Algèbre 2

Cours de Vlerë Mehmeti*

0 Rappels sur les anneaux

0.1 Anneaux

Définition 0.1. Un *anneau* $(A, +, \cdot)$ est un ensemble muni de deux lois de composition internes $+$ et $\cdot$ telles que

(1) $(A, +)$ est un groupe abélien (on note son élément neutre 0_A)

(2) $\cdot$ est associative

(3) $\cdot$ se distribue sur $+$.

S'il existe un élément neutre pour $\cdot$, on le note 1_A et on dit que A est *unitaire*. Si $\cdot$ est commutatif, on dit que A est *commutatif*.

Remarque. Dans ce cours, sauf mention explicite, tout anneau considéré sera unitaire et commutatif.

Définition 0.2. Un élément $a \in A \setminus \{0\}$ est dit *un diviseur de zéro* s'il existe $b \in A \setminus \{0\}$ tel que $ab = 0$. Si A ne possède pas de diviseurs de zéros, on dit que A est *intègre*. Un élément $a \in A$ est dit *inversible* s'il existe $b \in A$ tel que $ab = ba = 1$. On notera l'ensemble des éléments inversibles $A^\times$.

Remarque.

(1) Si $a \in A^\times$ est inversible, l'élément $b \in A$ tel que $ab = 1$ est unique[1]. On le note a^{-1}.

(2) Un élément inversible n'est pas un diviseur de zéro.

Dans un anneau intègre A, pour tous $a, b \in A$, $ab = ac$ implique $a = 0$ ou $b = c$. En particulier, si $a \neq 0$, on peut simplifier par a.

Exemple 0.3. (1) $(\mathbb{Z}, +, \cdot)$ est un anneau.

(2) $(\mathbb{Z}[\sqrt{d}], +, \cdot)$ est un anneau.

(3) $(\mathbb{Z}/n\mathbb{Z}, +_n, \cdot_n)$ l'est aussi.

(4) $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$ est un anneau non commutatif.

(5) L'anneau des quaternions $(\mathbb{H}_\mathbb{C}, +, \cdot)$ est aussi non commutatif.

Tous ces exemples sont des anneaux intègres.

*Notes originales trouvables à `https://webusers.imj-prg.fr/~vlere.mehmeti/teaching.html`

1. En effet, si $ab = b'a = 1$, alors $b' = b'ab = b$

(6) Si A, B sont des anneaux, alors $A \times B$ muni des lois produits (composante par composante) est un anneau en général non intègre car $(1_A, 0) \cdot (0, 1_B) = (0, 0)$. On peut généraliser à un produit quelconque d'anneaux.

(7) Soit A un anneau. Alors $(A[X], +, \cdot)$ est un anneau où $+, \cdot$ sont l'addition et la multiplication usuelle des polynômes à coefficients dans A. On peut définir récursivement, pour $n \in \mathbb{N}^*$, $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$, et les lois internes $+$ et $\cdot$ induites de celles de $A[X_1, \ldots, X_{n-1}]$. Par convention, pour $n = 0, A[X_1, \ldots, X_n] = A$.

(8) Soit A un anneau et X un ensemble. Alors $A^X = \{f \mid f : X \to A\}$ muni des lois données par

$$\begin{cases} (f+g)(x) & = f(x) +_A g(x) \\ (f \cdot g)(x) & = f(x) \cdot_A g(x) \end{cases}$$

est un anneau.

(9) L'ensemble $\{f : \mathbb{R} \to \mathbb{R} \mid \exists [a_f, b_f] \subseteq \mathbb{R}, f_{|[a_f, b_f]^c} = 0\}$ est un anneau.

(10) L'anneau nul $\{0\}$ est l'unique anneau où $0 = 1$.

Proposition 0.4. *Soit A un anneau. Alors*

(1) $a0 = 0a = 0$ *pour tout* $a \in A$

(2) $(-a)b = a(-b) = -(ab)$ *pour tous* $a, b \in A$

(3) $(-a)(-b) = ab$ *pour tous* $a, b \in A$

(4) $-a = (-1)a$ *pour tout* $a \in A$.

