1} - a_n q_n \\ &= u_{n-1} a_0 + v_{n-1} a_1 - (u_n a_0 + v_n a_1) q_n \\ &= (u_{n-1} - q_n u_n) a_0 + (v_{n-1} - q_n v_n) a_1. \end{aligned}$$

Ainsi $u_{n+1} = u_{n-1} - q_n u_n$ et $v_{n+1} = v_{n-1} - q_n v_n$. On itère.

Exemple 5.28. Calculer $597 \wedge 322$, ainsi que des coefficients de Bézout.

n	a_{n-1}	$=$	a_n	$\times$	q_n	$+$	a_{n+1}	u_n	v_n
0			597				322	1	0
1	597	$=$	322	$\times$	1	$+$	275	0	1
2	322	$=$	275	$\times$	1	$+$	47	1	-1
3	275	$=$	47	$\times$	5	$+$	40	-1	2
4	47	$=$	40	$\times$	1	$+$	7	6	-11
5	40	$=$	7	$\times$	5	$+$	5	-7	13
6	7	$=$	5	$\times$	1	$+$	2	41	-76
7	5	$=$	2	$\times$	2	$+$	1	-48	89
8	2	$=$	1	$\times$	2	$+$	0	137	-254

Ainsi $597 \wedge 322 = 1 = 597 \times 137 - 322 \times 254$.

Définition 5.29. Un anneau est *noetherien* s'il n'y a pas de chaîne $I_0 < I_1 < I_2 < \cdots$ infinie strictement croissante d'idéaux.

Proposition 5.30. *Un anneau est noethérien si et seulement si tout idéal est finiment engendré (c'est-à-dire engendré par un nombre fini d'éléments).*

Démonstration. Supposons que A est noethérien, mais que $I \trianglelefteq A$ est un idéal qui n'est pas finiment engendré. Supposons qu'on ait trouvé $a_1, \ldots, a_n \in I$ tel que $(a_1) < (a_1, a_2) < \cdots < (a_1, \ldots, a_n)$ (pour $n = 0$ l'hypothèse est vide). Puisque I n'est pas finiment engendré, on a $(a_1, \ldots, a_n) < I$ et il y a $a_{n+1} \in I \setminus (a_1, \ldots, a_n)$. Alors $(a_1, \ldots, a_n) < (a_1, \ldots, a_n, a_{n+1}) < I$. Ainsi on trouve une chaîne infinie strictement croissante d'idéaux, une contradiction. Donc tout idéal de A est finiment engendré.
Réciproquement, supposons que tout idéal est finiment engendré. Soit $I_0 < I_1 < \cdots \trianglelefteq A$ une chaîne infinie strictement croissante d'idéaux. Alors $I = \bigcup_{n\in\mathbb{N}} I_n$ est un idéal dans A, donc engendré par un nombre fini d'éléments $a_1, \ldots, a_k \in I$. Or, $I = \bigcup_{n\in\mathbb{N}} I_n$; il y a donc $n_0 \in \mathbb{N}$ tel que $a_1, \ldots, a_k \in I_{n_0}$. Alors $I = (a_1, \ldots, a_k) \leq I_{n_0} < I_{n_0+1} \leq I$, une contradiction. Ainsi A est noethérien. □

Corollaire 5.31. Un anneau principal est noethérien. □

Lemme 5.32. *Dans un anneau intègre unitaire noethérien, tout élément non-nul non-inversible se factorise comme produit d'éléments irréductibles.*

Démonstration. Soit $a \in A^*$ non-inversible, et supposons que a_0 ne se factorise pas comme produit d'éléments irréductibles. En particulier a_0 n'est pas irréductible, et il y a $b, c \in A$ non-inversibles avec $a = bc$. Alors a est associé ni à b ni à c. Donc soit a soit b ne se factorise pas comme produit d'irréductibles, et il y a $a_1 \in \{b, c\}$ avec $(a_0) < (a_1)$ (on ne peut pas avoir égalité, car sinon a_0 et a_1 seraient associés). On itère avec a_1 à la place de a_0, et on obtient une chaîne infinie strictement croissante d'idéaux, ce qui contredit la noethérianité. □

Proposition 5.33. *Dans un anneau intègre unitaire principal A, tout élément $a \in A^*$ non-inversible se factorise de manière unique (à permutation et association près) comme produit d'éléments premiers.*

Démonstration. A est principal, donc noethérien. D'après lelemme 5.32 tout élément $a \in A^*$ non-inversible se factorise en produit d'éléments irréductibles, qui sont premiers d'après la proposition 5.11. Pour montrer l'unicité, supposons que

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

pour des éléments premiers $p_1, \ldots, p_n$ et $q_1, \ldots, q_m$. On fait une récurrence sur n.
Initialisation. Si $n = 1$, alors $a = p_1 = q_1 \cdots q_m$. Puisque p_1 est premier, il y a $i \in [\![1, m]\!]$ tel que p_1 divise q_i. Mais q_i est premier, et il y a $b \in A^\times$ avec $p_1 = bq_i$. Donc $p_1 = bq_i = bq_1 \cdots q_m$. Par simplification on a $b = q_1 \cdots q_{i-1} q_{i+1} \cdots q_m$, ce qui implique que q_j est inversible pour $j \neq i$. Or, un élément premier n'est pas inversible. On a donc $m = 1$ et $p_1 = q_1 = a$.
Hypothèse. On suppose qu'un produit de $n-1$ éléments premiers a une unique factorisation en facteurs premiers.
Hérédité. On a $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$ comme ci-dessus. Alors $p_n \mid q_1 q_2 \cdots q_m$; puisque p_n est premier il y a $i \in [\![1, m]\!]$ tel que $p_n \mid q_i$, et il y a $b \in A$ avec $p_n = bq_i$; puisque q_i est irréductible et p_1 non-inversible, b est inversible et p_n est associé à q_i ; quitte à permuter les q_i on peut supposer $i = m$. Alors $p_1 \cdots p_{n-1} = q_1 \cdots q_{m-1}$ avec $q_1, \ldots, q_{m-2}, q_{m-1}b$ premiers. Par hypothèse de récurrence $n - 1 = m - 1$ et il y a une permutation σ de $[\![1, n-1]\!]$ tel que p_i est associé à $q_{\sigma(i)}$ pour $i = 1, \ldots, n-1$ (être associé à q_{m-1} est la même chose qu'être associé à $q_{m-1}b$). Donc la factorisation de a en éléments premiers est unique. □

Soit A un anneau factoriel, et $\mathcal{P}$ un système de représentants pour les classes d'association des éléments premiers. Cela signifie que tout élément premier dans A est associé à un unique élément de $\mathcal{P}$.

Lemme 5.34. *Tout $a \in A^*$ s'écrit de manière unique comme $a = u \prod_{p \in \mathcal{P}} p^{n_p}$, avec u inversible et $n_p \in \mathbb{N}$ pour tout $p \in \mathcal{P}$, et tous nuls sauf un nombre fini.*

Démonstration. On considère une factorisation $a = q_1 \cdots q_n$ de a en facteurs premiers. Alors pour tout $i \in [\![1, n]\!]$ il y a $p_i \in \mathcal{P}$ associé à q_i, et donc $u_i \in A^\times$ avec $q_i = p_i u_i$. Ainsi $a = u_1 \cdots u_n p_1 \cdots p_n$; on pose $u = u_1 \cdots u_n$ et regroupe les p_i identiques, ce qui nous donne la factorisation $a = u \prod_{p \in \mathcal{P}} p^{n_p}$ souhaité. L'unicité suit de la factorisation unique. □

Proposition 5.35. *Soit $a = u \prod_{p \in \mathcal{P}} p^{n_p}$ et $b = v \prod_{p \in \mathcal{P}} p^{m_p}$ avec $u, v \in A^\times$. Alors $a \mid b$ si et seulement si $n_p \leq m_p$ pour tout $p \in \mathcal{P}$.*

Démonstration. Si $n_p \leq m_p$ pour tout $p \in \mathcal{P}$, alors $c = \prod_{p \in \mathcal{P}} p^{m_p - n_p} \in A$, et $b = vu^{-1}ac$. Donc $a \mid b$.

Réciproquement, supposons que $a \mid b$. Alors il y a $c \in A$ tel que $ac = b$. Soit $c = w \prod_{p\in\mathcal{P}} p^{k_p}$ la factorisation de c, avec $w \in A^\times$. Donc

$$v \prod_{p\in\mathcal{P}} p^{m_p} = b = ac = u \prod_{p\in\mathcal{P}} p^{n_p}\, w \prod_{p\in\mathcal{P}} p^{k_p} = uw \prod_{p\in\mathcal{P}} p^{n_p+k_p}\,;$$

l'unicité donne $v = uw$ et $m_p = n_p + k_p \geq n_p$ pour tout $p \in \mathcal{P}$. □

Définition 5.36. Soit $a = u \prod_{p\in\mathcal{P}} p^{n_p}$ et $b = v \prod_{p\in\mathcal{P}} p^{m_p}$ avec $u, v \in A^\times$. Soit $k_p = \min\{n_p, m_p\}$ et $\ell_p = \max\{n_p, m_p\}$. On pose

$$\operatorname{pgcd}(a, b) = a \wedge b = \prod_{p\in\mathcal{P}} p^{k_p} \quad \text{et} \quad \operatorname{ppcm}\{a, b\} = a \vee b = \prod_{p\in\mathcal{P}} p^{\ell_p}.$$

Lemme 5.37. *Soient $a, b, c \in A^\times$. Alors*

$$c \mid a \text{ et } c \mid b \Leftrightarrow c \mid a \wedge b,$$
$$a \mid c \text{ et } b \mid c \Leftrightarrow a \vee b \mid c.$$

De plus, $(a \wedge b)\,(a \vee b)$ est associé à ab.

