

Anneaux et Corps

Frank Wagner

Table des matières

1	Anneaux	3
1	Anneaux, sous-anneaux et idéaux	3
2	Morphismes et anneau quotient	5
3	Ideaux	7
4	Inversibilité, anneaux intègres	10
5	Divisibilité, anneaux principaux	13
6	Anneaux factoriels	18
7	Anneaux de polynômes	21
2	Corps	24
8	Extensions, degré, caractéristique, corps premier	24
9	Extensions simples, extensions algébriques, polynôme minimal	26
10	Corps de rupture, corps de décomposition, clôture algébrique	28
11	Anneaux des polynômes sur un corps	31
12	Corps finis et polynômes cyclotomiques	36
13	Corps des nombres constructibles à la règle et au compas	39

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

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

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 vérifie 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. $\square$

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

Définition 1.8. Une partie non-vide $B \subseteq A$ est un *sous-anneau* si B est un sous-groupe additif, et clos par multiplication. C'est-à-dire, si $a, b \in B$ alors $a - b \in B$ et $ab \in B$. On note $B \leq A$.

Un sous-anneau $B \leq A$ est un *idéal à gauche* si $ab \in B$ pour tout $a \in A$ et $b \in B$. C'est un *idéal à droite* si $ba \in B$ pour tout $a \in A$ et $b \in B$, et un idéal (bilatère) si c'est à la fois un idéal à gauche et à droite. On le note $I \trianglelefteq A$.

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

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

Soient X et Y deux parties de A .

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

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

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

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

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

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

Exercice 1.14. Classifier tous les anneaux de cardinal 3.

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

2 Morphismes et anneau quotient

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

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

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

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

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

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

Définition 2.2. Soient A et B deux anneaux. Un homomorphisme de groupes additifs $f : A \rightarrow B$ est un *morphisme d'anneau* si $f(aa') = f(a)f(a')$ pour tout $a, a' \in A$. Si f est bijectif, alors f est un isomorphisme (d'anneaux). Si de plus $A = B$, alors f est un automorphisme (d'anneaux).

Remarque 2.3. Il est clair que l'image $\text{im} f$ est un sous-anneau de B .

Exemple 2.4. Les applications suivantes sont des morphismes d'anneau.

1. Si A est commutatif et $a \in A$, l'application

$$f_a : A[X] \rightarrow A, \quad P \mapsto P(a).$$

2. Si A et B sont deux anneaux, l'application

$$\pi : A \times B \rightarrow A, \quad (a, b) \mapsto a.$$

3. Si A et B sont deux anneaux, l'application

$$\iota : A \rightarrow A \times B, \quad a \mapsto (a, 0).$$

Cependant, si A et B sont unitaires, $A \times B$ l'est aussi avec unité $(1, 1)$, mais $f(1) = (1, 0) \neq (1, 1)$.

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

Définition 2.5. Soit $f : A \rightarrow B$ 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 2.6. Soit $f : A \rightarrow B$ un morphisme d'anneau. Alors $\ker f$ est un idéal dans A , et $\text{im} f \cong A/\ker f$.

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 droite 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 $\text{im} f$. Elle préserve la multiplication. C'est donc un isomorphisme d'anneaux. $\square$

Remarque 2.7. Si A est unitaire, alors $\text{im} f$ est un sous-anneau unitaire de B , mais son unité $f(1_A)$ n'est pas forcément unité de B .

Théorème 2.8. Soient A et B deux anneaux, $f : A \rightarrow B$ un morphisme d'anneaux, et $I \trianglelefteq A$ un idéal de A . Soit $\pi : A \rightarrow A/I$ la projection canonique. Alors il y a un morphisme $g : A/I \rightarrow B$ tel que $f = g \circ \pi$ si et seulement si $I \leq \ker f$.

Démonstration. S'il y a $g : A/I \rightarrow B$ 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 $g : A/I \rightarrow B$ est bien défini, et pour tout $a \in A$ on a bien $(g \circ \pi)(a) = g(a + I) = f(a)$, d'où $f = g \circ \pi$. $\square$

3 Ideaux

Proposition 3.1. Soit A un anneau, et $\{I_s : s \in S\}$ une collection d'idéaux de A .

1. L'intersection $I = \bigcap_{s \in S} I_s$ est un idéal de A .
2. Si pour tous $s, s' \in S$ on a soit $I_s \subseteq I_{s'}$ soit $I_{s'} \subseteq I_s$ (on dit que les $\{I_s : s \in S\}$ forment une chaîne), alors $J = \bigcup_{s \in S} I_s$ est un idéal de A .

Démonstration. 1. On a $0 \in I_s$ pour tout $s \in S$, d'où $0 \in I$. Si $a, a' \in I$ et $b \in A$, alors $a, a' \in I_s$ pour tout $s \in S$; puisque les I_s sont des idéaux, on a $a - a', ba, ab \in I_s$ pour tout $s \in S$, et $a - a', ba, ab \in I$. Ainsi I est un idéal.

2. Puisque la chaîne n'est pas vide, il y a un I_s , et $0 \in I_s \subseteq J$. Si $a, a' \in J$ et $b \in A$, alors il y a $s, s' \in S$ avec $a \in I_s$ et $a' \in I_{s'}$. On peut supposer que $I_{s'} \subseteq I_s$. Alors $a, a' \in I_s$, et donc $a - a', ba, ab \in I_s \subseteq J$. Ainsi J est un idéal de A . $\square$

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

Définition 3.2. Soit A un anneau commutatif, 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* s'il n'y a pas d'idéal J avec $I < J < A$.

Théorème 3.3. Soit A un anneau commutatif, et $I \trianglelefteq A$ un idéal.

1. I est premier si et seulement si A/I est intègre.
2. I est maximal si et seulement si A/I est un corps.

Démonstration. 1. Soit I premier, et $a, a' \in A$ avec $(a + I)(a' + I) = 0 + I$. Alors $ab + I = (a + I)(a' + I) = I$ et $ab \in I$. Puisque I est premier, soit $a \in I$ et $a + I = 0 + I$, soit $b \in I$ et $b + I = 0 + I$. 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 $b + I = 0 + I$ et $b \in I$. Ainsi I est premier.

2. Soit I maximal. Si $a + I \neq 0 + I$, alors $a \notin I$ et l'idéal $(I, a) = I + aA$ proprement contient I . Par maximalité de I on a $I + aA = A$. Il y a donc $c \in I$ et $e \in A$ avec $c + ae = a$. Ainsi $(a + I)(e + I) = a - c + I = a + I$. De même, pour tout $a' \in A$

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

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

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

Réciproquement, soit A/I un corps. Si J est un idéal de A avec $I \leq J \leq A$, alors J/I est un idéal de A/I . Mais un corps K n'a aucun idéal autre que (0) et K : Si I' est un idéal non-zéro, soit $0 \neq a \in I'$. Alors pour tout $b \in K$ on a $b = ba^{-1}a \in I'$ et $I' = K$. Il en suit que $J = A$. $\square$

Corollaire 3.4. Un idéal maximal est premier.

Démonstration. Si I est maximal, A/I est un corps, donc intègre, et I est premier. $\square$

Théorème 3.5. Soit A un anneau unitaire et $I \triangleleft A$ un idéal propre. Alors I est contenu dans un idéal maximal.

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

Définition 3.6. Un ensemble X avec une relation binaire $\leq$ est un *ordre partiel* si $\leq$ est *réflexif* (c'est-à-dire $x \leq x$ pour tout $x \in X$), *antisymétrique* (c'est-à-dire $x \leq x'$ et $x' \leq x$ implique $x = x'$) et *transitif* (c'est-à-dire $x \leq x'$ et $x' \leq x''$ implique $x \leq x''$). Un élément $x \in X$ est *maximal* si $x \leq x'$ implique $x' = x$ pour tout $x' \in X$, c'est-à-dire aucun élément de X est strictement plus grand (mais il peut y avoir des éléments incomparables avec x).

Une partie Y de X est une *chaîne* si Y est totalement ordonnée par $\leq$, c'est-à-dire pour tout $y, y' \in Y$ on a $y \leq y'$ ou $y' \leq y$. L'ordre partiel sur X est *inductif* si toute chaîne Y a un *majorant* dans X , c'est à dire un élément $x \in X$ tel que $y \leq x$ pour tout $y \in Y$. On ne demande pas que $x \in Y$.

Exemple 3.7. Soit E un ensemble, et $X = \mathcal{P}(E)$, l'ensemble des parties de E . Alors $\subseteq$ est un ordre partiel sur X . Si $\mathcal{Y}$ est une chaîne, alors $\bigcup \mathcal{Y} = \bigcup_{Y \in \mathcal{Y}} Y$ est un majorant pour $\mathcal{Y}$. Donc l'ordre est inductif.

Fait 3.8 (Lemme de Zorn). *Tout ordre partiel inductif 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 3.5. Soit $\mathcal{X} = \{J \triangleleft A : I \leq J\}$ l'ensemble des idéaux propres de A contenant I , ordonné partiellement par inclusion $\subseteq$. Notons qu'un idéal $J \triangleleft A$ est propre si et seulement si $1 \notin J$: Si $1 \in J$, alors pour tout $a \in A$ on a $a \cdot 1 \in J$ et $J = A$. Réciproquement, si $1 \notin J$ alors $J \neq A$.

Soit $\mathcal{C}$ une chaîne non-vidue dans $\mathcal{X}$. Alors $\bigcup \mathcal{C}$ est un idéal dans A contenant I majorant $\mathcal{C}$; puisque $1 \notin J$ pour tout $J \in \mathcal{C}$ on a $1 \notin \bigcup \mathcal{C}$ et $\bigcup \mathcal{C} \in \mathcal{X}$. Ainsi $\mathcal{X}$ est inductif et possède un élément maximal d'après le lemme de Zorn, c'est-à-dire un idéal propre maximal. $\square$

Exemple 3.9. Soit A l'anneau des polynômes sur $\mathbb{Z}$ sans terme constant en variables $X, X^{1/2}, X^{1/4}, \dots, X^{1/2^n}, \dots$, avec bien sur $(X^{1/2^{n+1}})^2 = X^{1/2^n}$ pour tout $n \in \mathbb{N}$. 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 $I_0 \leq I \triangleleft A$ avec I maximal, alors A/I est un corps. 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 $a \in I_n \setminus I$. Alors $a^2 \in I_{n-1} \leq I$. Comme I est maximal, il est premier, et $a \in I$, une contradiction. Donc I_0 n'est pas contenu dans un idéal maximal.