Définition 0.5. Un *sous-anneau* R d'un anneau $(A, +, \cdot)$ est un sous-groupe R de $(A, +)$ tel que pour tous $a, b \in R$, $ab \in R$.

Remarque. R est un sous-anneau si et seulement si $0 \in R$ (ou $R \neq \varnothing$) et pour tous $a, b \in R$, $a - b \in R$ et $ab \in R$.

Remarque. L'anneau nul n'est pas intègre.

Exemple 0.6.

(1) $n\mathbb{Z}$ est un sous-anneau de $\mathbb{Z}$ pour tout $n \in \mathbb{Z}$.

(2) $(\mathbb{Q}, +, \cdot)$ est un anneau et $\{\frac{m}{n} \mid m, n \in \mathbb{Z} \setminus \{0\}, m \wedge n = 1, n \text{ impair}\} \cup \{0\}$ est un sous-anneau. Si on remplace "n impair" par "m impair", ce n'est plus le cas.

Définition 0.7. Un *morphisme d'anneaux unitaires* est une application $\varphi : A \to B$ telle que

(1) $\varphi(a + b) = \varphi(a) + \varphi(b)$

(2) $\varphi(ab) = \varphi(a)\varphi(b)$

(3) $\varphi(1_A) = 1_B$

Le morphisme φ est dit un *isomorphisme* s'il est bijectif.
Si φ est un isomorphisme et $A = B$, on dit que φ est un *automorphisme de A*.

Remarque. On notera par $\mathrm{Aut}(A)$ l'ensemble des automorphismes de A. Muni de la composition, c'est un groupe.

Proposition 0.8. *Soit $\varphi : A \to B$ un morphisme d'anneaux. Alors*

(1) $\mathrm{Im}(\varphi)$ *est un sous-anneau de* B.

(2) φ *est injectif si et seulement si*

$$\ker(\varphi) = \{a \in A \mid \varphi(a) = 0_B\} = \{0_A\}$$

Proposition 0.9. *Si* $\varphi : A \to B$ *et* $\psi : B \to C$ *sont deux morphismes d'anneaux, alors* $\psi \circ \varphi : A \to C$ *en est un aussi.*

Exemple 0.10.

(1) $\pi : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ m & \mapsto & m \mod n \end{array}$ est un morphisme d'anneaux (surjectif, mais pas injectif).

(2) $\psi_n : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ x & \mapsto & nx \end{array}$ n'est pas un morphisme d'anneaux unitaires si $n \neq 1$.

(3) $\theta : \begin{array}{ccc} \mathbb{C} & \to & \mathbb{C} \\ z & \mapsto & \overline{z} \end{array}$ est un automorphisme de $\mathbb{C}$.

(4) $\begin{array}{ccc} \mathbb{Q}[X] & \to & \mathbb{Q} \\ P(X) & \mapsto & P(0) \end{array}$ est un morphisme d'anneaux (surjectif, non injectif).

(5) $\begin{array}{ccc} \mathbb{Z} \times \mathbb{Z} & \to & \mathbb{Z} \times \mathbb{Z} \\ (a,b) & \mapsto & (a,0) \end{array}$ n'est pas un morphisme d'anneaux unitaires.

Définition 0.11. Un *corps* est un anneau commutatif unitaire non nul où tout élément non nul est inversible.

Exemple 0.12.

(1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps (de nombres).

(2) Le corps des fractions rationnelles $\mathbb{Q}(T) = \{\frac{P}{Q} \mid P, Q \in \mathbb{Q}[T]\}$ est un corps.

(3) Le corps des nombres algébriques $\overline{Q} = \{x \in \mathbb{C} \mid \exists P \in \mathbb{Q}[X] \setminus \{0\}, P(x) = 0\}$ est un corps.