Démonstration. Les équivalences sont conséquence de la proposition 5.35. Le dernier énoncé est un simple calcul, en utilisant $\min\{m, n\} + \max\{m, n\} = m + n$. □

Un anneau factoriel permet donc un plus grand commun diviseur et un plus petit commun multiple, avec les propriétés habituels. Cependant, il satisfait une identité de Bézout si et seulement s'il est principal.

6 Anneaux de polynômes

Définition 6.1. Soit A un anneau unitaire. L'*anneau des polynômes sur A*, ou *avec coefficients dans A*, est l'anneau des tous les polynômes $\sum_i a_i X^i$ avec $a_i \in A$ pour tout i, et presque tous les a_i nuls. Il est noté $A[X]$.

Proposition 6.2 (Propriété universelle)**.** *Soient A et B deux anneaux unitaires et $f : A \to B$ un homomorphisme unitaire (donc avec $f(1_A) = 1_B$). Soit $b \in B$. Alors il existe un unique morphisme $\bar{f} : A[X] \to B$ qui prolonge f et tel que $\bar{f}(X) = b$. On a $(\ker f)[X] \leq \ker \bar{f}$.*

Démonstration. On pose $\bar{f} : \sum_i a_i X^i \mapsto \sum_i f(a_i) b^i$, et vérifie que c'est un homomorphisme. Quant à l'unicité, puisque $\bar{f}(a_i) = f(a_i)$ et $\bar{f}(X) = b$, ceci détermine $\bar{f}$. Enfin, si $\sum_i a_i X^i \in (\ker f)[X]$, alors

$$\bar{f}\big(\sum_i a_i X^i\big) = \sum_i f(a_i) X^i = 0$$

et $\sum_i a_i X^i \in \ker \bar{f}$. □

Remarque 6.3. Plus précisément, $\sum_i a_i X^i \in \ker \bar{f}$ si et seulement si b est racine de $\sum_i f(a_i)X^i$.

Corollaire 6.4. Soit $f : A \to B$ un morphisme d'anneaux unitaires. Alors f induit un morphisme $\bar{f} : A[X] \to B[X]$ donné par $\sum_i a_i X^i \mapsto \sum_i f(a_i)X^i$. On a $\ker \bar{f} = (\ker f)[X]$.

Démonstration. On considère f comme homomorphisme de A dans $B[X]$. On applique le lemme 6.2 avec $b = X$. Quant au noyau, $\sum_i f(a_i)X^i = 0$ si et seulement si $f(a_i) = 0$ pour tout i, et donc $a_i \in \ker f$ pour tout i. □

Définition 6.5. Soit A anneau unitaire, et $P(X) = \sum_i a_i X^i \in A[X]^*$.
- Le *degré* de P est $\deg P = \max\{i : a_i \neq 0\}$. On pose $\deg 0 = -\infty$.
- La *valuation* de P est $\operatorname{val} P = \min\{i : a_i \neq 0\}$. On pose $\operatorname{val} 0 = +\infty$.
- Si $\deg P = d$, le *coefficient dominant* est $cd(P) = a_d$, et le terme dominant est $td(P) = a_d X^d$.

Remarque 6.6. On vérifie facilement que $\deg(P + Q) \leq \max\{\deg P, \deg Q\}$, avec égalité si et seulement si $\deg P \neq \deg Q$, ou $\deg P = \deg Q$ et $cd(P) + cd(Q) \neq 0$. De même, $\operatorname{val}(P + Q) \geq \min\{\operatorname{val} P, \operatorname{val} Q\}$, avec égalite si $\operatorname{val} P \neq \operatorname{val} Q$.

Remarque 6.7. Si A est intègre, $\deg(PQ) = \deg P + \deg Q$ et $\operatorname{val}(PQ) = \operatorname{val} P + \operatorname{val} Q$. De plus, $td(PQ) = td(P)\, td(Q)$ et $cd(PQ) = cd(P)\, cd(Q)$.

Théorème 6.8. *Soit A un anneau intègre unitaire. Alors $A[X]$ est intègre ; il est principal si et seulement si A est un corps.*

Démonstration. Si $P, Q \in A[X]^*$, alors $cd(PQ) = cd(P)\, cd(Q) \neq 0$, donc $PQ \neq 0$ et $A[X]$ est intègre.
Si A est un corps, alors $A[X]$ est même euclidien, avec le degré comme norme, donc principal.
Réciproquement, supposons que $A[X]$ est principal. Soit $a \in A^*$ et considérons l'idéal $(a, X) \lhd A$. Soit $P \in A[X]$ tel que $(P) = (X, a)$. Alors a est multiple de P, d'où $\deg P \leq \deg a = 0$ et $P \in A$ est une constante. De même, X est multiple de P, et il y a $b, c \in A$ avec $P(bX + c) = X$, d'où $Pb = 1$ et P est inversible. Ainsi $(a, X) = (P) = A[X]$ et $1 \in (a, X)$. Il y a donc $Q, R \in A[X]$ avec $Qa + RX = 1$. Or, le terme constant de $Qa + RX$ est $q_0 a$, où q_0 est le terme constant de Q. Ainsi $q_0 a = 1$ et a est inversible. Donc $A^* = A^\times$ et A est un corps. □

Pour le reste du chapitre on prendra $A = \mathbb{Z}$.

Définition 6.9. Soit $P \in \mathbb{Z}[X]$. Le *contenu* $c(P)$ est le pgcd des coefficients de P.

Proposition 6.10. *Soient $P, Q \in \mathbb{Z}[X]$. Alors $c(PQ) = c(P)\, c(Q)$.*

Démonstration. On prend $\tilde{P}, \tilde{Q} \in \mathbb{Z}[X]$ avec $c(P)\tilde{P} = P$ et $c(Q)\tilde{Q} = Q$. Alors $c(\tilde{P}) = c(\tilde{Q}) = 1$; il suffit de montrer que $c(\tilde{P}\tilde{Q}) = 1$. Pour une contradiction, supposons que $c(\tilde{P}\tilde{Q}) \neq 1$.
Soit $p \in \mathbb{Z}$ premier avec $p \mid c(\tilde{P}\tilde{Q})$. Alors l'idéal $(p) = p\mathbb{Z}$ est premier et $\mathbb{Z}/p\mathbb{Z}$ est intègre (même un corps). On considère la projection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ et le morphisme induit

$$\bar{\pi} : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X], \qquad \sum_i a_i X^i \mapsto \sum_i (a_i + p\mathbb{Z})X^i,$$

la réduction modulo p.
Pour $R \in \mathbb{Z}[X]$ on a $\bar{\pi}(R) = 0$ si et seulement si $p \mid c(R)$. Donc $\bar{\pi}(\tilde{P}) \neq 0 \neq \bar{\pi}(\tilde{Q})$, mais $0 = \bar{\pi}(\tilde{P}\tilde{Q}) = \bar{\pi}(\tilde{P})\,\bar{\pi}(\tilde{Q})$, ce qui contredit l'intégrité de $(\mathbb{Z}/p\mathbb{Z})[X]$.
Ainsi $c(\tilde{P}\tilde{Q}) = 1$. □

Corollaire 6.11. Soit $P \in \mathbb{Z}[X]$ avec $c(P) = 1$. Alors P est irréductible dans $\mathbb{Z}[X]$ si et seulement si P est irréductible dans $\mathbb{Q}[X]$.