Définition 3.10. 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 $IJ = \langle ab : a \in I, b \in J \rangle_+$.

Remarque 3.11. — Si I et J sont des idéaux à gauche/droite, $I + J$ aussi.

- Si I est un idéal à gauche et X un ensemble quelconque, $\langle ab : a \in I, b \in X \rangle_+$ est un idéal à gauche.
- Si J est un idéal à droite et X un ensemble quelconque, $\langle ab : a \in X, b \in J \rangle_+$ est un idéal à droite.
- Si I est un idéal à gauche et J un idéal à droite, $\langle ab : a \in I, b \in J \rangle_+$ est un idéal (bilatère).

Remarque 3.12. 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.

Définition 3.13. Soit A un anneau. Deux idéaux I et J sont *étrangers* (ou *premiers entre eux*) si $I + J = A$.

Proposition 3.14. Soit A un anneau unitaire, et I, J deux idéaux étrangers. Alors $IJ + JI = I \cap J$.

Démonstration. Puisque I et J sont des idéaux, on a $IJ \leq I, IJ \leq J, JI \leq I$ et $JJ \leq J$. Ainsi $IJ + JI \leq I \cap J$.

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 $a = (i + j)a = ia + ja \in IJ + JI$, d'où $I \cap J \leq IJ + JI$ et on a égalité. $\square$

Théorème 3.15 (Théorème des restes chinois). Soit A un anneau unitaire, et $I_1, \dots, I_n$ des idéaux deux-à-deux étrangers. Alors le morphisme d'anneaux

$$\varphi : A/(I_1 \cap \dots \cap I_n) \rightarrow A/I_1 \times \dots \times A/I_n, \quad x + (I_1 \cap \dots \cap I_n) \mapsto (x + I_1, \dots, x + I_n)$$

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 $I = I_1 \cap \dots \cap I_n$. 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 $1 = \prod_{k=1}^n (i_k + j_k) \in i_1 i_2 \dots i_n + J \subseteq I + J$. Donc I et J sont étrangers. On considère donc

$$A/(I_1 \cap \dots \cap I_n \cap J) = A/(I \cap J) \rightarrow A/I \times A/J \rightarrow A/I_1 \times \dots \times A/I_n \times A/J;$$

d'après l'hypothèse de récurrence il suffit de montrer que $\varphi : A/(I \cap J) \rightarrow A/I \times A/J$ 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 $z \equiv a_k \pmod{I_k}$ pour $k = 1, \dots, n$, alors l'ensemble des solutions est précisément $z_0 + (I_1 \cap \dots \cap I_n)$.

Exemple 3.16. 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 $x \equiv a_i \pmod{n_i}$ 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. □

Dans un anneau euclidien comme $\mathbb{Z}$ on calcule i et j à l'aide de l'algorithme d'Euclide.

4 Inversibilité, anneaux intègres

Définition 4.1. Soit A un anneau. Un élément $a \in A^*$ est un *diviseur de zéro à gauche* s'il y a $b \in A^*$ avec $ab = 0$. Dans ce cas, b est un *diviseur de zéro à droite*.

Un anneau commutatif sans diviseur de zéro est un anneau *intègre*. Attention : Parfois on demande en plus que l'anneau soit unitaire !

Si A est unitaire, un élément $a \in A$ est *inversible* s'il y a $b \in A$ avec $ab = ba = 1$.

L'ensemble des éléments inversibles est noté $A^\times$. C'est un groupe multiplicatif.

Un anneau commutatif 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.

2. Si a n'est pas diviseur de zéro à gauche et $ab = ac$, alors $b = c$ (et similairement à droite). En particulier un anneau intègre a simplification multiplicative.

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

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

Exemple 4.4. 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 4.5. $\mathbb{Z}/n\mathbb{Z}$ 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

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

Donc $\mathbb{Z}/n\mathbb{Z}$ n'est pas intègre.

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

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

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

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

Proposition 4.6. 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 $A \rightarrow A$ 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. $\square$

En fait, le Théorème de Wedderburn affirme 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 4.7 (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 $f : A \rightarrow L$ est un morphisme d'anneaux avec L un corps, il se prolonge en morphisme $\bar{f} : K \rightarrow L$.*

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} :

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

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

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

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 $f : A \rightarrow K$ 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 :

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

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 $g : A \rightarrow L$ 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. $\square$

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 $ac = b$.
- Un élément a est *irréductible* si pour tous $b, c \in A$, si $a = bc$ alors b ou c est inversible.
- Un élément $a \in A$ est *premier* si pour tous $b, c \in A$, si $p \mid bc$ alors $p \mid b$ ou $p \mid c$.

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

Exemple 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 $|a|^2 \in \mathbb{N}$. On en déduit que $|a| = 1$ pour tout $a \in A$ inversible. Si $z = a + i\sqrt{5}b \in \mathbb{Z}[i\sqrt{5}]$ 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 $|z|^2 \in \{2, 3\}$.

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 .

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 $a = bc$. 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. $\square$

Remarque 5.4. La réciproque est fautive : Dans l'exemple 5.2 on a que 2 est irréductible et divise $6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$, mais ne divise aucun des deux facteurs.

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 $a \sim b$.

C'est une relation d'équivalence.

Lemme 5.6. *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 $ac = b$. $\square$

Proposition 5.7. *Soit A un anneau intègre unitaire, et $a \in A^*$.*

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 $(a) \leq (b) \leq A$. Donc $a \in (b)$ et il y a $c \in A$ avec $a = bc$. Si b est inversible, alors $(b) = A$; si c est inversible, alors $(a) = (b)$.

Réciproquement, supposons qu'il n'existe aucun $b \in A$ avec $(a) < (b) < A$. Soient $c, d \in A$ avec $a = cd$. Alors $(a) \leq (c) \leq A$. Si $(c) = A$ alors c est inversible; si $(c) = (a)$ alors a et c sont associés et d est inversible. Ainsi a est irréductible. $\square$

Définition 5.8. Un idéal I dans un anneau A est *principal* s'il est engendré par un seul élément : il y a $a \in A$ avec $I = (a)$.

Un anneau intègre unitaire A est *principal* si tout idéal dans A est principal.

Exemple 5.9. On va voir plus bas des exemples d'anneaux principaux. On note que $\mathbb{Z}[X]$ n'est pas principal.

Proposition 5.10. Soit A un anneau principal, et $a \in A^*$. Sont équivalents :

1. a est premier.
2. a est irréductible.
3. aA est premier.
4. aA est maximal.

Démonstration. On sait déjà que $4. \Rightarrow 3. \Rightarrow 1. \Rightarrow 2.$ Enfin, $2. \Rightarrow 4.$ découle de la proposition 5.7.2, sachant que tout idéal est principal. $\square$

Définition 5.11. Un anneau intègre unitaire est *euclidien* s'il y a une fonction $N : A \setminus \{0\} \rightarrow \mathbb{N}$ 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*.

Exemple 5.12. — $\mathbb{Z}$ 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

$$N(r) = |r|^2 = |a - bq|^2 \leq \frac{1}{2} |b|^2 < |b|^2 = N(b).$$

Lemme 5.13. Soit A un anneau euclidien. Alors $N(1) = \min \text{im}(N)$ 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. $\square$

Théorème 5.14. 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. $\square$

Exemple 5.15. 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 5.16. Soit A un anneau principal, et $a_1, \dots, a_n \in A$ non-nuls.

- Un élément $\delta \in A$ tel que $(\delta) = (a_1, \dots, a_n)$ est un pgcd de $a_1, \dots, a_n$. On le note $\delta = \text{pgcd}(a_1, \dots, a_n) = a_1 \wedge \dots \wedge a_n$. D'après le lemme 5.6 un pgcd est déterminé à un facteur inversible près.
- Un élément $\Delta \in A$ tel que $(\Delta) = (a_1) \cap \dots \cap (a_n)$ est un ppcm de $a_1, \dots, a_n$. Il est noté $\delta = \text{ppcm}(a_1, \dots, a_n) = a_1 \vee \dots \vee a_n$, et déterminé à facteur inversible près.

Remarque 5.17. Dans $\mathbb{Z}$ et $K[X]$ on peut éliminer l'ambiguïté dans la 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 5.18 (Relation de Bézout). Soit $\delta = a_1 \wedge \dots \wedge a_n$. Alors il y a $c_1, \dots, c_n \in A$ avec $\delta = c_1 a_1 + \dots + c_n a_n$.

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

Remarque 5.19. Les éléments $c_1, \dots, c_n$ sont des *coefficients de Bézout*.

Définition 5.20. Les éléments $a_1, \dots, a_n$ sont *premiers entre eux* si $a_1 \wedge \dots \wedge a_n = 1$.

Corollaire 5.21 (Théorème de Bézout). Soit A principal. Les éléments $a_1, \dots, a_n$ sont premiers entre eux si et seulement s'il y a $c_1, \dots, c_n \in A$ avec $a_1 c_1 + \dots + a_n c_n = 1$.

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

Théorème 5.22 (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 5.23. Soit $\delta = a_1 \wedge \dots \wedge a_n$ et $\Delta = a_1 \vee \dots \vee a_n$.