Définition 0.13. Soit A un anneau sans diviseur de zéro. Le *corps des fractions de* A, noté $\mathrm{Frac}\, A$, est

$$\left\{ \frac{a}{b} \,\middle|\, a \in A, b \in A \setminus \{0\} \right\} / \sim \quad \text{où} \quad \frac{a}{b} \sim \frac{c}{d} \iff ad - bc = 0$$

Proposition 0.14. *Les lois suivantes sont bien définies sur* $\mathrm{Frac}\, A$ *et en font un corps :*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

Proposition 0.15. *L'application* $\varphi : \begin{array}{ccc} A & \to & \mathrm{Frac}\, A \\ a & \mapsto & \frac{a}{1} \end{array}$ *est un morphisme d'anneaux injectif. Si* A *est un corps, c'est un isomorphisme.*

Remarque. $\mathrm{Frac}\, A$ est le plus petit corps contenant A.

Exemple 0.16.

(1) $\mathrm{Frac}\, \mathbb{Z} = \mathbb{Q}$

(2) Pour $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z}$ a des diviseurs de zéro, sauf si n est premier et dans ce cas c'est un corps.

(3) $\mathrm{Frac}\, \mathbb{Q}[X] = \mathbb{Q}(X)$. Plus généralement, on définit $K(X_1, \ldots, X_n) = \mathrm{Frac}\, K[X_1, \ldots, X_n]$ pour K un corps.

0.2 Idéaux

Définition 0.17. Soit A un anneau (commutatif, unitaire). Un idéal de A est un sous-ensemble $I \subseteq A$ tel que

(1) $(I, +)$ est un sous-groupe de $(A, +)$

(2) Pour tous $a \in A$ et $b \in I$, $ab \in I$.

On note $I \lhd A$.

Remarque. Comme $(A, +)$ est un groupe abélien et I en est un sous-groupe, il est distingué, donc A/I est un groupe abélien muni de l'addition $(a + I) + (b + I) = (a + b) + I$.

Proposition 0.18. *Soit I un idéal de l'anneau A. Alors $(A/I, +, \cdot)$ est un anneau de loi multiplicative $(a + I)(b + I) = ab + I$. En particulier, cette opération est bien définie. On appelle A/I* l'anneau quotient de A par I. *De plus, la projection canonique* $\pi : \begin{array}{ccc} A & \to & A/I \\ x & \mapsto & x + I \end{array}$ *est un morphisme d'anneaux surjectif.*

Remarque. La définition d'idéal est précisément faite pour que la proposition ci-dessus fonctionne.

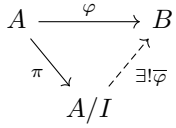
Théorème 0.19 (Premier théorème d'isomorphisme)**.**

(1) Si $\varphi : A \to B$ est un morphisme d'anneaux, alors $\ker \varphi$ *est un idéal de A et* $A/\ker \varphi \simeq \operatorname{im} \varphi$.

(2) Si I est un idéal de A alors $\pi : A \to A/I$ est surjective de noyau I.

Remarque. Les autres théorèmes d'isomorphisme fonctionnent aussi, par exemple si $I \subseteq J$ sont deux idéaux de A, alors $A/J \simeq (A/I)(J/I)$.

Théorème 0.20 (Propriété universelle du quotient)**.** *Soit $\varphi : A \to B$ un morphisme d'anneaux. Soit I un idéal de A tel que $\varphi(I) = \{0_B\}$. Alors il existe un unique $\overline{\varphi} : A/I \to B$ tel que $\varphi = \overline{\varphi} \circ \pi$ avec $\pi : A \to A/I$ la projection canonique.*



Exemple 0.21.

(1) $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$ pour $n \in \mathbb{N}$

(2) $\{0\}$ et A sont des idéaux de A

(3) $\{XP(X) \mid P \in \mathbb{Q}[X]\}$ est un idéal de $Q[X]$

Proposition 0.22. *Soit I un idéal de A. L'application*

$$\begin{array}{ccc} \{\textit{idéaux de } A \textit{ contenant } I\} & \to & \{\textit{idéaux de } A/I\} \\ J & \mapsto & J/I \end{array}$$

est une bijection.

Démonstration. **TODO** □

Exemple 0.23. Les idéaux de $\mathbb{Z}/n\mathbb{Z}$ sont $m\mathbb{Z}/n\mathbb{Z}$ tel que $m\mathbb{Z} \supseteq n\mathbb{Z}$ c'est-à-dire tels que $m \mid n$.