Démonstration. Soit P est irréductible dans $\mathbb{Q}[X]$, et considérons $Q, R \in \mathbb{Z}[X]$ avec $P = QR$. Alors Q ou R est inversible dans $\mathbb{Q}[X]$ et donc de degré zéro ; par symétrie on peut supposer que $Q \in \mathbb{Q}$. Mais $Q \in \mathbb{Z}[X]$ et donc $Q \in \mathbb{Z}$. Mais $|Q| = c(Q)$ divise $c(P) = 1$. Ainsi $Q = \pm 1$ est inversible dans $\mathbb{Z}$.
Réciproquement, soit P irréductible dans $\mathbb{Z}[X]$, et considérons $Q, R \in \mathbb{Q}[X]$ avec $P = QR$. En chassant les dénominateurs, on obtient $d \in \mathbb{N}^*$ et $\tilde{Q}, \tilde{R} \in \mathbb{Z}[X]$ avec $dP = \tilde{Q}\tilde{R}$. Alors $d = d\,c(P) = c(dP) = c(\tilde{Q})\,c(\tilde{R})$. Si $\hat{Q}, \hat{R} \in \mathbb{Z}[X]$ avec $c(\tilde{Q})\hat{Q} = \tilde{Q}$ et $c(\tilde{R})\hat{R} = \tilde{R}$, alors $P = \hat{Q}\,\hat{R}$. Par irréducibilité de P dans $\mathbb{Z}[X]$ soit $\hat{Q}$ soit $\hat{R}$ est inversible dans $\mathbb{Z}[X]$, donc dans $\mathbb{Q}[X]$. Ainsi P est irréductible dans $\mathbb{Q}[X]$. □

Exemple 6.12. Montrons que $P = X^4+X+1$ est irréductible dans $\mathbb{Q}[X]$. Puisque $P \in \mathbb{Z}[X]$ avec $c(P) = 1$, il suffit de montrer que P est irréductible dans $\mathbb{Z}[X]$. Supposons donc que $P = QR$ avec $\deg Q \leq \deg R$. Si $\deg Q = 0$, alors $Q \mid c(P) \sim 1$ et $Q = \pm 1$ est inversible. Si $\deg Q = 1$ alors $Q = aX + b$ avec $a, b \in \mathbb{Z}$, et a divise le coefficient dominant de P, et b divise le terme constant. Donc $Q = \pm X \pm 1$, mais ± 1 n'est pas racine de P, une contradiction. Enfin, si $\deg Q = 2$ on a $Q = aX^2 + bX + c$ et $R = a'X^2 + b'X + c'$, ce qui donne $aa' = 1$ et $cc' = 1$. On peut donc supposer que $a = a' = 1$ et $c = c' = \pm 1$. Or,

$$(X^2+bX+c)\,(X^2+b'X+c) = X^4+(b+b')X^3+(bb'+2c)X^2+c(b+b')X+1 = X^4+X+1,$$

ce qui donne $b + b' = 0$ mais $c(b + b') = 1$, une contradiction.

Ceci donne un critère utile d'irréducibilité.

Théorème 6.13 (Critère d'Eisenstein)**.** *Soit $P = \sum_{i=0}^{d} a_i X^i \in \mathbb{Z}[X]$ de degré d. Soit $p \in \mathbb{Z}$ premier tel que*
— *p divise $a_0, \ldots, a_{d-1}$,*

— *p ne divise pas a_d, et*
— *p^2 ne divise pas a_0.*

Alors P est irréductible dans $\mathbb{Q}[X]$.

Démonstration. On peut supposer que $c(P) = 1$, puisque $c(P)$ est inversible dans $\mathbb{Q}[X]$. Il suffit donc de montrer que P est irréductible dans $\mathbb{Z}[X]$. Supposons que $P = QR$ avec $Q, R \in \mathbb{Z}[X]$ non-constants. Soit $\bar{\pi} : \mathbb{Z}[X] \to ()\mathbb{Z}/p\mathbb{Z})[X]$ la réduction modulo (p). Alors $\bar{\pi}(a_k) = 0$ pour $k = 0, \dots, d-1$ et $\bar{\pi}(a_d) \neq 0$.
Soient $Q = \sum_{i=0}^{n} b_i X^i$ et $R = \sum_{i=0}^{d-n} c_i X^i$ avec $0 < n < d$. Alors $a_0 = b_0 c_0$, et donc soit $p \nmid b_0$ soit $p \nmid c_0$; par symétrie on peut supposer $p \nmid b_0$ et $\bar{\pi}(b_0) \neq 0$. Puisque $\bar{\pi}(b_n)\bar{\pi}(c_{d-n}) = \bar{\pi}(a_d) \neq 0$ et $\mathbb{Z}/p\mathbb{Z}$ est intègre, on peut choisir $k \leq d - n$ minimal avec $\bar{\pi}(c_k) \neq 0$. Alors

$$0 = \bar{\pi}(a_k) = \bar{\pi}\big(\sum_{i=0}^{k} b_i c_{k-i}\big) = \sum_{i=0}^{k} \bar{\pi}(b_i)\bar{\pi}(c_{k-i}) = \bar{\pi}(b_0)\bar{\pi}(c_k) \neq 0,$$

,puisque $\bar{\pi}(c_i) = 0$ pour $i < k$. Cette contradiction termine la démonstration. □

Exemple 6.14. Une réduction modulo 5 montre que $3X^4 + 15X^2 + 10$ est irréductible dans $\mathbb{Q}[X]$.

Exemple 6.15. Soit p premier, et $P(X) = 1 + X + \cdots + X^{p-1}$. On fait un changement de variable en posant $X = Y + 1$. Alors

$$P(X) = \frac{X^p - 1}{X - 1} = \frac{(Y+1)^p - 1}{Y} = \sum_{k=1}^{p} \binom{p}{k} Y^{k-1} = \sum_{k=0}^{p-1} a_k Y^k.$$

Alors $a_0 = p$, $a_{p-1} = 1$ et $p \mid a_k$ pour $k = 0, \dots, p-2$. D'après les critère d'Eisenstein $P(Y+1)$ est irréductible sur $\mathbb{Q}$, et sur $\mathbb{Z}$ puisque son contenu est 1. Le même vaut pour $P(X)$, bien sur.

Voici deux autres critères d'irréducibilité.

Proposition 6.16. *Soit $P \in \mathbb{Z}[X^*]$ avec $c(P) = 1$. Supposons qu'il y a un nombre premier p tel que $p \nmid cd(P)$ et P est irréductible modulo p. Alors P est irréductible sur $\mathbb{Z}$.*

Démonstration. Supposons que $P = QR$ avec $Q, R \in \mathbb{Z}[X]$. Soient $\bar{\pi}(P)\bar{P}$, $\bar{\pi}(Q) = \bar{Q}$ et $\bar{\pi}(R) = \bar{R}$ leurs réductions modulo p, ou $\bar{\pi} : \mathbb{Z}[X] \to (\mathbb{Z}/p\mathbb{Z})[X]$. Alors $\bar{P} = \bar{Q}\,\bar{R}$. On a $cd(P) = cd(Q)\,cd(R)$; puisque $p \nmid cd(P)$ on a $p \nmid cd(Q)$ et $p \nmid cd(R)$. Ainsi $\deg P = \deg \bar{P}$, $\deg Q = \deg \bar{Q}$ et $\deg R = \deg \bar{R}$.
Puisque $\bar{P} = \bar{Q}\,\bar{R}$ est irréductible, soit $\bar{Q}$ soit $\bar{R}$ est inversible dans $(\mathbb{Z}/p\mathbb{Z})[X]$, donc constant. Alors soit Q soit P est constant, divise $c(P) = 1$, et est inversible dans $\mathbb{Z}[X]$. Ainsi P est irréductible. □

Proposition 6.17. *Soit $P \in \mathbb{Z}[X]^*$ avec $c(P) = 1$. Supposons qu'il y a deux nombres premiers $p \neq q$ tels que*

- *ni p ni q divise $cd(P)$,*
- *P se factorise comme produit de deux polynômes irréductibles modulo p et modulo q, et*
- *si $\bar{\pi}_p P = Q_p R_p$ et $\bar{\pi}_q P = Q_q R_q$ sont ces factorisations, alors $\{\deg Q_p, \deg R_p\} \neq \{\deg Q_q, \deg R_q\}$.*

Alors P est irréductible sur $\mathbb{Z}$.

Démonstration. Supposons que $P = ST$ avec $S, T \in \mathbb{Z}[X]$ non-inversibles. Puisque $c(P) = 1$ ni S ni T sont constants. Ni p ni q divise $cd(P)$, et donc ne divise pas $cd(S)$ ni $cd(T)$ non plus. Ainsi $\deg P = \deg \bar{\pi}_p(P) = \deg \bar{\pi}_q(P)$, $\deg S = \deg \bar{\pi}_p(S) = \deg \bar{\pi}_q(S)$ et $\deg T = \deg \bar{\pi}_p(T) = \deg \bar{\pi}_q(T)$.
La décomposition de $\bar{\pi}_p(P)$ et $\bar{\pi}_q(P)$ en polynômes irréductibles est unique à association près d'après la proposition 5.33. Or, $\bar{\pi}_p(P) = \bar{\pi}_p(S)\,\bar{\pi}_p(T)$ et $\bar{\pi}_q(P) = \bar{\pi}_q(S)\,\bar{\pi}_q(T)$, et aucun de ces polynômes n'est constant. Il en découle que $\bar{\pi}_p(S)$ est associé à un de Q_p ou à R_p, et $\bar{\pi}_p(T)$ est associé à l'autre ; de même $\bar{\pi}_q(S)$ est associé à un de Q_q ou à R_q, et $\bar{\pi}_p(T)$ est associé à l'autre. Ainsi

$$\begin{aligned}\{\deg Q_p, \deg R_p\} &= \{\deg \bar{\pi}_p(S), \deg \bar{\pi}_p(T)\} = \{\deg S, \deg T\} \\ &= \{\deg \bar{\pi}_q(S), \deg \bar{\pi}_q(T)\} = \{\deg Q_q, \deg R_q\},\end{aligned}$$

une contradiction. □

Chapitre 2

Corps

7 Extensions, degré, caractéristique, corps premier

Définition 7.1. Un *corps* est un anneau commutatif unitaire tel que tout élémént a un inverse multiplicatif.