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

Démonstration. 1. D'après Bézout il y a $c_1, \dots, c_n \in A$ avec $\delta = c_1 a_1 + \dots + c_n a_n$. Donc si $b \mid a_i$ pour $i = 1, \dots, n$ alors $b \mid c_1 a_1 + \dots + c_n a_n = \delta$.
Réciproquement, $a_i \in (\delta)$ pour $i = 1, \dots, n$, 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 $i = 1, \dots, n$, 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 $i = 1, \dots, n$.
Réciproquement, si $a_i \mid b$ alors $b \in (a_i)$ pour $i = 1, \dots, n$, et donc $b \in (a_1) \cap \dots \cap (a_n) = (\Delta)$. Ainsi $\Delta \mid b$. $\square$

Remarque 5.24. Puisque $a \mid b$ si et seulement $ca \mid cb$, on a $ca_1 \wedge \dots \wedge ca_n = c(a_1 \wedge \dots \wedge a_n)$ et $ca_1 \vee \dots \vee ca_n = c(a_1 \vee \dots \vee a_n)$.

Théorème 5.25. Soit A un anneau principal, et $a, b \in A^*$. Alors $(a \wedge b)(a \vee b) = (ab)$. Autrement dit, si $\delta = a \wedge b$ et $\Delta = a \vee b$, alors il y a $u \in A$ inversible avec $\delta\Delta = uab$.

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

Soient $u, v \in A$ avec $a'u + b'v = 1$. Puisque $a' \mid a' \vee b'$ il y a $c \in A$ avec $a'c = a' \vee b'$. Alors $c = a'cu + b'cv$. Or, $b' \mid b'cv$ et $b' \mid (a' \vee b') = a'cu$, ce qui donne $b' \mid a'cu + b'cv = c$, et il y a $c' \in A$ avec $b'c' = c$. Ainsi $a' \vee b' = a'c = a'b'c'$ et $a' \vee b' \in (a'b')$. Donc $(a' \vee b') \leq (a'b')$.

Réciproquement, $a'b' \in (a') \cap (b')$, d'où $(a'b') \leq (a') \cap (b') = (a' \vee b')$ ce qui donne l'égalité. $\square$

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 $N(a_2) < N(a_1)$. 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 $(a, b) = (a_0, a_1) = (a_1)$, d'où $a \wedge b = a_1$. Si $a_2 \neq 0$ on itère avec a_1, a_2 . Puisque la suite d'entiers $(N(a_i))_{i \geq 0}$ décroît strictement, l'algorithme s'arrête. Pour calculer des coefficients de Bézout, on calcule $u_n, v_n \in A$ tel que $a_n = u_n a + v_n b$. On pose $u_0 = v_1 = 1$ et $u_1 = v_0 = 0$. Si $a_{n-1} = u_{n-1}a + v_{n-1}b$ et $a_n = u_n a + v_n b$, on obtient

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

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 5.26. 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	$597 \quad 322$	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 5.27. Un anneau est *noethérien* s'il n'y a pas de chaîne $I_0 < I_1 < I_2 < \dots$ infinie strictement croissante d'idéaux à gauche ou à droite.

Proposition 5.28. *Un anneau est noethérien si et seulement si tout idéal à gauche ou à droite 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 à gauche qui n'est pas finiment engendré. Supposons qu'on a trouvé $a_1, \dots, a_n \in I$ tel que $(a_1) < (a_1, a_2) < \dots < (a_1, \dots, a_n)$ (pour $n = 0$ l'hypothèse est vide). Puisque I n'est pas finiment engendré, on a $(a_1, \dots, a_n) < I$ et il y a $a_{n+1} \in I \setminus (a_1, \dots, a_n)$. Alors $(a_1, \dots, a_n) < (a_1, \dots, a_n, a_{n+1})$. Ainsi on trouve une chaîne infinie strictement croissante d'idéaux à gauche, une contradiction. Donc tout idéal à gauche de A est finiment engendré. Par symétrie, tout idéal à droite est aussi finiment engendré.

Réciproquement, supposons que tout idéal à gauche ou à droite est finiment engendré. Soit $I_0 < I_1 < \dots \trianglelefteq A$ est une chaîne infinie strictement croissante d'idéaux à gauche. Alors $I = \bigcup_{n \in \mathbb{N}} I_n$ est un idéal à gauche dans A , donc engendré par un nombre fini d'éléments $a_1, \dots, a_k \in I$. Or, $I = \bigcup_{n \in \mathbb{N}} I_n$; il y a donc $n_0 \in \mathbb{N}$ tel que $a_1, \dots, a_k \in I_{n_0}$. Alors $I = (a_1, \dots, a_k) \leq I_{n_0} < I_{n_0+1} \leq I$, une contradiction. Par symétrie, il n'y a pas de chaîne infinie strictement croissante d'idéaux à droite non plus, et A est noethérien. $\square$

Corollaire 5.29. Un anneau principal est noethérien. $\square$

6 Anneaux factoriels

Définition 6.1. Un anneau intègre unitaire est *factoriel* si tout élément $a \in A^*$ non-inversible se factorise comme produit d'éléments irréductibles, et que cette factorisation est unique à association et permutation près.

Cela veut dire que si $a \in A^*$ est non-inversible il y a une unique, des irréductibles $p_1, \dots, p_n \in A$ tel que $a = p_1 p_2 \dots p_n$, et si $q_1, \dots, q_m \in A$ sont irréductibles avec $a = q_1 q_2 \dots q_m$ alors $n = m$ et il y a une permutation σ de $\llbracket 1, n \rrbracket$ tel que p_i et $q_{\sigma(i)}$ sont associés pour tout $i = 1, \dots, n$.

Exemple 6.2. $\mathbb{Z}[X]$ est un anneau factoriel qui n'est pas principal.

La démonstration se fera dans le prochain chapitre.

Lemme 6.3. *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. $\square$

Proposition 6.4. *Dans un anneau factoriel, un élément est irréductible si et seulement s'il est premier.*

Démonstration. On sait déjà que premier implique irréductible dans un anneau intègre unitaire. Soit $p \in A$ irréductible, et $b, c \in A$ tel que $p \mid bc$. Il y a donc $a \in A$ avec $ap = bc$. Soient $a = p_1 \cdots p_n$, $b = q_1 \cdots q_m$ et $c = r_1 \cdots r_k$ les factorisations de a , b et c en facteurs irréductibles. Alors $pp_1 \cdots p_n = q_1 \cdots q_m r_1 \cdots r_k$ sont deux factorisations de $ap = bc$ en facteurs irréductibles. Par unicité il y a soit $i \in \llbracket 1, m \rrbracket$ avec p associé à q_i , et $p \mid b$, soit $j \in \llbracket 1, k \rrbracket$ avec p associé à r_j , et $p \mid c$. Ainsi p est premier. $\square$

Proposition 6.5. *Un anneau intègre unitaire A est factoriel si et seulement si tout élément $a \in A^*$ non-inversible se factorise comme produit d'éléments premiers.*

Démonstration. Soit A factoriel. Alors tout élément non-nul non-inversible se factorise comme produit d'éléments irréductibles, qui sont premiers d'après la proposition 6.4. Réciproquement, supposons que tout élément $a \in A^*$ non-inversible se factorise comme produit d'éléments premiers. Puisque un élément premier est irréductible, a se factorise comme produit d'éléments irréductibles. Supposons donc que

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

pour des éléments premiers $p_1, \dots, p_n$ et des éléments irréductibles $q_1, \dots, q_m$. 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 $i \in \llbracket 1, m \rrbracket$ tel que p_1 divise q_i . Il y a donc $b \in A$ avec $p_1 b = q_i$. Donc $p_1 = b^{-1} q_i = q_1 \cdots q_m$. Par simplification on a $b^{-1} = q_1 \cdots q_{i-1} q_{i+1} \cdots q_m$, ce qui implique que q_j est inversible pour $j \neq i$. Or, un élément irréductible 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 irréductibles.

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 $i \in \llbracket 1, m \rrbracket$ tel que $p_n \mid q_i$, et il y a $b \in A$ avec $p_n b = q_i$; puisque q_i est irréductible et p_n 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 $p_1 \cdots p_{n-1} = q_1 \cdots q_{m-1} b^{-1}$ avec $q_1, \dots, q_{m-2}, q_{m-1} b^{-1}$ irréductibles. Par hypothèse de récurrence $n - 1 = m - 1$ et il y a une permutation σ de $\llbracket 1, n - 1 \rrbracket$ tel que p_i est associé à $q_{\sigma(i)}$ pour $i = 1, \dots, n - 1$ (être associé à q_{m-1} est la même chose qu'être associé à $q_{m-1} b^{-1}$). Donc la factorisation de a en éléments irréductibles est unique. $\square$

Corollaire 6.6. Un anneau principal est factoriel.

Démonstration. Un anneau principal est euclidien, et chaque élément non-nul non-inversible s'écrit donc comme produit d'irréductibles. Or, dans un anneau principal un élément irréductible est premier. On termine avec la proposition 6.5. $\square$

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 est associé à un unique élément de $\mathcal{P}$.

Lemme 6.7. *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 $i \in \llbracket 1, n \rrbracket$ 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. $\square$

Proposition 6.8. *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 $p \in \mathcal{P}$. $\square$

Définition 6.9. 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

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

Lemme 6.10. *Soient $a, b, c \in A^\times$. Alors*

$$\begin{aligned} c \mid a \text{ et } c \mid b &\Leftrightarrow c \mid a \wedge b, \\ a \mid c \text{ et } b \mid c &\Leftrightarrow a \vee b \mid c. \end{aligned}$$

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

Démonstration. Les équivalences sont conséquence de la proposition 6.8. Le dernier énoncé est un simple calcul, en utilisant $\min\{m, n\} + \max\{m, n\} = m + n$. $\square$

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.

7 Anneaux de polynômes

Définition 7.1. Soit A un anneau. 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 $A[X]$.

En particulier, $X \in A[X]$ si et seulement si A est unitaire.

Proposition 7.2 (Propriété universelle). Soient A et B deux anneaux unitaires et $f : A \rightarrow B$ un homomorphisme d'anneaux unitaires (donc avec $f(1_A) = 1_B$). Soit $b \in B$ central, c'est-à-dire $bb' = b'b$ pour tout $b' \in B$. Alors il existe un unique morphisme $\bar{f} : A[X] \rightarrow B$ qui prolonge f et tel que $\bar{f}(X) = b$.