Proposition 0.24. *Un anneau A est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et A.*

Démonstration. Si A est un corps et $J \subseteq A$ un idéal non nul, alors J contient un élément $x \in A\setminus\{0\}$. Ainsi pour tout $a \in A$, $a = ax^{-1}x \in J$, donc $J = A$. Réciproquement, si les seuls idéaux de A sont $\{0\}$ et A, pour $x \in A \setminus \{0\}$, l'ensemble $\{ax \mid a \in A\}$ est un idéal non nul de A, donc égal à A, d'où il existe $a \in A$ tel que $ax = 1$. □

Corollaire 0.25. *Soit $A \neq 0$ un anneau et K un corps. Tout morphisme d'anneaux $\varphi : K \to A$ est injectif.*

Démonstration. Le noyau $\ker\varphi$ est un idéal de K et $1_K \notin \ker\varphi$ car $\varphi(1_K) = 1_A$ donc $\ker\varphi = \{0\}$. □

Proposition 0.26. *Une intersection d'idéaux est un idéal.*

Définition 0.27. Soit A un anneau et $S \subseteq A$. *L'idéal engendré par S* est le plus petit idéal de A contenant S. On le note (S).

Remarque.

(1) $(S) = \bigcap_{\substack{I \lhd A \\ S \subseteq I}} I$

(2) $(S) = \left\{ \sum_{\text{finie}} as \,\middle|\, a \in A, s \in S \right\}$

(3) Si $S = \{a\}$, alors $(a) = \{ax \mid x \in A\}$ et $(a) = A$ si et seulement si $a \in A^\times$ et $(a) = \{0\}$ si et seulement si $a = 0$.

Définition 0.28. Un idéal I de A est dit *principal* s'il existe $a \in A$ tel que $I = (a)$. Si A est intègre et que tout idéal de A est principal, A est dit *principal*. L'idéal I est dit de *type fini* s'il existe $S \subseteq A$ finie telle que $I = (S)$.

Remarque. Soit A intègre et $a, b \in A \setminus \{0\}$. Alors

$$(a) = (b) \iff \exists x \in A^\times, a = bx$$

Exemple 0.29.

(1) L'idéal (X, Y^2+1) de $\mathbb{Q}[X, Y]$ est celui des polynômes de la forme $P(X, Y)X+Q(X, Y)(Y^2+1)$ avec $P, Q \in \mathbb{Q}[X, Y]$.

(2) On a $(X, X - 1) = \mathbb{Q}[X]$ car $1 = X - (X - 1)$.

Remarque. Il est en général difficile de déterminer si un idéal est de type fini et de trouver un ensemble générateur. Un ensemble générateur d'un idéal n'est pas unique, par exemple $(1) = (X, X-1)$ ou $(X - Y, Y) = (X, Y) = (X, Y, X + Y)$.

0.3 Idéaux premiers et maximaux

Définition 0.30.

(1) Un idéal $\mathfrak{p}$ de A est dit *premier* si $\mathfrak{p} \neq A$ et pour tous $a, b \in A$, $ab \in \mathfrak{p}$ implique $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$.

(2) Un idéal $\mathfrak{m}$ de A est dit *maximal* si $\mathfrak{m} \neq A$ et que les seuls idéaux de A qui le contiennent sont $\mathfrak{m}$ et A.

Théorème 0.31.

(1) Un idéal $\mathfrak{p}$ de A est premier si et seulement si $A/\mathfrak{p}$ est intègre.

(2) Un idéal $\mathfrak{m}$ de A est maximal si et seulement si $A/\mathfrak{m}$ est un corps.

En particulier, tout idéal maximal est premier.

Démonstration. Soient $a, b \in A$. Alors, $(a+\mathfrak{p})(b+\mathfrak{p}) = \mathfrak{p}$ si et seulement si $ab \in \mathfrak{p}$ si et seulement si $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$ si et seulement si $(a+\mathfrak{p}) = \mathfrak{p}$ ou $b + \mathfrak{p} = \mathfrak{p}$. De cela découle (1).
On sait qu'on a une bijection entre les idéaux de A qui contiennent $\mathfrak{m}$ et les idéaux de $A/\mathfrak{m}$. De cette bijection et du fait que $A/\mathfrak{m}$ est un corps si et seulement si ses seuls idéaux sont $\{0\}$ et lui-même, on déduit (2). □

Exemple 0.32.