Donc dans un corps K on a $K^\times = K^* = K \setminus \{0\}$, le *groupe multiplicatif* du corps.

Exemple 7.2.
- Les corps bien connus $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$.
- Les corps finis $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, pour p premier.
- $\mathbb{Q}[i] = \mathbb{Q} \oplus \mathbb{Q}i$.
- Le corps $K(X) = \mathrm{frac}(K[X])$ des *fractions rationnelles*, qui est le corps des fractions de l'anneau des polynômes $K[X]$.

Par contre, $\mathbb{N}$ n'est pas un corps (manque d'inverses additifs et multiplicatifs), ni $\mathbb{Z}$ (manque d'inverses multiplicatifs), ni $\mathbb{Z}/n\mathbb{Z}$ avec n composé (diviseurs de zéro).

Définition 7.3. Soit L un corps. Un sous-anneau $K \leq L$ est un *sous-corps* si $a^{-1} \in K$ pour tout $a \in K^*$. De manière équivalente, une partie $K \subseteq L$ est un sous-corps si K^* est non-vide, et pour $a, b \in K$ on a $a - b \in K$ et $ab^{-1} \in K$ (si $b \neq 0$). Alors on dit aussi que L est une extension de K.

Définition 7.4. Soit $K \leq L$. Alors L est en particulier un K-espace vectoriel. On définit le *degré* de l'extension comme la dimension de L en tant que K-espace vectoriel, $[L : K] = \dim_K L$.

Exemple 7.5. On a $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$, $[\mathbb{Q}[i] : \mathbb{Q}] = 2$.

Lemme 7.6. *Soit K un corps. Si $(K_i : i \in I)$ est une famille de sous-corps, alors $\bigcap_{i\in I} K_i$ est un sous-corps. Si I est totalement ordonné et $(K_i : i \in I)$ est une chaîne de sous-corps, alors $\bigcup_{i\in I} K_i$ est un sous-corps.*

Démonstration. On sait qu'une intersection de sous-anneaux est un sous-anneau, et une réunion d'une chaîne de sous-anneaux est un sous-anneau. Or, chaque K_i contient 0 et 1, et donc $\bigcap_I K_i$ et $\bigcup_I K_i$ aussi. De plus, comme chaque K_i est clos par inverse multiplicatif, $\bigcap_I K_i$ et $\bigcup_I K_i$ le sont aussi. Ce sont donc des sous-corps. □

Théorème 7.7. *Soient $K \leq L \leq M$ des extensions de corps. Alors $[M : K]$ est fini si et seulement si $[M : L]$ et $[L : K]$ sont finis, et dans ce cas $[M : K] = [M : L]\,[L : K]$.*

Démonstration. Si $[L : K]$ est infini, alors une famille infinie K-libre dans L est une famille infinie K-libre dans L. Ainsi $[L : K]$ est infini.
Si $[M : L]$ est infini, alors une famille infinie L-libre dans M est K-libre, et donc $[M : K]$ est infini.
Supposons $[M : L] = n$ et $[L : K] = m$ avec des bases $(a_1, \ldots, a_n)$ et $(b_1, \ldots, b_m)$. Alors pour tout $a \in M$ il y a $k_1, \ldots, k_n \in L$ avec $a = \sum_{i=1}^{n} k_i a_i$, et pour tout $i = 1, \ldots, n$ il y a $k_{ij} \in K$ avec $k_i = \sum_{j=1}^{m} k_{ij} b_j$. Ainsi

$$a = \sum_{i=1}^{n} k_i a_i = \sum_{i=1}^{n} \sum_{j=1}^{m} k_{ij} b_j a_i.$$

Donc les $(a_i b_j : 1 \leq i \leq n,\ 1 \leq j \leq m)$ forment un ensemble générateur de M en tant que K-espace vectoriel, et$[M : K] \leq mn$. On veut montrer que cette famille est libre. Supposons donc que $k_{ij} \in K$ avec

$$0 = \sum_{i,j} k_{ij} a_i b_j = \sum_{i} \big(\sum_{j} k_{ij} b_j \big) a_i.$$

Puisque les $(a_i)_i$ sont libres sur L, on a $\sum_j k_{ij} b_j = 0$ pour tout $i = 1, \ldots, n$. Mais puisque les $(b_j)_j$ sont libres sur K, on a $k_{ij} = 0$ pour tout i, j. Ainsi $(a_i b_j)_{ij}$ est une base, et $[M : K] = mn$. □

Soit K un corps. On considère l'application

$$\phi : \mathbb{Z} \to K \quad \text{donné par} \quad n \mapsto \begin{cases} \underbrace{1_K + \cdots + 1_K}_{n \text{ fois}} & \text{si } n > 0, \\ 0 & \text{si } n = 0, \\ -\phi(-n) & \text{si } n < 0. \end{cases}$$

On vérifie facilement que c'est un morphisme d'anneaux. Alors $\mathbb{Z}/\ker\phi \cong \mathrm{im}\phi$. Puisque $\mathrm{im}\phi$ est un sous-anneau d'un corps et contient 1, il est intègre. Donc $\ker\phi$ est premier, et soit $\ker\phi = (0)$ et $\mathrm{im}\phi \cong \mathbb{Z}$, soit $\ker\phi = (p)$ pour un entier p premier et $\mathrm{im}\phi \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, un corps à p éléments. Dans le premier cas K contient également le corps des fractions de $\mathrm{im}\phi$, $\mathrm{frac}(\mathrm{im}\phi) \cong \mathrm{frac}(\mathbb{Z}) = \mathbb{Q}$.

Définition 7.8. Si $\ker\phi = (n)$ on dit que la *caractéristique* de K vaut n (qui est soit 0, soit un entier premier). On le note $\mathrm{car}(K) = n$. Le *corps premier* de K est le plus petit sous-corps de K ; c'est le corps engendré par 1_K. Si $\mathrm{car}(K) = p > 0$ il est isomorphe à $\mathbb{F}_p$; si $\mathrm{car}(K) = 0$ il est isomorphe à $\mathbb{Q}$.

Lemme 7.9. *Si $\mathrm{car}(K) = p > 0$, le groupe additif $(K, 0, +)$ est un groupe abélien d'exposant p (c'est-à-dire l'ordre de tout élément divise p) ; si $\mathrm{car}(K) = 0$ le groupe additif est un groupe abélien divisible (pour tout a et tout entier $n > 0$ il y a b avec $nb = a$) sans torsion (= élément non-trivial d'ordre fini).*

Démonstration. Si $\mathrm{car}(K) = p > 0$ alors $pa = \phi(p)a = 0$ pour tout $a \in K$. Réciproquement supposons que $a \in K^*$ soit un élément de torsion, disons $na = \phi(n)a = 0$. Alors $a \neq 0$ implique $\phi(n) = 0$, et $\mathrm{car}(K) \neq 0$.
Si $\mathrm{car}(K) = 0$, soit $n > 0$ un entier. Alors $\phi(n) \neq 0$ et pour tout $a \in K$ on a $n\,(\phi(n)^{-1}a) = \phi(n)\phi(n)^{-1}a = a$. Donc le groupe additif est divisible. □

8 Extensions simples, extensions algébriques, polynôme minimal

Définition 8.1. Soit $K \leq L$ une extension de corps, et $a \in L$. Alors $K(a)$ est le plus petit sous-corps de L contenant K et a. L'extension $K \leq L$ est *simple* s'il y a $a \in L$ avec $K(a) = L$. Dans ce cas on dit que L est *engendré* sur K par a.
L'élément $a \in L$ est *algébrique* sur K si $[K(a) : K] < \infty$, sinon il est transcendant. L'extension $K \leq L$ est *algébrique* si tout $a \in L$ est algébrique sur K.

Remarque 8.2. La notation $K(a)$ suppose que a est un élément dans une extension L de K qui est implicite.

Exemple 8.3. Les éléments $i, \sqrt{3}, 1 + i\sqrt{2}$ are algébriques sur $\mathbb{Q}$. Par contre, e et π sont transcendants sur $\mathbb{Q}$.

Exemple 8.4. Soit I un idéal maximal dans $K[X]$. Puisque $K[X]$ est principal, il y a un polynôme unitaire irréductible P tel que $I = (P)$, et $K[X]/(P)$ est une extension simple algébrique de K, engendré sur k par l'élément $X + (P)$.

La proposition suivante nous dit que toute extension algébrique simple est de cette forme.