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 $\bar{f}$. $\square$

Remarque 7.3. n n'a pas besoin que b soit central dans tout B , ni que B soit unitaire. Il nous faut que $bb' = b'b$ pour tout $b' \in \text{im}(f)$, et que $f(1)b = b$.

Corollaire 7.4. Soit $f : A \rightarrow B$ un morphisme d'anneaux unitaires. Alors il induit un morphisme $\bar{f} : A[X] \rightarrow B[X]$ 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 $B[X]$. Alors X est central dans $B[X]$ et on peut appliquer le lemme 7.2. 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 . $\square$

Théorème 7.5. Soit A un anneau intègre unitaire. Alors $A[X]$ est intègre ; il est principal si et seulement si A est un corps.

Démonstration. Pour deux polynômes non-nuls $P, Q \in A[X]$ le coefficient dominant de PQ est le produit des coefficients dominants de P et de Q . Il en suit que $A[X]$ est intègre.

Si A est un corps, alors $A[X]$ est même euclidien, avec le degré comme norme.

Soit donc $a \in A^*$ non-inversible. On considère l'idéal $(X, a) \triangleleft A[X]$, qui consiste de tous les polynômes dont le terme constant est divisible par a . Supposons que $P \in A[X]$ engendre (X, a) . Alors $\deg a = 0$ et a est multiple de P , d'où $\deg P = 0$ et $P \in A$ est une constante. Mais $(P) = (X, a) < A[X]$, donc P n'est pas inversible. Or, X est multiple de P , et il y a un polynôme $Q \in A[X]$ avec $PQ = X$. On a $\deg Q = 1$, et donc $Q = bX + c$, avec $Pb = 1$ et $Pc = 0$. Ainsi P est inversible, une contradiction. Donc $A[X]$ n'est pas principal. $\square$

Théorème 7.6 (Transfert de Gauss). Soit A un anneau factoriel. Alors $A[X]$ est factoriel.

Il nous faut quelques considérations préliminaires.

Définition 7.7. Soit A un anneau factoriel, et $P \in A[X]$. Le *contenu* $c(P)$ est le pgcd des coefficients de P .

Remarque 7.8. En général, le contenu, comme le pgcd, n'est déterminé qu'à multiplication par un élément inversible près.

Proposition 7.9. Soit A factoriel, et $P, Q \in A[X]$. Alors $c(PQ) = c(P)c(Q)$.

Démonstration. On prend $\tilde{P}, \tilde{Q} \in A[X]$ avec $c(P)\tilde{P} = P$ et $c(Q)\tilde{Q} = Q$. Alors $c(\tilde{P}) = c(\tilde{Q}) \sim 1$; il suffit de montrer que $c(\tilde{P}\tilde{Q}) \sim 1$. Pour une contradiction, supposons que $c(\tilde{P}\tilde{Q}) \not\sim 1$.

Soit $p \in A$ irréductible avec $p \mid c(\tilde{P}\tilde{Q})$. Alors l'idéal $I = (p)$ est premier et $\bar{A} = A/I$ est intègre. On considère l'application

$$\pi : A[X] \rightarrow \bar{A}[X], \quad \sum_i a_i X^i \mapsto \sum_i (a_i + I) X^i,$$

la réduction modulo I .

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

Corollaire 7.10. Soit A un anneau factoriel, K son corps des fraction, et $P \in A[X]$ avec $c(P) \sim 1$. Alors P est irréductible dans $A[X]$ si et seulement si P est irréductible dans $K[X]$.

Démonstration. Soit P est irréductible dans $K[X]$, et considérons $Q, R \in A[X]$ avec $P = QR$. Alors Q ou R est inversible dans $K[X]$ et donc de degré zéro : c'est un élément de A . Il divise $c(P) \sim 1$, et est inversible dans A .

Réciproquement, soit P irréductible dans $A[X]$, et considérons $Q, R \in K[X]$ avec $P = QR$. En chassant les dénominateurs, on obtient $d \in A$ et $\tilde{Q}, \tilde{R} \in A[X]$ avec $dP = \tilde{Q}\tilde{R}$. Alors $d \sim dc(P) = c(dP) = c(\tilde{Q})c(\tilde{R})$. Si $\hat{Q}, \hat{R} \in A[X]$ avec $c(\tilde{Q})\hat{Q} = \tilde{Q}$ et $c(\tilde{R})\hat{R} = \tilde{R}$, alors $P = \hat{Q}\hat{R}$. Par irréductibilité de P dans $A[X]$ soit $\hat{Q}$ soit $\hat{R}$ est inversible dans $A[X]$, donc dans $K[X]$. Ainsi P est irréductible dans $K[X]$. $\square$

Exemple 7.11. 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.

Démonstration du théorème 7.6. Soit $P \in A[X]$. On le factorise comme $P = c(P)\tilde{P}$, où $\tilde{P} \in A[X]$ avec $c(\tilde{P}) \sim 1$. Or, toute factorisation de P se raffine en une factorisation de $c(P)\tilde{P}$. La factorisation de $c(P)$ en irréductibles est unique, puisque A est factoriel. Il suffit donc de montrer que $\tilde{P}$ se factorise de manière unique en irréductibles.

Puisque $c(\tilde{P}) \sim 1$, tout facteur de $\tilde{P}$ de degré zéro est inversible ; il y a donc une factorisation $\tilde{P} = Q_1 \cdots Q_n$ en polynômes $Q_i \in A[X]$ de degré ≥ 1 , avec $n \leq \deg P$ maximal. Alors Q_i est irréductible dans $A[X]$ et $c(Q_i) \sim 1$ pour tout $i = 1, \dots, n$. Ainsi Q_i est irréductible dans $K[X]$, où K est le corps des fractions de A .

Si $\tilde{P} = R_1 \cdots R_m$ est une autre factorisation en irréductibles de $A[X]$ (et donc de $K[X]$), alors par factorisation unique dans $K[X]$ on a $m = n$, et quitte à permuter, Q_i et R_i sont associés dans $K[X]$. Il y a donc $a, b \in A$ non-nuls avec $aQ_i = bR_i$. Ainsi $a \sim a c(Q_i) = c(aQ_i) = c(bR_i) = b c(R_i) \sim b$, ce qui donne $a = ub$ pour un $u \in A$ inversible. Alors Q_i et R_i sont associés dans $A[X]$, ce qui montre que la factorisation est unique. $\square$

Ceci donne un critère utile d'irréductibilité.

Théorème 7.12 (Critère d'Eisenstein). *Soit A anneau factoriel avec corps des fractions K , et $P = \sum_{i=0}^n a_i X^i \in A[X]$. Soit $p \in A$ premier tel que*

- p divise $a_0, \dots, a_{n-1}$,
- p ne divise pas a_n , et
- p^2 ne divise pas a_0 .

Alors P est irréductible dans $K[X]$.

Démonstration. On peut supposer que $c(P) = 1$, puisque $c(P)$ est inversible dans $K[X]$. Il suffit donc de montrer que P est irréductible dans $A[X]$. Supposons que $P = QR$ avec $Q, R \in A[X]$ non-constants, et considérons la réduction modulo (p) . On a $\pi : A \rightarrow \bar{A} = A/(p)$, avec $\pi(a_k) = 0$ pour un $k = 0, \dots, n-1$ et $\pi(a_n) \neq 0$.

Soient $Q = \sum_{i=0}^d b_i X^i$ et $R = \sum_{i=0}^{n-d} c_i X^i$ avec $0 < d < n$. 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 $\pi(b_0) \neq 0$. Puisque $\pi(b_d)\pi(c_{n-d}) = \pi(a_n) \neq 0$ et $\bar{A}$ est intègre, on peut choisir $k \leq n-d$ minimal avec $\pi(c_k) \neq 0$. Alors $0 = \pi(a_k) = \pi(b_0)\pi(c_k) \neq 0$, une contradiction. $\square$

Exemple 7.13. Une réduction modulo 5 montre que $3X^4 + 15X^2 + 10$ est irréductible dans $\mathbb{Q}[X]$.

Exemple 7.14. 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 critères 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.

Chapitre 2

Corps

8 Extensions, degré, caractéristique, corps premier

Définition 8.1. Un *corps* est un anneau commutatif unitaire tel que tout élément a un inverse multiplicatif.

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

Exemple 8.2. — 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 $K(X) = \text{frac}(K[X])$ 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 8.3. 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 8.4. 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 8.5. On a $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$, $[\mathbb{Q}[i] : \mathbb{Q}] = 2$.

Lemme 8.6. 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. $\square$

Théorème 8.7. 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 $[L : K] = n$ et $[M : L] = m$ avec des bases $(a_1, \dots, a_n)$ et $(b_1, \dots, b_m)$. Alors pour tout $a \in M$ il y a $k_1, \dots, k_n \in L$ avec $a = \sum_{i=1}^n k_i a_i$, et pour tout $i = 1, \dots, n$ il y a $k_{ij} \in M$ 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 $k_{ij} \in M$ avec

$$0 = \sum_{i,j} k_{ij} a_i b_j = \sum_i \left(\sum_j k_{ij} b_j \right) a_i.$$

Puisque les $(a_i)_i$ sont libres sur L , on a $\sum_j k_{ij} b_j = 0$ pour tout $i = 1, \dots, n$. 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 $[M : K] = mn$. $\square$

Soit K un corps. On considère l'application

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

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

Définition 8.8. Si $\ker \phi = (n)$ on dit que la *caractéristique* de K vaut n (qui est soit 0, soit un entier premier). On le note $\text{car}(K) = n$. Le *corps premier* de K est le plus petit sous-corps de K . Si $\text{car}(K) = p > 0$ il est isomorphe à $\mathbb{F}_p$; si $\text{car}(K) = 0$ il est isomorphe à $\mathbb{Q}$.

Lemme 8.9. Si $\text{car}(K) = p > 0$, le groupe additif $(K, 0, +)$ est un groupe abélien d'exposant p ; si $\text{car}(K) = 0$ le groupe additif est un groupe abélien divisible sans torsion.