(1) $n\mathbb{Z}$ est un idéal premier (ou maximal) de $\mathbb{Z}$ si et seulement si n est premier.

(2) $(P) \subseteq \mathbb{Q}[X_1, \ldots, X_n]$ est premier si et seulement si P nul ou irréductible c'est-à-dire non constant et que si $P = AB$, alors A ou B est constant.

(3) Si K est un corps, (X) est un idéal maximal de $K[X]$ car $K[X]/(X) \simeq K$ (premier théorème d'isomorphisme appliqué au morphisme d'évaluation en 0_K).

(4) Pour $\alpha_1, \ldots, \alpha_n \in K$, l'idéal $(X_1 - \alpha_1, \ldots, X_n - \alpha_n) \subseteq K[X_1, \ldots, X_n]$ est maximal.

Proposition 0.33. *Soit A un anneau commutatif unitaire. Tout idéal propre de A est inclus dans un idéal maximal.*

Démonstration. Soit I un idéal de A distinct de A. On considère $\mathcal{J} = \{J \lhd \mathrm{A} |\ I \subseteq J, J \neq A\}$. Par propreté de I, cet ensemble est non vide. Il est ordonné pour l'inclusion. Soit $\mathcal{A} \subseteq \mathcal{J}$ une partie de $\mathcal{J}$ totalement ordonnée pour l'inclusion. On pose $\bigcup_{J \in \mathcal{A}} J$. C'est un idéal car $\mathcal{A}$ est totalement ordonnée pour l'inclusion. De plus, pour tout $J \in \mathcal{A}$, $1 \notin J$, donc $1 \notin \bigcup_{J \in \mathcal{A}} J$. Ainsi, $\bigcup_{J \in \mathcal{A}} J$ est une borne supérieure de $\mathcal{A}$ dans $\mathcal{J}$. Cela démontre que $\mathcal{J}$ est un ensemble inductif. Ainsi, le lemme de Zorn donne l'existence d'un élément maximal $\mathfrak{m} \in \mathcal{J}$. Par l'absurde, si $\mathfrak{m}$ n'est pas un idéal maximal, on dispose de $J \neq A$ idéal qui contient strictement $\mathfrak{m}$. Cela contredit la maximalité de $\mathfrak{m}$ dans $(\mathcal{J}, \subseteq)$. □

Exemple 0.34.

(1) (X) est un idéal premier mais non maximal de $\mathbb{Z}[X]$.

(2) $(X, 2)$ est un idéal maximal de $\mathbb{Z}[X]$.

(3) $(\mathbb{Q}, +, \cdot_0)$ où $\cdot_0$ est définie par $a \cdot_0 b = 0$ pour tous $a, b \in \mathbb{Q}$ n'a pas d'idéaux maximaux. C'est un anneau non unitaire.

0.4 Anneaux principaux

Remarquons que $\mathbb{Z}$ est un exemple d'anneau principal et $\mathbb{Z}[X]$ un exemple d'anneau non-principal, car $(X, 2) \lhd \mathbb{Z}[X]$ n'est pas principal.

Proposition 0.35. *Soit A un anneau principal. Alors, un idéal propre (distinct de A) et non-trivial (distinct de $\{0\}$) est premier si et seulement s'il est maximal.*

Démonstration. Un idéal maximal est toujours premier. Soit (a) avec $a \in A$ un idéal premier. On a $(a) \neq A$. Soit $(b) \supseteq (a)$ un autre idéal le contenant. Alors, $a = bx$ avec $x \in A$. Par primalité de (a), ou bien $b \in (a)$, dans ce cas $(a) = (b)$, ou bien $x \in (a)$, dans ce cas $x = ay$ avec $y \in A$, donc $a = aby$, donc $by = 1$ par intégrité, donc $(b) = A$. Ainsi (a) est maximal. □

Définition 0.36. Pour $a, b \in A$, on dit que a *divise* b et on écrit $a \mid b$ s'il existe $x \in A$ tel que $b = ax$.