Proposition 8.5. *Soit $K \leq K(a)$ une extension simple.*

1. *Si a est algébrique, alors il y a un unique polynôme unitaire irréductible $P \in K[X]$ tel que $P(a) = 0$. De plus,* $\deg P = [K(a) : K]$, *et $K(a) \cong K[X]/(P)$. On appelle P le* polynôme minimal *de a sur K. Les puissances $1, a, a^2, \ldots, a^{d-1}$ forment une K-base de $K(a)$.*
2. *Si a est transcendant, alors $K(a) \cong K(X) = \mathrm{frac}(K[X])$. Les puissances $1, a, a^2, \ldots$ forment une famille libre sur K. C'est une base de $K[a] \cong K[X]$, mais pas de $K(a)$.*

Démonstration. On considère l'évaluation en a, $\mathrm{eval}_a : K[X] \to K(a)$ donnée par $P(X) \mapsto P(a)$, un morphisme d'anneaux. Puisque $\mathrm{im}(\mathrm{eval}_a)$ est intègre, $I = \ker(\mathrm{eval}_a)$ est premier.
Supposons d'abord que $I = (0)$. Alors eval_a est un plongement de $K[X]$ dans $K(a)$ qui se prolonge en un plongement $\overline{\mathrm{eval}_a} : K(X) \to K(a)$. Or, $\mathrm{im}(\overline{eval_a})$ est une extension de K qui contient a ; on a ainsi $K(X) \cong K(a)$. Puisque $1, X, X^2, \ldots$ sont une K-base de

$K[X]$, leurs images $1, a, a^2, \ldots$ sont une K-base de $K[a]$. En particulier ils sont K-libres dans $K(a)$, d'où $[K(a) : K] = \infty$ et a est transcendant.
Sinon $I = (P)$ pour un polynôme non-constant irréductible, qu'on peut choisir unitaire. On a $P \in \ker \mathrm{eval}_a$, donc $P(a) = 0$. Puisque $K[X]$ est principal, l'idéal premier (P) est maximal, et $K[X]/(P)$ est un corps qui contient K comme sous-corps. Chaque polynôme $Q \in K[X]$ est congru modulo (P) à l'unique reste de la division euclidienne de Q par P, c'est-à-dire à un unique polynôme de degré $< \deg P = d$. Puisque $\mathrm{eval}_a(X) = a$, le sous-corps $\mathrm{im}(\mathrm{eval}_a) \leq K(a)$ contient a et on a égalité : $K(a) \cong K[X]/(P)$. Les polynômes $1, X, \ldots, X^{d-1}$ forment une K-base de $K[X]/(P)$, et donc leurs images $1, a, a^2, \ldots, a^{d-1}$ forment une K-base de $K(a)$. En particulier $[K(a) : K] = d$ et a est algébrique sur K. De plus, si $Q(a) = 0$ pour un $Q \in K[X]^*$, alors $Q \in \ker \mathrm{eval}_a) = (P)$ et donc $P \mid Q$. En particulier $\deg Q \geq \deg P$; en cas d'égalité Q est associé à P. Donc $P(X)$ est l'unique polynôme unitaire non-nul annulé par a ; c'est aussi l'unique polynôme unitaire de degré minimal annulé par a. □

Définition 8.6. Une extension $K \leq L$ est *algébrique* si $[K(a) : K] < \infty$ pour tout $a \in L$.

En particulier une extension de degré fini est algébrique. Attention, si L n'est pas engendré par un nombre fini d'éléments sur K, alors L peut être algébrique sur K sans que $[L : K]$ soit fini.

Lemme 8.7. *Soit $K \leq L \leq M$ des extensions de corps. Si $a \in M$ est tel que $[K(a) : K] \leq \infty$ alors $[L(a) : L] \leq [K(a) : K]$, et le polynôme minimal de a sur L divise le polynôme minimal de a sur K.*

Démonstration. Soit $P(X) \in K[X]$ le polynôme minimal de a sur K. Alors $P \in L[X]$, avec $P(a) = 0$. Si $Q \in L[X]$ est le polynôme minimal de a sur L, soit $R \in L[X]$ le reste de la division euclidienne de P par Q. Alors il y a $S \in L[X]$ avec $P = QS + R$, et $R(a) = P(a) - Q(a)S(a) = 0$. Par minimalité de $\deg Q$ on a $R = 0$ et $Q \mid P$. En particulier $[L(a) : L] = \deg Q \leq \deg P = [K(a) : K]$. □

Proposition 8.8. *Si $K \leq L$ et $L \leq M$ sont des extensions algébriques, $K \leq M$ est une extension algébrique.*

Démonstration. Soit $a \in M$. Alors $[L(a) : L] < \infty$. Soit $P(X) \in L[X]$ le polynôme minimal de a sur L, et $b_0, \ldots, b_d \in L$ les coefficients de P. On considère la suite d'extensions

$$K \leq K(b_0) \leq K(b_0, b_1) \leq \cdots \leq K(b_0, b_1, \ldots, b_d) \leq K(b_0, b_1, \ldots, b_k, a).$$

Pour tout $i < d$ on a

$$\begin{aligned}&[K(b_0, b_1, \ldots, b_i, b_{i+1}) : K(b_0, b_1, \ldots, b_i)] \\ &\qquad = [K(b_0, b_1, \ldots, b_i)(b_{i+1}) : K(b_0, b_1, \ldots, b_i)] \leq [K(b_{i+1}) : K] < \infty.\end{aligned}$$

De plus, $P \in K(b_0, b_1, \ldots, b_i)[X]$ et $P(a) = 0$, d'où

$$[K(b_0, b_1, \ldots, b_i)(a) : K(b_0, b_1, \ldots, b_i)] < \infty.$$

Pour $0 \leq i \leq d$ on pose $K_i = K(b_j : j \leq i)$. Alors

$$\begin{aligned}[K(a) : K] &\leq [K(b_0, b_1, \ldots, b_d)(a) : K] = [K_{\leq d}(a) : K] \\ &= [K_0 : K]\,[K_1 : K_0]\,[K_2 : K_1] \cdots [K_d : K_{d-1}]\,[K_d(a) : K_d] < \infty.\end{aligned}$$

Donc a est algébrique sur K, et $K \leq L$ est une extension algébrique. □

Corollaire 8.9. Soit $K \leq L$ une extension, et $\bar{K}^L = \{a \in L : \ a \text{ algébrique sur } K\}$. Alors $\bar{K}^L$ est un sous-corps de L contentant K.

Démonstration. K est algébrique sur K, donc $K \leq \bar{K}^L$. Si $a, b \in \bar{K}^L$ et $b \neq 0$, alors

$$[K(a, b) : K] = [K(a, b) : K(a)]\,[K(a) : K] < [K(b) : K]\,[K(a) : K] < \infty$$

et $a - b, ab^{-1} \in K(a, b)$. Donc $a - b, ab^{-1} \in \bar{K}^L$. □

On appelle $\bar{K}^L$ la *clôture algébrique relative* de K dans L.

Exemple 8.10.
— $\bar{Q} = \bar{Q}^{\mathbb{C}} = \{a \in \mathbb{C} : \ a \text{ algébrique sur } \mathbb{Q}\}$ est le *corps des nombres algébriques.*
— $\bar{Q}^{\mathbb{R}} = \{a \in \mathbb{R} : a \text{ algébrique sur } \mathbb{Q}\}$ est le *corps des nombres réels algébriques.*

9 Corps de rupture, corps de décomposition, clôture algébrique

Dans la section précédente, nous sommes partis d'une extension algébrique $K(a)$ et avons trouvé le polynôme minimal P de a sur K, avec $K(a) \cong K[X]/(P)$. Nous allons changer de perspective sur cette extension.

Définition 9.1. Soit K un corps et $P \in K[X]$ un polynôme irréductible non-constant. Le *corps de rupture* de P est une extension L minimale telle que P possède un zéro dans L (c'est-à-dire P possède un zéro dans L, mais pour tout $K \leq M < L$ il n'y a pas de zéro de P dans M). Il est unique à K-isomorphisme près, et isomorphe à $K[X]/(P)$.

Démonstration. $K[X]/(P)$ est une extension de K où P possède un zéro $X + (P)$. Si L est une extension quelconque où P possède un zéro a, alors $\bar{P} = P/\mathrm{cd}(P)$ est un polynôme sur K unitaire et irréductible annulé par a, et donc son polynôme minimal. On a $(P) = (\bar{P})$, et $K(a) \cong K[X]/(\bar{P}) = K[X]/(P)$, ce qui montre minimalité et unicité du corps de rupture. □

Corollaire 9.2. Soit K un corps et $P \in K[X]$ non-constant. Alors il y a une extension $L \geq K$ où P a un zéro.

Démonstration. P possède un facteur irréductible Q, et on peut prendre L le corps de rupture de Q. □

Lemme 9.3. *Soit $P \in K[X]$ de degré $d > 0$. Alors il y a une extension $L \geq K$ de degré $\leq d!$ telle que P possède d racines dans L (avec multiplicités).*

Démonstration. Par récurrence sur $\deg P$. Si $d = 1$, alors $P(X) = c(X - a)$ pour un $a \in K$ et $c \in K^*$. On peut donc prendre $L = K$.
On suppose donc le théorème vrai pour les polynômes (sur un corps quelconque) de degre d, et on considère $P \in K[X]$ de degré $d + 1$. Soit Q un facteur irréductible de P sur K, et soit $K(a)$ le corps de rupture de Q, où $Q(a) = 0$, avec $[K(a) : K] = \deg Q \leq \deg P = d + 1$. Alors P se factorise sur $K(a)$ comme $P = (X - a)R$, avec $\deg R = \deg P - 1 = d$. Par hypothèse de récurrence il y a une extension $L \geq K(a)$ de degré $\leq d!$ où R possède d racines. Alors $[L : K] = [L : K(a)]\,[K(a) : K] \leq d!\,(d+1) = (d + 1)!$, et P possède $d + 1$ racines dans L (avec multiplicités). □

Définition 9.4. Soit K un corps, $P \in K[X]$ un polynôme de degré $d > 0$. Une extension $L \geq K$ est un *corps de décomposition* de P si L contient d racines $a_1, \ldots, a_d$ de P (avec multiplicités) et $L = K(a_1, \ldots, a_d)$.