Démonstration. Si $\text{car}(K) = p > 0$ alors $pa = 0$ pour tout $a \in K$. Puisque p est premier cela signifie que tout $a \in K^*$ est d'ordre additif p . 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 $\text{car}(K) \neq 0$.

Si $\text{car}(K) = 0$, 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. $\square$

9 Extensions simples, extensions algébriques, polynôme minimal

Définition 9.1. 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 $K(a) = L$. 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 .

Exemple 9.2. Les éléments $i, \sqrt{3}, 1 + i\sqrt{2}$ sont algébriques sur $\mathbb{Q}$. Par contre, e et π sont transcendants sur $\mathbb{Q}$.

Proposition 9.3. 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 $1, a, a^2, \dots, a^{d-1}$ forment une K -base de $K(a)$.
2. Si a est transcendant, alors $K(a) \cong K(X) = \text{frac}(K[X])$. Les puissances $1, a, a^2, \dots$ forment une famille libre sur K .

Démonstration. On considère l'évaluation en a , $\text{eval}_a : K[X] \rightarrow K(a)$ donnée par $P(X) \mapsto P(a)$, un morphisme d'anneaux. Puisque $\text{im}(\text{eval}_a)$ est intègre, $I = \ker(\text{eval}_a)$ 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 $\overline{\text{eval}}_a : K(X) \rightarrow K(a)$. Or, $\text{im}(\overline{\text{eval}}_a)$ est une extension de K qui contient a ; on a ainsi $K(X) \cong K(a)$. Puisque $1, X, X^2, \dots$ sont K -libres dans $K[X]$, leurs images $1, a, a^2, \dots$ sont K -libres dans $K(a)$.

Sinon $I = (P)$ pour un polynôme non-constant irréductible, qu'on peut choisir unitaire. On a $P \in \ker \text{eval}_a$, 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) au reste de la division euclidienne de Q par P , c'est-à-dire un polynôme de degré $< \deg P = d$. Puisque $\text{eval}_a(X) = a$, le sous-corps $\text{im}(\text{eval}_a) \leq K(a)$ contient a et on a égalité : $K(a) \cong K[X]/(P)$. Les polynômes $1, X, \dots, X^{d-1}$ forment une K -base de $K[X]/(P)$, et donc leurs images $1, a, a^2, \dots, a^{d-1}$ forment une K -base de $K(a)$. Ceci signifie en particulier que $Q(a) \neq 0$ si $\deg Q < d$. Donc $P(X)$ est l'unique polynôme unitaire non-trivial de degré minimal annule par a . $\square$

Définition 9.4. Une extension $K \leq L$ est *algébrique* si $[K(a) : K] < \infty$ for all $a \in L$.

En particulier une extension de degré fini est algébrique.

Lemme 9.5. 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 $[L(a) : L] = \deg Q \leq \deg P = [K(a) : K]$. $\square$

Proposition 9.6. 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 $b_0, \dots, b_d \in L$ les coefficients de P . On considère la suite d'extensions

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

Pour tout $i < d$ on a

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

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

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

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

$$\begin{aligned} [K(a) : K] &\leq [K(b_0, b_1, \dots, b_d)(a) : K] = [K_{\leq d}(a) : K] \\ &= [K_{\leq 0} : K] [K_{\leq 1} : K_{\leq 0}] [K_{\leq 2} : K_{\leq 1}] \dots [K_{\leq d} : K_{\leq d-1}] [K_{\leq d}(a) : K_{\leq d}] < \infty. \end{aligned}$$

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

Corollaire 9.7. 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 contenant 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 $a - b, ab^{-1} \in \bar{K}^L$. $\square$

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

Exemple 9.8. — $\bar{\mathbb{Q}} = \bar{\mathbb{Q}}^{\mathbb{C}} = \{a \in \mathbb{C} : a \text{ algébrique sur } \mathbb{Q}\}$ est le *corps des nombres algébriques*.

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

10 Corps de rupture, corps de décomposition, clôture algébrique

Dans la section précédente, nous sommes parties 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 10.1. Soit K un corps et $P \in K[X]$ un polynôme irréductible. Le *corps de rupture* de P est une extension L minimale telle que P possède un zéro dans L . 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 $\bar{P} = P/\text{cd}(P)$ 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. $\square$

Corollaire 10.2. 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 . $\square$

Lemme 10.3. 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. On fait une récurrence forte sur $\deg P$. On suppose donc le théorème vrai pour les polynômes (sur un corps quelconque) de degré $< d$, et on considère $P \in K[X]$ de degré d . Soit Q un facteur irréductible de P sur K , et soit $K(a)$ le corps de rupture de Q , où $Q(a) = 0$, avec $[K(a) : K] = \deg Q \leq \deg P = d$. Alors P se factorise sur $K(a)$ comme $P = (X - a)R$, avec $\deg R = \deg P - 1$. Si $\deg R = 0$ alors on a terminé. Sinon, par hypothèse de récurrence il y a une extension $L \geq K(a)$ de degré $\leq (d - 1)!$ où R possède $d - 1$ racines. Alors $[L : K] = [L : K(a)][K(a) : K] \leq (d - 1)!d = d!$, et P possède d racines dans L (avec multiplicités). $\square$

Définition 10.4. 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 $a_1, \dots, a_d$ de P (avec multiplicités) et $L = K(a_1, \dots, a_d)$.

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

Proposition 10.5. Soit $\phi : K \rightarrow L$ un isomorphisme de corps, $\bar{\phi} : K[X] \rightarrow L[X]$ l'isomorphisme induit sur les anneaux de polynômes, $P \in K[X]$ 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 $\phi' : K' \rightarrow L'$, 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 $P = X - a$ est linéaire et possède déjà une unique racine 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 $\phi_1 : K(a_1) \cong K[X]/(Q) \rightarrow L[X]/(\bar{\phi}(Q)) \cong L(b_1)$.

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, 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 $L(b_1)$. Par hypothèse de récurrence il y a un isomorphisme $\phi' : K' \rightarrow L'$ qui prolonge ϕ_1 , et donc ϕ . Cet isomorphisme doit envoyer les racines de P sur les racines de $\bar{\phi}(P)$. $\square$

Corollaire 10.6. Le corps de décomposition est unique à K -isomorphisme près.

Démonstration. On prend pour ϕ l'identité sur K . $\square$

Théorème 10.7. Soit $\phi : K \rightarrow L$ un isomorphisme de corps, $P \in K[X]$ un polynôme 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 $K' \rightarrow L'$ de ϕ .

Démonstration. Par récurrence forte sur n . Pour $n = 1$ il n'y a rien à démontrer. On suppose donc le théorème vrai pour des extensions de degré $< n$. Puisque $n > 1$ 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 $b_1, \dots, b_d$ dans L' , et il y a d plongements distincts $\phi_1, \dots, \phi_d$ de $K(a_1)$ dans L' tel que $\phi_i(a_1) = b_i$. Chaque plongement $K(a_1) \rightarrow L'$ 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 $K' \rightarrow L'$. Au total il y a donc $d \cot n/d = n$ prolongements de ϕ . $\square$

Définition 10.8. Un corps est *algébriquement clos* s'il n'a aucune extension algébrique propre.

Remarque 10.9. 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. $\square$

Exemple 10.10. Le corps complexe $\mathbb{C}$ et le corps des nombres algébriques $\bar{\mathbb{Q}}$ sont algébriquement clos.

Lemme 10.11. 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 $\prod_{i \in I_1} P_i$, 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 $\phi : K[X_i : i \in I_1] \rightarrow K'$ qui fixe K et avec $\phi(X_i) = a_i$. Alors

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

la contradiction recherché.

Ainsi $J < A$ et il y a un idéal maximal $J \leq M \triangleleft A$. On considère le corps $L = K[X_i : i \in I]/M$. Comme $M \neq A$ aucun élément de K n'est dans M , et L est une extension de K . Or, $P_i(X_i + M) = P_i(X_i) + M = M$, 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 $X_{i_1}, \dots, X_{i_n}$, et est donc dans $K(X_{i_1} + M, \dots, X_{i_n} + M)$, ce qui est une extension finie de K . $\square$

Lemme 10.12. Soit K un corps. Il existe une extension L algébrique de K qui est algébriquement clos.

Démonstration. D'après le lemme 10.11 il existe une suite $K = K_0 \leq K_1 \leq K_2 \leq \dots$ 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 déjà dans un K_i , qui est algébrique sur K .

Mais tout polynôme $P \in L[X]$ est déjà dans $K_i[X]$ pour un i suffisamment grand, et a un zéro dans $K_{i+1} \leq L$. Ainsi L est algébriquement clos. $\square$

Remarque 10.13. 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 10.11. On pourrait aussi construire la clôture algébrique de K par récurrence transfinie : On commence avec $K_0 = K$; si on a trouvé K_α pour un ordinal α et K_α n'est pas algébriquement clos, on pose $K_{\alpha+1} = K_\alpha[X]/(P)$ où $P \in K[X]$ est irréductible de

degré > 1 , et pour un ordinal limite λ on pose $K_\lambda = \bigcup_{\alpha < \lambda} K_\alpha$. Alors chaque K_α est une extension algébrique de K , et puisque dans chaque étape successeur on ajoute un élément on a $|K_\alpha \setminus K| \geq |\alpha|$. Or, il y a au plus $|K|^d$ polynômes unitaires de degré d sur K , et chacun a au plus d racines, ce qui signifie qu'une extension algébrique de K a au plus $\sum_{d \in \mathbb{N}} d |K|^d = |K| + \aleph_0$ éléments. Puisque tout K_α est algébrique sur K , on doit s'arrêter après moins que $|K|^+$ étapes, et on a trouvé la clôture algébrique.

Pour tout α il faut choisir un polynôme irréductible dans $K_\alpha[X]$. Donc cette démonstration a également besoin de l'axiome du choix. Il pourrait donc surprendre que néanmoins le théorème suivant affirme l'unicité de la clôture algébrique.