Remarque. Pour $a, b \in A$, $a \mid b$ équivaut à $(b) \subseteq (a)$. Si $x \in A^\times$, alors $x \mid a$ pour tout $a \in A$.

Brièvement, quelques rappels sur $K[X]$.

Théorème 0.37. *Soit K un corps. Alors $K[X]$ est un anneau principal.*

Théorème 0.38. *Soit K un corps. Pour tout polynôme $P \in K[X] \setminus \{0\}$, il existe une unique décomposition $P = \alpha \prod_{i=1}^{d} P_i^{n_i}$ (unique à permutation près des P_i) avec $\alpha \in K^\times$, P_i unitaires et irréductibles et deux à deux distincts.*

Lemme 0.39. *Un idéal (P) est premier si et seulement si $P = 0$ ou P est irréductible.*

Quelques rappels :

(1) L'algorithme de division euclidienne fonctionne dans $K[X]$.

(2) Si $P, Q \in K[X]$ alors leur PGCD est bien défini (à multiplication par un élément de $K^\times$ près) et $(P, Q) = (\mathrm{pgcd}(P, Q))$.

(3) Si $K \subseteq L$ avec L un corps, pour $P, Q \in K[X]$, on a $\mathrm{pgcd}_K(P, Q) = \mathrm{pgcd}_L(P, Q)$.

Référence : Abstract Algebra de Dummit and Foote.

1 Théorie des corps

1.1 Extensions de corps

Définition 1.1. Soit K un corps. Une *K-algèbre* est un anneau A muni d'un morphisme d'anneaux $i : K \to A$ (forcément injectif car K est un corps). Si $K \xrightarrow{i} A$ et $K \xrightarrow{j} B$ sont deux K-algèbres, un *morphisme de K-algèbres* (parfois appelé un *K-morphisme*) est un morphisme d'anneaux $\varphi : A \to B$ tel que $\varphi \circ i = j$.

Définition 1.2. Soit K un corps. Une *extension de corps de K* est un corps L muni d'un morphisme de corps $K \xrightarrow{\theta} L$. On écrit L/K. Une *sous-extension de L/K* est un corps E muni de morphismes de corps $K \xrightarrow{i} E \xrightarrow{j} L$ tels que $j \circ i = \theta$. On écrit $L/E/K$ et on parle de *tour de corps*.

Remarque. Comme le morphisme θ dans la définition précédente est injectif, on fait régulièrement l'abus de notation d'identifier K à $\theta(K)$ pour écrire $K \subseteq L$.

Exemple 1.3.

(1) $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$ sont des extensions de corps.

(2) $\begin{array}{ccc} \mathbb{Q}(i) & \to & \mathbb{C} \\ i & \mapsto & i \end{array}$ et $\begin{array}{ccc} \mathbb{Q}(i) & \to & \mathbb{C} \\ i & \mapsto & -i \end{array}$ sont deux $\mathbb{Q}$-morphismes (où $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$).

(3) $\begin{array}{ccc} \mathbb{Q}(\sqrt[3]{2}) & \to & \mathbb{C} \\ \sqrt[3]{2} & \mapsto & \sqrt[3]{2} \end{array}$ et $\begin{array}{ccc} \mathbb{Q}(\sqrt[3]{2}) & \to & \mathbb{C} \\ \sqrt[3]{2} & \mapsto & j\sqrt[3]{2} \end{array}$ sont deux $\mathbb{Q}$-morphismes, où $j^3 = 1$ et $j \neq 1$ et $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$.

(4) Pour $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ avec p premier, l'application Frob : $\begin{array}{ccc} \mathbb{F}_p(T) & \to & \mathbb{F}_p(T) \\ x & \mapsto & x^p \end{array}$ est un morphisme de corps (donc est injective) mais n'est pas surjective. Le fait que $\mathrm{Frob}(1) = 1$ et $\mathrm{Frob}(xy) = \mathrm{Frob}(x)\,\mathrm{Frob}(y)$ est clair. De plus,

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

Et par primalité de p et comme $p = 0$ dans $\mathbb{Z}/p\mathbb{Z}$, pour $0 < k < p$, $\binom{p}{k} = 0$. Ainsi, $(x+y)^p = x^p + y^p$.