Le théorème précédent montre que tout polynôme admet un corps de décomposition.

Proposition 9.5. *Soit $\phi : K \to L$ un isomorphisme de corps, $\bar{\phi} : K[X] \to L[X]$ l'isomorphisme induit sur les anneaux de polynômes, $P \in K[X]$ non-constant et $\bar{\phi}(P) \in L[X]$ son image. Soit $K' \geq K$ un corps de décomposition de P et $L' \geq L$ un corps de décomposition de $\bar{\phi}(P)$. Alors ϕ se prolonge en un isomorphisme $\phi' : K' \to L'$, et ϕ' induit une bijection entre les racines de P dans K' et les racines de $\bar{\phi}(P)$ dans L'.*

Démonstration. Par récurrence sur $\deg P$. Si $\deg(P) = 1$ alors $P = c(X - a)$ est linéaire et possède déjà une unique racine a dans K ; de même $\bar{\phi}(P) = X - \phi(a)$ possède une unique racine $\phi(a) \in L$, et on prend $\phi' = \phi$.
On suppose donc que le théorème est vrai pour les polynômes de degré d, et on considère $P \in K[X]$ de degré $d+1$. Soit Q un facteur irréductible de P sur K. Alors $\bar{\phi}(Q)$ est un facteur irréductible de $\bar{\phi}(P)$. Soit $a_1 \in K'$ une racine de Q, et $b_1 \in L'$ une racine de $\bar{\phi}(Q)$. Alors l'isomorphisme ϕ se prolonge en un isomorphisme $\phi_1 : K(a_1) \cong K[X]/(Q) \to L[X]/(\bar{\phi}(Q)) \cong L(b_1)$.
On considère $R = P/(X - a_1) \in K(a_1)[X]$ de degré d. Alors

$$\bar{\phi}_1(R) = \bar{\phi}(P)/(X - \phi_1(a_1)) = \bar{\phi}(P)/(X - b_1).$$

Or, on vérifie facilement que K' est un corps de décomposition de R sur $K(a_1)$, et L' est un corps de décomposition de $\bar{\phi}_1(R)$ sur $L(b_1)$: ce sont des extensions minimales de $K(a_1)$ (resp. $K(b_1)$) qui contiennent toutes les racines de R (resp. $\bar{\phi}_1(R)$). Par hypothèse de récurrence il y a un isomorphisme $\phi' : K' \to L'$ qui prolonge ϕ_1, et donc ϕ. De plus ϕ' induit une bijection entre les racines de R dans K' et les racines de $\bar{\phi}(R)$ dans L' ; puisque $\phi'(a_1) = b_1$ il induit également une bijection entre les racines de P dans K' et les racines de $\bar{\phi}(P)$ dans L'. □

Corollaire 9.6. Le corps de décomposition est unique à K-isomorphisme près.

Démonstration. Dans la proposition 9.5 on prend $L = K$ et $\phi = \mathrm{id}_K$. □

Théorème 9.7. *Soit $\phi : K \to L$ un isomorphisme de corps, $P \in K[X]$ un polynôme non-constant et $\bar{\phi}(P) \in L[X]$ son image. Soit $K' \geq K$ le corps de décomposition de P et $L' \geq L$ le corps de décomposition de $\bar{\phi}(P)$. On suppose que P n'a que des racines simples. Soit $n = [K' : K]$. Alors il y a n prolongements $K' \to L'$ de ϕ.*

Démonstration. Par récurrence forte sur n. Pour $n = 1$ il n'y a rien à démontrer : on a $K = K'$ et $L = L'$, et ϕ est son propre prolongement unique. On suppose donc le théorème vrai pour des extensions de degré $< n$. Puisque $n > 1$ on a $K < K'$. Ainsi les racines de P ne sont pas tous dans K et P a un facteur irréductible Q de degré $d > 1$. Soit $a \in K'$ une racine de Q. Alors $\bar{\phi}(Q)$ a d racines distinctes $b_1, \ldots, b_d$ dans L', et il y a d plongements distincts $\phi_1, \ldots, \phi_d$ de $K(a_1)$ dans L' tel que $\phi_i(a_1) = b_i$. Chaque plongemet $K(a_1) \to L'$ est déterminé par l'image de a_1 ; comme il n'y a que d racines de $\bar{\phi}(Q)$ dans L' il n'y a pas d'autres possibilités.
Par hypothèse de récurrence chaque ϕ_i a $[K' : K(a)] = n/d$ prolongements en isomorphisme $K' \to L'$. Au total il y a donc $d \cot n/d = n$ prolongements de ϕ. □

Définition 9.8. Un corps est *algébriquement clos* s'il n'a aucune extension algébrique propre.

Remarque 9.9. De manière équivalente, K est algébriquement clos si tout polynôme sur K a un zéro dans K.

Démonstration. Si K a une extension algébrique propre L, alors le polynôme minimal de tout $a \in L \setminus K$ n'a pas de zéro dans K. Inversement, le corps de décomposition d'un polynôme $P \in K[X]$ sans zéro dans K est une extension algébrique propre. □

Exemple 9.10. Le corps complexe $\mathbb{C}$ et le corps des nombres algébriques $\bar{\mathbb{Q}}$ sont algébriquement clos.

Lemme 9.11. *Soit K un corps. Alors il y a une extension algébrique $L \geq K$ telle que tout polynôme $P \in K[X]$ non-constant a un zéro dans L.*

Démonstration. Soit $\{P_i : i \in I\}$ l'ensemble de tous les polynômes irréductibles sur K. On considère l'anneau $A = K[X_i : i \in I]$ des polynômes en variables $\{X_i : i \in I\}$, et l'idéal $J = (P_i(X_i) : i \in I)$.
Pour une contradiction, supposons que $J = A$. Alors $1 \in J$, et il y a $I_0 \in I$ fini et des polynômes $Q_i \in A$ pour $i \in I_0$ tel que $\sum_{i \in I_0} Q_i P_i(X_i) = 1$. Soit $I_0 \subseteq I_1 \subset I$ fini tel que $\{X_i : i \in I_1\}$ sont toutes les variables qui interviennent dans cette somme — c'est-à-dire dans les $(Q_i : i \in I_0)$, et tous les $(X_i : i \in I_0)$. Soit $K' \geq K$ le corps de décomposition de $\prod_{i \in I_0} P_i(X)$, et $a_i \in K'$ un zéro de P_i. Par la propriété universelle de l'anneau des polynômes, il y a un morphisme d'anneaux $\phi : K[X_i : i \in I_1] \to K'$ qui

fixe K et avec $\phi(X_i) = a_i$ pour $i \in I_0$ (et $\phi(X_i) = 0$ pour $i \in I_1 \setminus I_0$, ou un autre choix arbitraire). Alors

$$1 = \phi(1) = \phi(\sum_{i \in I_0} Q_i P_i(X_i)) = \sum_{i \in I_0} Q_i P_i(a_i) = 0,$$

la contradiction recherché.
Ainsi $J < A$ et il y a un idéal maximal $J \leq M \lhd A$. On considère le corps $L = A/M$. Comme $M \neq A$ aucun élément de K^* n'est dans M, et $a \mapsto a + M$ est un morphisme de K dans L de noyau trivial, donc une injection. Ainsi on peut supposer que L est une extension de K. Or, $P_i(X_i + M) = P_i(X_i) + M = M = 0_L$, et $X_i + M$ est un zéro de P_i dans L. On note que L est une extension algébrique sur K : Chaque $X_i + M$ est un zéro de P_i et donc algébrique sur K, et tout élément dans L est de la forme $Q + M$, où Q est un polynôme en un nombre fini de variables $X_{i_1}, \ldots, X_{i_n}$, et est donc dans $K(X_{i_1} + M, \ldots, X_{i_n} + M)$, ce qui est une extension de degré fini sur K. □

Lemme 9.12. *Soit K un corps. Il existe une extension L algébrique de K qui est algébriquement clos.*

Démonstration. D'après le lemme 9.11 il existe une suite $K = K_0 \leq K_1 \leq K_2 \leq \cdots$ d'extensions algébriques telle que tout polynôme non-constant sur K_i a un zéro dans K_{i+1}. On pose $L = \bigcup_{i \in \mathbb{N}} K_i$. Rappelons qu'une réunion d'une chaîne de corps est un corps. Alors L est une extension algébrique de K, puisque tout $a \in L$ est déja dans un K_i, qui est algébrique sur K.
Mais tout polynôme $P \in L[X]$ est déja dans $K_i[X]$ pour un i suffisamment grand, et a un zéro dans $K_{i+1} \leq L$. Ainsi L est algébriquement clos. □

Définition 9.13. Une extension algébrique algébriquement clos de K s'appelle une *clôture algébrique* de K, notée $\bar{K}$.