Théorème 10.14. *Chaque corps K a, à K -isomorphisme près, une unique extension algébrique algébriquement clos.*

Définition 10.15. On appelle l'extension donnée par le théorème 10.14 la *clôture algébrique* de K , notée $\bar{K}$.

Démonstration du théorème 10.14. On a vu l'existence dans le lemme 10.12. Montrons l'unicité. Soient donc $\bar{K}$ et $\bar{K}'$ deux extensions algébriques algébriquement clos de K . On considère la famille $\mathcal{X}$ de K -isomorphismes d'un sous-corps de $\bar{K}$ contenant K vers un sous-corps de $\bar{K}'$ contenant K . On ordonne $\mathcal{X}$ par inclusion (prolongement). Si $(\phi_i : i \in I)$ est une chaîne dans $\mathcal{X}$, alors $\bigcup_{i \in I} \phi_i$ est encore un K -isomorphisme de $\bigcup_{i \in I} \text{dom}(\phi_i)$ vers $\bigcup_{i \in I} \text{im}(\phi_i)$ qui prolonge tous les ϕ_i et majore la chaîne. $\mathcal{X}$ est donc inductif, et par le lemme de Zorn admet un élément σ maximal. Soit $K_0 = \text{dom}(\sigma)$ et $K'_0 = \text{im}(\sigma)$. 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 $K_0(a) \cong K_0[X]/(P) \rightarrow K'_0[X]/(\bar{\sigma}(P)) \cong K'_0(b)$, 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 $K_0(a) \cong K_0[X]/(\bar{\sigma}^{-1}(Q)) \rightarrow K'_0[X]/(Q) \cong K'_0(b)$ est un prolongement propre de σ , une contradiction. Donc $K'_0 = \bar{K}'$ et σ est le K -isomorphisme recherché. $\square$

Remarque 10.16. Soit L une extension algébrique de K . Alors $\bar{L} = \bar{K}$.

Démonstration. Si $a \in \bar{L}$ alors $L(a)$ est algébrique 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 . $\square$

11 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 $1, X, X^2, \dots$, donc de dimension dénombrable.

Définition 11.1. Soit $P(X) = \sum_i a_i X^i \in K[X]$. Alors P induit la fonction polynomiale $\hat{P} : K \rightarrow K$ donné par $x \mapsto \sum_i a_i x^i$.

Remarque 11.2. Il est facile de voir que $\widehat{P \pm Q} = \hat{P} \pm \hat{Q}$ et $\widehat{PQ} = \hat{P}\hat{Q}$.

Définition 11.3. Soit $P \in K[X]$. Un élément $a \in K$ est un *zéro*, ou une *racine* de P si $\hat{P}(a) = 0$.

Proposition 11.4. Un élément $a \in K$ est un zéro d'un polynôme non-nul $P \in K[X]$ si et seulement si $X - a$ divise P .

Démonstration. 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, $0 = P(a) = 0 + R$, d'où $R = 0$ et $(X - a)$ divise P . Réciproquement, si $P = (X - a)Q$, alors $P(a) = 0$. $\square$

Proposition 11.5. 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 $a \in K$ 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 . $\square$

Corollaire 11.6. La fonction $P \mapsto \hat{P}$ est injective si et seulement si K est fini.

Démonstration. Si K est fini, il y a au plus $|K|^{|K|}$ fonctions $K \rightarrow K$, mais une infinité de polynômes, à savoir $1, X, X^2, \dots$. 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. $\square$

Définition 11.7. Un polynôme $P \in K[X]$ non-nul est *scindé* si P se factorise sur K en facteurs linéaires.

Proposition 11.8. Soit $P \in K[X]$ non-nul scindé. Alors P a précisément $\deg(P)$ racines, comptées avec leurs multiplicités.

Démonstration. Un facteur linéaire est irréductible; deux facteurs linéaires distincts sont premiers entre eux. La proposition est donc une conséquence du lemme de Gauss. $\square$

Remarque 11.9. Un polynôme $P \in K[X]$ est toujours scindé sur la clôture algébrique $\bar{K}$.

Proposition 11.10 (Relations coefficients-racines). *Soit $P \in K[X]$ scindé sur K . Disons*

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

Alors

$$\begin{aligned} \frac{a_0}{a_d} &= (-1)^d \prod_{j=1}^d b_j \\ \frac{a_1}{a_d} &= (-1)^{d-1} \sum_{1 \leq j_1 < j_2 < \dots < j_{d-1} \leq d} b_{j_1} b_{j_2} \dots b_{j_{d-1}} \\ \frac{a_2}{a_d} &= (-1)^{d-2} \sum_{1 \leq j_1 < j_2 < \dots < j_{d-2} \leq d} b_{j_1} b_{j_2} \dots b_{j_{d-2}} \\ &\vdots \\ \frac{a_{d-2}}{a_d} &= \sum_{1 \leq j_1 < j_2 \leq d} b_{j_1} b_{j_2} \\ \frac{a_{d-1}}{a_d} &= - \sum_{j=1}^d b_j. \end{aligned}$$

Démonstration. Simple calcul. □

Définition 11.11. Soient $P, Q \in K[X]$. Si $P(X) = \sum_i a_i X^i$, on pose la *substitution* (ou *composition*)

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

Remarque 11.12. L'application $P \mapsto P \circ Q$ est linéaire, mais $Q \mapsto P \circ Q$ ne l'est pas.

Définition 11.13. Soit $P(X) = \sum_{i=0}^d a_i X^i \in K[X]$. Le polynôme dérive de P est le polynôme

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

Remarque 11.14. Dans $\mathbb{R}[X]$ la dérivation des polynômes coïncide 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 11.15 (Propriétés de la dérivation). *Soient $P, Q \in K[X]$. On a*

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

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

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

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

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

Proposition 11.16 (Formule de Taylor). *Soit $P \in K[X]$ et $\deg P \leq n < \text{car}(K)$. 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 11.17 (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 11.15). Supposons qu'elle est vraie pour n . Alors

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

Définition 11.18. 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 $n + 1$.

Proposition 11.19. Soit $P \in K[X]$ non-nul, et $a \in K$. Si a est zéro de P d'ordre au moins n , alors

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

Si $\text{car}(K) > \deg(P)$, 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

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

Ainsi pour $k < n$ on a

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

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

Réciproquement, supposons que $P(a) = P'(a) = \dots = P^{(n-1)}(a) = 0$. 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 11.20. En caractéristique $p > 0$ on a $(X^p)' = pX^{p-1} = 0$. Donc la dérivée peut s'annuler sans que le polynôme soit constant.

12 Corps finis et polynômes cyclotomiques

Proposition 12.1. Soit K un corps premier de caractéristique $p > 0$. Alors $|K| = p^n$ pour un certain $n \in \mathbb{N}^\times$. Les éléments de K sont précisément les racines du polynôme $P(X) = X^{p^n} - X \in \mathbb{F}_p[X]$. En particulier K est le corps de décomposition de P sur $\mathbb{F}_p$.

Démonstration. Le corps premier de K est fini, et donc isomorphe à $\mathbb{F}_p$. Alors K est un espace vectoriel sur K ; si $[K : \mathbb{F}_p] = n$, alors $|K| = p^n$.

On a $|K^\times| = p^n - 1$. Donc l'ordre multiplicatif de tout élément $a \in K^\times$ divise $p^n - 1$, et $a^{p^n-1} = 1$. Ceci donne $a^{p^n} - a = 0$, et cette égalité est aussi satisfaite par 0. Or, $X^{p^n} - X$ a au plus p^n racines. Donc les éléments de K sont précisément les racines de $X^{p^n} - X$, et K est le corps de décomposition de $X^{p^n} - X$ sur son corps premier $\mathbb{F}_p$. □

Théorème 12.2. Pour tout entier p premier et tout entier $n > 0$ il y a un unique corps de cardinal p^n , à isomorphisme près. On le dénote par $\mathbb{F}_{p^n}$.

Démonstration. On considère l'ensemble R des racines de $P(X) = X^{p^n} - X \in \mathbb{F}_p[X]$ dans $\bar{\mathbb{F}}_p$. On a $P'(X) = p^n X^{p^n-1} - 1 = -1$. Ainsi toutes les racines sont des racines simples, et $|R| = p^n$. Or, $0, 1 \in R$, et si $a, b \in R$ avec $b \neq 0$, alors $a^{p^n} = a$ et $b^{p^n} = b$, ce qui donne $(a/b)^{p^n} = a/b$ et $(a-b)^{p^n} = a-b$, puisque $p \mid \binom{p}{i}$ pour $0 < i < p$ et donc en caractéristique p on a

$$(a+b)^p = \sum_{i=0}^p \binom{p}{i} a^i b^{p-i} = a^p + b^p.$$

Donc R est un sous-corps de $\bar{\mathbb{F}}_p$ de cardinal p^n , ce qui montre l'existence. C'est le corps de décomposition de P sur $\mathbb{F}_p$, ce qui montre l'unicité de $\mathbb{F}_{p^n}$. □

Théorème 12.3. Le groupe multiplicatif $\mathbb{F}_{p^n}^\times$ est cyclique, isomorphe à $\mathbb{Z}/(p^n - 1)\mathbb{Z}$.