(5) Soit $f : \mathbb{R} \to \mathbb{R}$ un morphisme de corps. Comme $f(1) = 1$, on a $f(n) = n$ pour tout $n \in \mathbb{Z}$, puis $f(r) = r$ pour tout $r \in \mathbb{Q}$, donc f stabilise $\mathbb{Q}$. Pour $x \geq 0$, $x = \sqrt{x}^2$, donc $f(x) = f(\sqrt{x})^2 \geq 0$, donc f préserve $\mathbb{R}^+$. Ainsi, si $x \geq y$, $x - y \geq 0$, donc $f(x-y) \geq 0$, donc $f(x) \geq f(y)$, donc f est croissante. Soit (x_n) une suite réelle telle que $x_n \to x \in \mathbb{R}$. Alors, $x - x_n \to 0$, donc on peut trouver deux suites de rationnels $(r_n), (s_n)$ de limites nulles telles que pour tout n, $r_n \leq x - x_n \leq s_n$. Par croissance de f et comme f préserve $\mathbb{Q}$, $r_n \leq f(x) - f(x_n) \leq s_n$. Ainsi, $f(x_n) \to f(x)$, ce qui démontre que f est continue. Par densité de $\mathbb{Q}$ dans $\mathbb{R}$ et comme $f_{|\mathbb{Q}} = \mathrm{id}$, on en déduit que $f = \mathrm{id}$. Ainsi, le seul automorphisme de corps de $\mathbb{R}$ est l'identité.

Définition 1.4. Soit I un ensemble et $S = (X_i)_{i \in I}$ une famille d'indéterminées indexée par I. On définit :

$$K[X_i \mid i \in I] = \{P(X_{i_n}, \ldots, X_{i_m}) \mid \exists \{i_1, \ldots, i_n\} \subseteq I, P \in K[X_{i_1}, \ldots, X_{i_n}]\}$$

Remarquons que $K[X_i \mid i \in I] = \bigcup_{E \subseteq I \text{ fini}} K[X_i \mid i \in E]$, ce qui permet de définir les lois internes $+$ et $\cdot$ sur $K[X_i \mid i \in I]$. On construit ainsi une structure de K-algèbre sur $K[X_i \mid i \in I]$. De plus, $K[X_i \mid i \in I]$ est intègre.

Définition 1.5. On définit $K(X_i \mid i \in I) = \mathrm{Frac}\, K[X_i \mid i \in I]$. C'est une extension de corps de K.

Exemple 1.6. Soit $I = \mathbb{N}$. Le K-morphisme $\begin{array}{ccc} K(X_i \mid i \in I) & \to & X_i \\ K(X_i \mid i \in I) & \mapsto & X_{i+1} \end{array}$ est un morphisme de corps non surjectif.

Si I est fini, on écrit $I = \{1, 2, \ldots, n\}$ et on a $K[X_i \mid i \in I] = K[X_1, \ldots, X_n]$ et $K(X_i \mid i \in I) = K(X_1, \ldots, X_n)$.

Proposition 1.7. *Si L/K est une extension de corps, alors L est muni d'une structure de K-espace vectoriel par la loi externe* $\begin{array}{ccc} K \times L & \to & L \\ (k,v) & \mapsto & k \cdot_L v \end{array}$ *(ou si on ne fait pas l'identification, $(k,v) \mapsto i(k) \cdot_L v$).*

Définition 1.8. Le *degré* d'une extension de corps L/K est la dimension de L vu comme K-espace vectoriel. On le note $[L : K]$. Si $[L : K] < \infty$, on dira que L/K est une *extension finie*. Si $[L : K] = \infty$, elle est dite *infinie*.

Remarque. Le résultat bien connu d'algèbre linéaire qui dit qu'en dimension finie, toutes les bases ont même cardinal est vrai en général (deux bases dans un espace vectoriel sont toujours en bijection). Ainsi, on peut parler du degré d'une extension infinie de manière plus précise en parlant du cardinal des bases.

Exemple 1.9.