Remarque 9.14. La construction de la clôture algébrique nécessite le lemme de Zorn afin de trouver l'idéal maximal M contenant J dans la démonstration du lemme 9.11. Il pourrait donc surprendre que néanmoins le théorème suivant affirme l'unicité de la clôture algébrique, à K-isomorphisme près.

Théorème 9.15. *Chaque corps K a, à K-isomorphisme près, une unique extension algébrique algébriquement clos.*

Démonstration. On a vu l'existence dans le lemme 9.12. Montrons l'unicité. Soient donc $\bar{K}$ et $\bar{K}'$ deux extensions algébriques algébriquement clos de K. On considère la famille $\mathcal{X}$ des graphes des K-isomorphismes d'un sous-corps de $\bar{K}$ contenant K vers un sous-corps de $\bar{K}'$ contentant K, autrement dit

$$\mathcal{X} = \{\Gamma(\sigma) : \sigma \text{ isomorphisme}, K \leq \text{dom}\sigma \leq \bar{K}, K \leq \text{im}\sigma \leq \bar{K}'\} \subseteq \mathcal{P}(\bar{K} \times \bar{K}'),$$

où $\Gamma(\sigma)$ est le graphe de σ, et $\mathcal{P}(Z)$ l'ensemble des parties de Z. On ordonne $\mathcal{X}$ par inclusion, et on note que $\Gamma(\sigma) \subseteq \Gamma(\sigma')$ ssi σ' prolonge σ.

Si $(\Gamma(\sigma_i) : i \in I)$ est une chaîne dans X, alors $\bigcup_{i\in I} \Gamma(\sigma_i)$ est encore le graphe d'un K-isomorphisme de $\bigcup_{i\in I} \mathrm{dom}(\sigma_i)$ vers $\bigcup_{i\in I} \mathrm{im}(\sigma_i)$ qui prolonge tous les σ_i et majore la chaîne. $\mathcal{X}$ est donc inductif, et par le lemme de Zorn admet un élément $\Gamma(\sigma)$ maximal. Soit $K_0 = \mathrm{dom}(\sigma)$ et $K_0' = \mathrm{im}(\sigma)$. Alors $K \leq K_0 \leq \bar{K}$ et $K \leq K_0' \leq \bar{K}'$.
Supposons pour une contradiction que $K_0 < \bar{K}$, et soit $a \in \bar{K} \setminus K_0$. Alors a est algébrique sur K, donc sur K_0 ; soit $P \in K_0[X]$ son polynôme minimal, de degré ≥ 2. Alors $\bar{\sigma}(P) \in K_0'[X]$ est aussi irréductible, et doit avoir un zéro b dans $\bar{K}'$. Mais σ se prolonge en un isomorphisme $K_0(a) \cong K_0[X]/(P) \to K_0'[X]/(\bar{\sigma}(P)) \cong K_0'(b)$, ce qui contredit la maximalité de σ. Ainsi $K_0 = \bar{K}$.
Si $K_0' < \bar{K}'$, on considère $b \in \bar{K}' \setminus K_0'$, son polynôme minimal Q sur K_0', et un zéro a de $\bar{\sigma}^{-1}(Q) \in K_0[X]$. Alors $K_0(a) \cong K_0[X]/(\bar{\sigma}^{-1}(Q)) \to K_0'[X]/(Q) \cong K_0'(b)$ est un prolongement propre de σ, une contradiction. Donc $K_0' = \bar{K}'$ et σ est le K-isomorphisme recherché. □

Remarque 9.16. Soit L une extension algébrique de K. Alors $\bar{L} = \bar{K}$.

Démonstration. Si $a \in \bar{L}$ alors $L(a)$ est agébrique sur L et L est algébrique sur K, donc $L(a)$ est algébrique sur K, et $\bar{L}$ est algébrique sur K. De plus, $\bar{L}$ est algébriquement clos. Donc $\bar{L}$ est la clôture algébrique de K. □

10 Anneaux des polynômes sur un corps

Soit K un corps et $K[X]$ son anneau de polynômes. Alors $K[X]$ est un espace vectoriel sur K avec base $1, X, X^2, \ldots$, donc de dimension dénombrable.

Définition 10.1. Soit $P(X) = \sum_i a_i X^i \in K[X]$. Alors P induit la *fonction polynomiale* $\hat{P} : K \to K$ donné par $x \mapsto \sum_i a_i x^i$.

Remarque 10.2. Il est facile de voir que $\widehat{P \pm Q} = \hat{P} \pm \hat{Q}$ et $\widehat{PQ} = \hat{P}\,\hat{Q}$.

Définition 10.3. Soit $P \in K[X]$. Un élément $a \in K$ est un *zéro*, ou une *racine* de P si $\hat{P}(a) = 0$.

Proposition 10.4. *Un élément $a \in K$ est un zéro d'un polynôme $P \in K[X]$ si et seulement si $X - a$ divise P.*

Démonstration. Si $P = 0$ il n'y a rien a démontrer. On suppose donc $P \neq 0$, et on effectue la division euclidienne de P par $X - a$. Alors il y a $Q, R \in K[X]$ avec $\deg R < \deg(X - a) = 1$ tel que $P = (X - a)\,Q + R$. Or, $0 = P(a) = 0 + R(a)$ et $R = R(a)$ est une constante, d'où $R = 0$ et $(X - a)$ divise P. Réciproquement, si $P = (X - a)\,Q$, alors $P(a) = 0$. □

Proposition 10.5. *Soit $P \in K[X]$ de degré $d \geq 0$. Alors P a au plus d racines distinctes.*

Démonstration. Par récurrence sur d. Si $\deg P = 0$, alors p est une constante non-nulle et n'a pas de zéro. Si $\deg(P) = 1$, alors $p = aX + b$ pour $a \in K^\times$ et $b \in K$, et a un seul zéro $-b/a$. Supposons donc l'énoncé vrai pour les polynômes de degré d, et considérons $P \in K[X]$ de degré $d+1$. Si P n'a aucun zéro dans K, l'énoncé est satisfait. Sinon, soit $a \in K$ un zéro de P. Alors il y a $Q \in K[X]$ non-nul avec $P = (X-a)\,Q$, et $\deg(Q) = \deg(P) - 1 = d$. Par hypothèse de récurrence Q a au plus d zéros dans K. Mais un zéro de P est soit a, soit un zéro de Q. Ainsi P a au plus $d+1$ zéros dans K. □

Corollaire 10.6. La fonction $P \mapsto \hat{P}$ est injective si et seulement si K est infini.

Démonstration. Si K est fini, il y a au plus $|K|^{|K|}$ fonctions $K \to K$, mais une infinité de polynômes, à savoir $1, X, X^2, \ldots$. D'après le principe des tiroirs il y a deux polynômes $P, Q \in K[X]$ avec $\hat{P} = \hat{Q}$.
Si K est infini et $\hat{P} = \hat{Q}$, alors $\widehat{P-Q} = \hat{P} - \hat{Q}$ s'annule sur K entier. Donc le polynôme $P - Q$ a une infinité de zéros, et doit être 0. □

Définition 10.7. Soit $P \in K[X]$ non-nul. Un élément $a \in K$ est une racine d'*ordre* (ou de *multiplicité*) au moins n si $(X-a)^n$ divise P. C'est une racine d'ordre (exactement) n si a est ne racine d'ordre au moins n, mais pas une racine d'ordre au moins $n+1$.

Définition 10.8. Un polynôme $P \in K[X]$ non-nul est scindé si P se factorise sur K en facteurs linéaires.

Proposition 10.9. *Soit $P \in K[X]$ non-nul scindé. Alors P a précisément* $\deg(P)$ *racines, comptées avec leurs multiplicités.*

Démonstration. Puisque P est scindé, il y a $k \in \mathbb{N}^*$, $a_i \in K$ et $d_i \in \mathbb{N}^*$ pour $i \leq k$ tels que

$$P(X) = cd(P) \prod_{i \leq k} (X - a_i)^{d_i}$$

avec $\sum_{i \leq k} d_i = \deg P$. Or, un facteur linéaire est irréductible et deux facteurs linéaires unitaires distincts sont premiers entre eux. La proposition en découle. □

Remarque 10.10. Un polynôme $P \in K[X]$ est toujours scindé sur la clôture algébrique $\bar{K}$.

Définition 10.11 (Fonctions symétriques)**.** Soit A un anneau et $n \in \mathbb{N}^*$. Les fonctions symétriques en n variables sont les polynômes suivantes dans $A[X_1, \ldots, X_n]$:

$$\begin{aligned}
\sigma_1(X_1,\dots,X_n) &= \sum_{i=1}^{n} X_i\,;\\
\sigma_2(X_1,\dots,X_n) &= \sum_{1\le i<j\le n} X_iX_j\,;\\
\sigma_3(X_1,\dots,X_n) &= \sum_{1\le i<j<k\le n} X_iX_jX_k\,;\\
&\vdots\\
\sigma_j(X_1,\dots,X_n) &= \sum_{1\le i_1<i_2<\cdots<i_j\le n}\ \prod_{\ell=1}^{j} X_{i_\ell}\,;\\
&\vdots\\
\sigma_n(X_1,\dots,X_n) &= \prod_{i=1}^{n} X_i.
\end{aligned}$$

Remarque 10.12. Les fonctions symétriques sont invariants par permutations des variables. C'est-à-dire, si $\sigma \in \mathrm{Sym}(n)$, alors $\sigma_j(X_1,\cdots,X_n) = \sigma_j(X_{\sigma(1)},\dots,X_{\sigma(n)})$.