Démonstration. $\mathbb{F}_{p^n}^\times = \bigoplus_{q|p^n-1} S_q$, où S_q pour q premier divisant $p^n - 1$ est le Sylow q -sous-groupe de $\mathbb{F}_{p^n}^\times$. On a $\prod_q |S_q| = |\mathbb{F}_{p^n}^\times| = p^n - 1$. Mais si $|S_q| = q^k$ et S_q n'est pas cyclique, S_q serait d'exposant q^{k-1} au plus, et tous ses éléments seraient racines de $X^{q^{k-1}} - 1$. Mais ce polynôme a au plus $q^{k-1} < q^k$ racines, une contradiction. Donc tous les S_q sont cycliques ; comme leurs ordres sont premiers entre eux, $\mathbb{F}_{p^n}^\times$ est cyclique. □

Soit $n \in \mathbb{N}^*$. On rappelle que $\mathbb{U}_n \leq \mathbb{C}^\times$ est le sous-groupe des nombres complexes racines n -ièmes de l'unité. Donc les éléments de $\mathbb{U}_n$ sont précisément les racines du polynôme $X^n - 1 \in \mathbb{Z}[X]$. On pose

$$\mathbb{U}_n^* = \mathbb{U}_n \setminus \bigcup_{d|n, d < n} U_d,$$

l'ensemble des racines *primitives* n -ièmes de l'unité. On a

$$\mathbb{U}_n = \{e^{i\frac{k}{n}2\pi} : k = 0, \dots, n-1\} \quad \text{et} \quad \mathbb{U}_n^* = \{e^{i\frac{k}{n}2\pi} : k = 0, \dots, n-1, \text{pgcd}(k, n) = 1\}.$$

Définition 12.4. Le *polynôme cyclotomique d'indice n* est le polynôme unitaire

$$\Phi_n(X) = \prod_{\zeta \in \mathbb{U}_n^*} (X - \zeta).$$

Exemple 12.5. On a

$$\Phi_0 = 1, \quad \Phi_1 = X - 1, \quad \Phi_2 = X + 1, \quad \Phi_3 = X^2 + X + 1, \quad \Phi_4 = X^2 + 1.$$

Lemme 12.6. Soit $P \in \mathbb{Z}[X]$ unitaire, et $Q, R \in \mathbb{Q}[X]$ unitaires avec $P = QR$. Alors Q et R sont dans $\mathbb{Z}[X]$, de contenu 1.

Démonstration. Soit q le ppcm des dénominateurs des coefficients de Q , et r celui de R . Alors $qQ, rR \in \mathbb{Z}[X]$. Puisque Q est unitaire, on a $c(qQ) \mid cd(Q) = q$. On suppose pour une contradiction que $c(qQ) \neq 1$. Soit donc p premier avec $p \mid c(qQ)$, et soit $n \in \mathbb{N}^*$ maximal avec $p^n \mid c(qQ)$. Alors il y a un coefficient $\frac{a}{b}$ de q telle que $a \nmid a$ et $p^n \mid b$. Alors $a\frac{a}{b}$ est un coefficient de qQ , et $p \nmid q\frac{a}{b}$, ce qui contredit $p \mid c(qQ) \mid q\frac{a}{b}$. Donc $c(qQ) = 1$. De même, $c(rR) = 1$. Or

$$1 = c(qQ)c(rR) = c(qrP) = qr c(P) = qr.$$

Donc $q = r = 1$. Ainsi $Q, R \in \mathbb{Z}[X]$, de contenu 1. □

Proposition 12.7. On a $X^n - 1 = \prod_{d|n} \Phi_d(X)$. De plus, $\Phi_n \in \mathbb{Z}[X]$ pour tout $n \in \mathbb{N}^\times$.

Démonstration. Si $\zeta^n = 1$, alors l'ordre d de ζ divise n , et $\zeta \in \mathbb{U}_d^*$. Donc $\mathbb{U}_n = \bigcup_{d|n} \mathbb{U}_d^*$, et la réunion est disjointe. Ainsi

$$X^n - 1 = \prod_{\zeta \in \mathbb{U}_n} (X - \zeta) = \prod_{d|n} \prod_{\zeta \in \mathbb{U}_d^*} (X - \zeta) = \prod_{d|n} \Phi_d.$$

Si n est premier, alors $\mathbb{U}_n = \mathbb{U}_n^* \cup \{1\}$ et

$$\Phi_n(X) = \frac{X^n - 1}{X - 1} = 1 + X + \dots + X^{n-1} \in \mathbb{Z}[X].$$

Si n est composé, par récurrence on peut supposer $\Phi_d \in \mathbb{Z}[X]$ pour tout $d < n$. Soit $\Psi_n(X) = \prod_{d|n, d < n} \Phi_d(X)$. Alors $\Psi_n(X) \in \mathbb{Z}[X]$ est unitaire, et $X^n - 1 = \Phi_n(X)\Psi_n(X)$. Or, $\Phi_n \in \mathbb{Q}[X]$, puisque c'est le quotient de la division euclidienne de $X^n - 1$ par Ψ_n . De plus, Φ_n est unitaire. D'après le lemme précédent $\Phi_n \in \mathbb{Z}[X]$. □

Théorème 12.8. Φ_n est irréductible sur $\mathbb{Z}$ et sur $\mathbb{Q}$.

Démonstration. Soit ζ une racine primitive n -ième, et P son polynôme minimal sur $\mathbb{Q}$. Alors $\text{pgcd}(P, X^n - 1) \neq 1$; puisque P est irréductible sur $\mathbb{Q}$, il divise $X^n - 1$. Il y a donc $Q \in \mathbb{Q}[X]$ avec $PQ = X^n - 1$. Or, P et $X^n - 1$ sont unitaires, donc Q aussi; d'après le lemme $P, Q \in \mathbb{Z}[X]$.

Soit p premier, avec $p \nmid n$. Alors ζ^p est aussi une racine primitive n -ième de l'unité. Supposons pour une contradiction que $P(\zeta^p) \neq 0$. Alors ζ^p doit être racine de Q , et ζ est racine de $Q(X^p)$. Donc P divise $Q(X^p)$, et $Q(X^p) = PR$ pour un $R \in \mathbb{Z}[X]$ d'après le lemme. Puisque $a^p = a$ pour tout $a \in \mathbb{F}_p$ et $(b + c)^p = b^p + c^p$ en caractéristique p , la réduction modulo p donne

$$\bar{Q}(X)^p = \overline{Q(X^p)} = \bar{P} \bar{R}.$$

Soit $\bar{S} \in \mathbb{F}_p[X]$ un facteur irréductible de $\bar{P}$. Alors $\bar{S}$ divise $\bar{Q}$ et $\bar{P}$. Ainsi $\bar{S}^2$ divise $X^n - 1$. Or, $\overline{X^n - 1}' = (X^n - 1)' = nX^{n-1} \neq 0$ puisque p est premier avec n . Donc $X^n - 1$ n'a pas de racine commune avec son polynôme dérivé sur $\mathbb{F}_p$, et donc n'a pas de racine double dans la clôture algébrique $\bar{\mathbb{F}}_p$, une contradiction.

Donc pour tout p premier avec $p \nmid n$ on a aussi que ζ^p est racine de P . Par récurrence pour tout k premier avec n on a que ζ^k est racine de P . Ainsi toutes les racines primitives n -ièmes sont racines de P , et $\Phi_n = P$ est irréductible sur $\mathbb{Z}$, et donc sur $\mathbb{Q}$. $\square$

Théorème 12.9 (Wedderburn). Un anneau $A \neq \{0\}$ fini sans diviseur de zéro est un corps (commutatif).

Démonstration. Si $A = \{0, 1\}$ alors $A = \mathbb{F}_2$ et on a terminé. Sinon, soit $a \in A^*$ avec $a \neq 1$ (s'il y a une unité). Puisque A est fini il y a $m < n$ avec $a^m = a^n$. On pose $e = a^{n-m}$. Alors pour tout $b \in A$ on a $bea^m = ba^n = ba^m$, d'où $be = b$ par simplification; de même $a^m eb = a^n b = a^m b$ et $eb = b$. Donc A est unitaire avec $1 = e$. On note que a^{n-m-1} est l'inverse de a . Ainsi A est un corps gauche, ou anneau à division. Supposons A non-commutatif.

Soit $a \in A$ et $C_a = C_A(a) = \{b \in A : ab = ba\}$ le centralisateur de a . On pose $Z = \{b \in A : bc = cb \text{ pour tout } c \in A\}$, le centre de A . Par distributivité, C_a et Z sont des sous-corps gauches, Z est même un sous-corps (commutatif), et $Z \leq C_a \leq A$. Ainsi A est un C_a - et un Z -espace vectoriel, et C_a est un Z -espace vectoriel. Soit $d_a = \dim_Z C_a$, $e_a = \dim_{C_a} A$ et $n = \dim_Z A > 1$. Alors $d_a e_a = n$.

Soit $Z = \mathbb{F}_q$, où q est une puissance de $p = \text{car}(A)$. Alors $|Z^\times| = q - 1$, $|C_a^\times| = q^{d_a} - 1$ et $|A^\times| = q^n - 1$.

On considère la partition de A en classes de conjugaison. Soit X un système de représentants pour les classes de conjugaison non-triviales. Notons que la classe de a est triviale si et seulement si $a \in Z$ si et seulement si $e_a = 1$, et pour $a \notin Z$ on a $|a^{A^\times}| = |A^\times|/|C_a^\times| = (q^n - 1)/(q^{d_a} - 1)$ et d_a est un diviseur propre de n . L'équation des classes donne

$$q^n - 1 = |A^\times| = |Z| + \sum_{a \in X} |a^{A^\times}| = q - 1 + \sum_{a \in X} \frac{q^n - 1}{q^{d_a} - 1}.$$

Puisque d_a est un diviseur propre de n , on a que $\Phi_n(X)$ divise

$$\frac{X^n - 1}{X^{d_a} - 1} = \frac{\prod_{d|n} \Phi_d(X)}{\prod_{d|d_a} \Phi_d(X)} = \prod_{d|n, d \nmid d_a} \Phi_d(X) = \Phi_n(X) \prod_{d|n, d \nmid d_a, d < n} \Phi_d(X),$$

et donc $\Phi_n(q)$ divise tous les $(q^n - 1)/(q^{d_a} - 1)$. Ainsi $\Phi_n(q)$ divise

$$q - 1 = q^n - 1 - \sum_{a \in X} \frac{q^n - 1}{q^{d_a} - 1}.$$

Évaluons $\Phi_n(q) = \prod_{\zeta \in \mathbb{U}_n^*} (q - \zeta)$. La valeur absolue de chaque facteur est $> q - 1$ puisque $1 \notin \mathbb{U}_n^*$ pour $n > 1$, et donc $|\Phi_n(q)| > q - 1$, ce qui donne la contradiction recherchée. $\square$

13 Corps des nombres constructibles à la règle et au compas

Dans cette section, pour deux nombres complexes $z, z' \in \mathbb{C}$ on dénote par (zz') la droite dans $\mathbb{C}$ qui passe par les points d'affixes z et z' , et par $C(z, z')$ le cercle de centre z qui passe par z' (donc de rayon $|z' - z|$).