Remarque 10.13. Tout polynôme dans $A[X_1,\dots,X_n]$ invariant par permutation des varaibales est un polynôme en les fonctions symétriques. Par exemple $X_1^2 + X_2^2 = \sigma_1^2(X_1,X_2) - 2\sigma_2(X_1,X_2)$.

Proposition 10.14 (Relations coefficients-racines)**.** *Soit $P \in K[X]$ scindé sur K. Disons*

$$P(X) = \sum_{i=0}^{d} a_iX^i = a_d\prod_{j=1}^{d}(X-b_j).$$

Alors pour $j = 1,\dots,d$ on a

$$\frac{a_{d-j}}{a_d} = (-1)^j\sigma_j(b_1,\dots,b_d).$$

Démonstration. Simple calcul. □

Définition 10.15. Soient $P,Q \in K[X]$. Si $P(X) = \sum_i a_iX^i$, on pose la *substitution* (ou *composition*)

$$(P\circ Q)(X) = \sum_i a_iQ(X)^i.$$

On a $\widehat{Q\circ P} = \hat{Q}\circ\hat{P}$.

Remarque 10.16. L'application $P \mapsto P\circ Q$ est linéaire, mais $Q \mapsto P\circ Q$ ne l'est pas.

Définition 10.17. Soit $P(X) = \sum_{i=0}^{d} a_iX^i \in K[X]$. Le polynôme dérive de P est le polynôme

$$P'(X) = \sum_{i=0}^{d} i\,a_iX^{i-1}.$$

On note que le premier terme dans la somme a un coéfficient zéro. P' est donc un polynôme.

Remarque 10.18. Dans $\mathbb{R}[X]$ la dérivation des polynômes coincide avec la dérivation habituelle des fonctions réelles. Mais la dérivation des polynômes est défini sur tout corps de base, et ne fait pas appel à une notion de limite ou de continuité.

Proposition 10.19 (Propriétés de la dérivation)**.** *Soient $P, Q \in K[X]$. On a*

$$(P \pm Q)' = P' \pm Q', \quad (PQ)' = P'Q + PQ' \quad \textit{et} \quad (P \circ Q)' = (P' \circ Q)\, Q'.$$

Démonstration. Il est évident de la définition que $P \mapsto P'$ est linéaire. Puisque le produit et la substitution sont linéaires en P, il suffit de vérifier les propriétés pour des monômes $P(X) = X^n$. Soit $Q(X) = \sum_{i=0}^{d} a_i X^i$. On a

$$\begin{aligned}(PQ)' = \big(X^n \sum_{i=0}^{d} a_i X^i\big)' = \big(\sum_{i=0}^{d} a_i X^{n+i}\big)' = \sum_{i=0}^{d} (n+i)\, a_i X^{n+i-1} \\ = nX^{n-1} \sum_{i=0}^{d} a_i X^i + X^n \sum_{i=0}^{d} i\, a_i X^{i-1} = (X^n)'\, Q + X^n\, Q' = P'Q + PQ'.\end{aligned}$$

On démontre la dernière formule par récurrence sur n. Si $n = 0$, alors $P \circ Q = 1$ et $P' = 0$, ce qui donne $(P \circ Q)' = 0 = 0 \cdot Q = (P' \circ Q)\, Q$. Si $n = 1$ on a $P' = 1$ et $(P \circ Q)' = Q' = 1 \cdot Q' = (P' \circ Q)\, Q'$.
Supposons donc la formule vraie pour n, et considérons $P(X) = X^{n+1}$. Alors

$$\begin{aligned}(P \circ Q)' = (Q^{n+1})' = (Q\, Q^n)' = Q'\, Q^n + Q\, (Q^n)' = Q'\, Q^n + Q\, (X^n \circ Q)' \\ = Q'\, Q^n + Q\, (nX^{n-1} \circ Q)\, Q' = Q^n Q' + nQ^n Q' = (n+1) Q^n\, Q' \\ = \big((X^n)' \circ Q\big)\, Q' = (P' \circ Q)\, Q'. \quad \square\end{aligned}$$

Proposition 10.20 (Formule de Taylor)**.** *Soit $P \in K[X]$ et $\deg P \leq n < \operatorname{car}(K)$. Alors*

$$P(X) = \sum_{i=0}^{n} \frac{P^{(i)}(a)}{i!} (X - a)^i.$$

Démonstration. Par linéarité, il suffit de montrer la formule pour $P(X) = X^d$ avec $d \leq n$. Alors $P^{(i)}(a) = d\,(d-1) \cdots (d-i+1)\, a^{d-i}$, et

$$\sum_{i=0}^{n} \frac{P^{(i)}(a)}{i!} (X-a)^i = \sum_{i=0}^{d} \binom{d}{i} a^{d-i} (X-a)^i = (a + X - a)^d = X^d. \quad \square$$

Proposition 10.21 (Formule de Leibnitz)**.** *Soient $P, Q \in K[X]$. Alors*

$$(PQ)^{(n)} = \sum_{i=0}^{n} \binom{n}{i} P^{(i)} Q^{(n-i)}.$$

Démonstration. Par récurrence sur n. La formule est vraie pour $n = 0$ (trivial) et $n = 1$ (proposition 10.19). Supposons qu'elle est vraie pour n. Alors

$$\begin{aligned}
(PQ)^{(n+1)} &= \big((PQ)^{(n)}\big)' = \big(\sum_{i=0}^{n} \binom{n}{i} P^{(i)}Q^{(n-i)}\big)' = \sum_{i=0}^{n} \binom{n}{i} (P^{(i)}Q^{(n-i)})' \\
&= \sum_{i=0}^{n} \binom{n}{i} (P^{(i+1)}Q^{(n-i)} + P^{(i)}Q^{(n-i+1)}) \\
&= \sum_{i=0}^{n} \binom{n}{i} P^{(i+1)}Q^{(n-i)} + \sum_{i=0}^{n} \binom{n}{i} P^{(i)}Q^{(n-i+1)} \\
&= P^{(n+1)}Q + \sum_{i=0}^{n-1} \binom{n}{i} P^{(i+1)}Q^{(n-i)} + \sum_{i=1}^{n} \binom{n}{i} P^{(i)}Q^{(n-i+1)} + PQ^{(n+1)} \\
&= P^{(n+1)}Q + \sum_{i=1}^{n} \binom{n}{i-1} P^{(i)}Q^{(n+1-i)} + \sum_{i=1}^{n} \binom{n}{i} P^{(i)}Q^{(n-i+1)} + PQ^{(n+1)} \\
&= P^{(n+1)}Q + \sum_{i=1}^{n} (\binom{n}{i-1} + \binom{n}{i}) P^{(i)}Q^{(n+1-i)} + PQ^{(n+1)} \\
&= P^{(n+1)}Q + \sum_{i=1}^{n} \binom{n+1}{i} P^{(i)}Q^{(n+1-i)} + PQ^{(n+1)} \\
&= \sum_{i=0}^{n+1} \binom{n+1}{i} P^{(i)}Q^{(n+1-i)}. \quad \square
\end{aligned}$$

Proposition 10.22. *Soit $P \in K[X]$ non-nul, et $a \in K$. Si a est zéro de P d'ordre au moins n, alors*

$$P(a) = P'(a) = \cdots = P^{(n-1)}(a) = 0.$$

Si $\mathrm{car}(K) > \deg(P)$*, la réciproque est vraie.*

Démonstration. Supposons que $P(X) = (X-a)^n Q(X)$ pour un $Q \in K[X]$. On note que pour $k \leq n$ on a

$$\big((X-a)^n\big)^{(k)} = n\,(n-1)\cdots(n-k+1)(X-a)^{n-k}.$$

Ainsi pour $k < n$ on a

$$\begin{aligned}
P^{(k)}(X) &= \sum_{i=0}^{k} \binom{k}{i} \big((X-a)^n\big)^{(i)} Q^{(k-i)} \\
&= \sum_{i=0}^{k} \binom{k}{i} n\,(n-1)\cdots(n-i+1)(X-a)^{n-i} Q^{(k-i)}
\end{aligned}$$

et donc $P^{(k)}(a) = 0$.

Réciproquement, supposons que $P(a) = P'(a) = \cdots = P^{(n-1)}(a) = 0$ et $n \leq \deg P < \operatorname{car} K$. Alors

$$P(X) = \sum_{i=0}^{d} \frac{P^{(i)}(a)}{i!}(X-a)^i = (X-a)^n \sum_{i=n}^{d} \frac{P^{(i)}(a)}{i!}(X-a)^{i-n}$$

et $(X-a)^n$ divise P. □

Remarque 10.23. En caractéristique $p > 0$ on a $(X^p)' = pX^{p-1} = 0$. Donc la dérivée peut s'annuler sans que le polynôme soit constant.