Définition 13.1. Soit $S \subseteq \mathbb{C}$. Un nombre complexe z est *élémentairement constructible* à partir de S s'il y a $z_1 \neq z_2$ et $z_3 \neq z_4$ dans S tel qu'on se trouve dans une des configurations suivantes :

- les droites $(z_1 z_2)$ et $(z_3 z_4)$ sont distincts et s'intersectent en z .
- z est dans l'intersection de la droite $(z_1 z_2)$ et du cercle $C(z_3, z_4)$.
- z est dans l'intersection des cercles $C(z_1, z_2)$ et $C(z_3, z_4)$.

Un nombre $z \in \mathbb{C}$ est *constructible* s'il y a une suite $z_0 = 0, z_1 = 1, z_2, z_3, \dots, z_n = z$ tel que z_i est élémentairement constructible à partir de $\{z_j : j < i\}$ pour tout $2 \leq i \leq n$. On note $\mathcal{K}$ l'ensemble des nombres complexes constructibles.

Théorème 13.2. $\mathcal{K}$ est un sous-corps de $\mathbb{C}$ contenant i . Il est clos par prise de partie réelle et imaginaire.

Démonstration. On sait comment construire à la règle et au compas la droite perpendiculaire à une droite qui passe par un point donné. On peut donc construire les droites réelles et imaginaires, ainsi que i , et les parties réelles et complexes d'un nombre complexe. On peut également compléter à la règle et au compas un parallélogramme si on a deux côtes adjacentes. Donc $\mathcal{K}$ est clos par addition. On peut faire une symétrie centrale par l'origine, donc $\mathcal{K}$ est clos par inverse additif. La règle de Thalès nous permet de multiplier et diviser deux réels. Pour la multiplication et division complexe, on fait les calculs en coordonnées sous forme algébrique. $\square$

Un corps est *constructible* s'il est contenu dans $\mathcal{K}$.

Théorème 13.3 (Wantzel). *Un réel a est constructible si et seulement s'il y a une chaîne de corps réels $\mathbb{Q} = K_0 < K_1 < \dots < K_n < \mathbb{R}$ tel que $a \in K_n$ et $[K_{j+1} : K_j] = 2$ pour tout $j < n$.*

Démonstration. On note d'abord que tous les rationnels sont constructibles d'après le théorème 13.2. On va montrer que si K est constructible et $[K(a) : K] = 2$, alors a est constructible. Puisque $K(b) = K(a)$ pour tout $b \in K(a) \setminus K$, ceci montre la direction réciproque.

Soit $P(X) = X^2 + bX + c \in K[X]$ le polynôme minimal de a sur K . Puisque $a \in \mathbb{R}$ est racine de P on a $b^2 - 4c \geq 0$, et donc $(X + \frac{b}{2})^2 = (\frac{b}{2})^2 - c = d \geq 0$. Il suffit donc de montrer que les nombres constructibles sont clos par racine carrée d'un nombre positif. Or, dans un triangle ABC rectangle en C , si D est le pied de la hauteur en C , on a $DB \times DA = DC^2$, puisque ADC et BDC sont semblables.

Pour construire $\sqrt{d}$, on trace un segment $[AB]$ de longueur $d + 1$, puis un demi-cercle de diamètre AB , ensuite le point D sur $[AB]$ tel que $BD = 1$, enfin la perpendiculaire à (AB) en D , qui intersecte le demi-cercle en C . D'après le théorème de Thalès, le triangle ABC est rectangle en C . Ainsi $DC^2 = 1 \times d$, et $\sqrt{d} = DC$ est constructible.

Pour la direction directe, on note que si $z_1 = x_1 + iy_1$ et $z_2 = x_2 + iy_2$ avec $x_1, y_1, x_2, y_2 \in K$, alors la droite $(z_1 z_2)$ est donnée par une équation $ax + by + c = 0$ avec $a = y_1 - y_2$, $b = x_2 - x_1$ et $c = x_1 y_2 - x_2 y_1$ tous dans K , et le cercle $C(z_1, z_2)$ est donné par une équation de la forme $x^2 + y^2 + ax + by + c = 0$ avec $a = -2x_1$, $b = -2y_1$ et $c = 2x_1 x_2 - x_2^2 + 2y_1 y_2 - y_2^2$ tous dans K .

- L'intersection de deux droites $ax + by + c = 0$ et $a'x + b'y + c' = 0$ est la solution d'un système linéaire, donc dans $\mathbb{Q}(a, b, c, a', b', c')$.
- L'intersection d'une droite $ax + by + c = 0$ avec un cercle $x^2 + y^2 + a'x + b'y + c' = 0$ s'obtient en substituant $-(by + c)/a$ pour x ou $-(ax + c)/b$ pour y . On se ramène à une équation de degré 2. Donc $[K(x) : K] \leq 2$ et $[K(y) : K] \leq 2$.
- L'intersection d'un cercle $x^2 + y^2 + ax + by + c = 0$ avec un cercle $x^2 + y^2 + a'x + b'y + c' = 0$ s'obtient en soustrayant les deux équations. On se ramène au cas précédent.

Dans tous les cas, les coordonnées du nouveau point engendrent des extensions de degré au plus 2 sur les corps qui contiennent les coordonnées de z_1, z_2, z_3, z_4 , ce qui démontre le théorème. $\square$

Corollaire 13.4. Soit z constructible. Alors $[\mathbb{Q}(z) : \mathbb{Q}]$ est une puissance de 2.

Démonstration. Si z est constructible, ses parties réelles x et imaginaires y le sont. D'après le théorème de Wantzel il y a une suite d'extensions

$$\mathbb{Q} = K_0 < K_1 < \dots < K_n < \mathbb{R}$$

telle que $[K_{j+1} : K_j] = 2$ pour tout $j < n$, avec $x, y \in K_n$. Alors $[K_n(i) : K_n] = 2$ et $z \in K_n(i)$. Donc $\mathbb{Q} \leq \mathbb{Q}(z) \leq K_n(i)$ et

$$2^{n+1} = [K_n(i) : \mathbb{Q}] = [K_n(i) : \mathbb{Q}(z)] [\mathbb{Q}(z) : \mathbb{Q}].$$

Ainsi $[\mathbb{Q}(z) : \mathbb{Q}]$ est n diviseur de 2^{n+1} , c'est-à-dire une puissance de 2. $\square$

Remarque 13.5. La réciproque est fautive : le polynôme $X^4 + 2X - 2$ est irréductible sur $\mathbb{Q}$. Donc une racine engendre une extension de degré 4, mais elle n'est pas constructible, puisque cette extension de degré 4 n'est pas contenue dans une tour d'extensions de degré 2.

Cependant, a est constructible si le degré du corps de décomposition de a sur $\mathbb{Q}$ est une puissance de 2. C'est facile à voir, une fois qu'on connaît la théorie de Galois.

Ce théorème résout négativement plusieurs problèmes célèbres de l'Antiquité

1. la quadrature du cercle (puisque π n'est pas algébrique, encore moins constructible),
2. la trisection de l'angle (si $a = \cos \theta$, alors $x = \cos \frac{\theta}{3}$ satisfait $4x^3 - 3x = a$),
3. la duplication du cube (puisque $\sqrt[3]{2}$ n'est pas constructible).

Définition 13.6. Un nombre premier est *nombre premier de Fermat* s'il est de la forme $2^{2^k} + 1$ pour un $k \in \mathbb{N}$.

Remarque 13.7. Si $2^n + 1$ est premier, alors n est une puissance de 2.

Démonstration. Si $n = k\ell$ contient un facteur impair $k > 1$, alors

$$2^n + 1 = (2^\ell)^k - (-1)^k = [(2^\ell) - (-1)] \sum_{j=0}^{k-1} 2^{\ell j} (-1)^{k-1-j}$$

n'est pas premier. □

Théorème 13.8 (Gauss-Wantzel). *Le n -gone régulier est constructible si et seulement si n est le produit d'une puissance de 2 et de nombres premiers de Fermat distincts.*

Démonstration. Soit ζ une racine primitive n -ième de l'unité. Alors le n -gone régulier est constructible à la règle et au compas si et seulement si ζ est constructible. On sait que Φ_n est irréductible sur $\mathbb{Q}$ et que les racines de Φ_n sont les racines primitives n -ièmes de l'unité, soit les puissances de ζ . Donc $\mathbb{Q}[\zeta]$ est le corps de décomposition de Φ_n sur $\mathbb{Q}$, et pour que ζ soit constructible il faut et suffit que $\deg \Phi_n$ soit une puissance de 2. Or, $\deg \Phi_n = \varphi(n)$, où $\varphi(n)$ est l'*indicatrice d'Euler*, le nombre d'entiers dans $\llbracket 1, n \rrbracket$ premiers avec n . On voit facilement que pour un nombre p premier et $k \in \mathbb{N}$ on a $\varphi(p^k) = (p-1)p^{k-1}$, et que pour k, ℓ premiers entre eux on a $\varphi(k\ell) = \varphi(k)\varphi(\ell)$. Donc si $n = \prod_i p_i^{\alpha_i}$ alors $\varphi(n) = \prod_i (p_i - 1)p_i^{\alpha_i - 1}$. Ainsi $\varphi(n)$ est une puissance de 2 si et seulement si $\alpha_i = 1$ et $p_i - 1$ est une puissance de 2, sauf si $p_i = 2$. D'après la remarque 13.7, si $p_i = 2^{\alpha_i} + 1$ est premier, alors α_i est une puissance de 2 et p_i est un nombre premier de Fermat. □