(1) On a $[\mathbb{C} : \mathbb{R}] = 2 = [\mathbb{Q}(i) : \mathbb{Q}]$ et $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

(2) $[\mathbb{R} : \mathbb{Q}]$ est non dénombrable sinon $\mathbb{R}$ serait dénombrable.

(3) $[K(X) : K] = \max(\mathrm{Card}(K), \mathrm{Card}(\mathbb{N}))$. Une base est donnée par

$$\left\{ X^j, \frac{X^i}{P^n} \,\middle|\, j \in \mathbb{N}, i, n \in \mathbb{N}^*, i < \deg P, P \text{ unitaire irréductible dans } K[X] \right\}$$

Théorème 1.10. *Soit $M/L/K$ une tour de corps. Alors*

$$[M : K] = [M : L][L : K]$$

En particulier, M/K est finie si et seulement si M/L et L/K le sont.

Remarque. La relation est à lire : si $\mathcal{B}_1$ est une base de M/L et $\mathcal{B}_2$ une base de L/K, alors $\dim_K M = \mathrm{Card}(\mathcal{B}_1 \times \mathcal{B}_2)$.

Démonstration. Soit $(e_i)_{i \in I}$ une base du L-espace vectoriel M et $(f_j)_{j \in J}$ une base du K-espace vectoriel L. On montre que $(e_i f_i)_{(i,j) \in I \times J}$ est une base de M/K.

Cette famille est libre : si $\sum_{i,j} \lambda_{ij} e_i f_j = 0$ avec $\lambda_{ij} \in K$ presque nulle, alors $\sum_{i \in I} e_i \left(\sum_{j \in J} \lambda_{ij} f_j \right) = 0$. Comme (e_i) est libre sur L, on a pour tout $i \in I$, $\sum_{j \in J} \lambda_{ij} f_j = 0$. Comme (f_j) est libre sur K, les λ_{ij} sont nuls, d'où la liberté. Cette famille est génératrice : pour $x \in M$,

$$x = \sum_{j \in J} \lambda_j f_j = \sum_{j \in J} \sum_{i \in I} \mu_i e_i f_j$$

Où les $\lambda_j \in L$ existent car (f_j) engendre M et les $\mu_i \in K$ existent car (e_i) engendre L. □

Définition 1.11. Soit L/K une extension de corps et $S \subseteq L$.

(1) Le *sous-anneau de L/K engendré par S*, noté $K[S]$, est défini par

$$K[S] = \bigcap_{\substack{K \cup S \subseteq A \subseteq L \\ A \text{ sous-anneau} \\ \text{de } L}} A$$

C'est le plus petit sous-anneau de L qui contient K et S.

(2) La *sous-extension L/K engendrée par S*, notée $K(S)$ est définie par

$$K(S) = \bigcap_{\substack{K \cup S \subseteq E \subseteq L \\ E \text{ sous-corps} \\ \text{de } L}} E$$

C'est le plus petit sous-corps de L qui contient K et S.

(3) On dira que L/K est *de type fini* s'il existe $S \subseteq L$ fini tel que $L = K(S)$.

Remarque.

(1) On a $K[S] = \mathrm{Vect}_K(\mathcal{B})$ avec $\mathcal{B} = \left\{ \prod_{\text{fini}} \alpha \;\middle|\; \alpha \in S \right\}$.

(2) On a $K(S) = \mathrm{Frac}\, K[S]$. Si $S = \{a_1, \ldots, a_n\} \subseteq L$, on écrira $K[a_1, \ldots, a_n]$ et $K(a_1, \ldots, a_n)$ pour $K[S]$ et $K(S)$, respectivement.
On a alors $K[a_1, \ldots, a_n] = \{P(a_1, \ldots, a_n) \mid P \in K[X_1, \ldots, X_n]\}$.

(3) $K(S) = \bigcup_{\substack{A \subseteq S \\ \text{finie}}} K(A)$ car $\bigcup_{A \text{ finie}} K(A)$ est un corps.

(4) Toute extension de corps finie est de type fini (car une base est un ensemble générateur).

Exemple 1.12.

(1) $\mathbb{Q}(\mu_n)/\mathbb{Q}$ avec $\mu_n \in \mathbb{C}$ une racine primitive n-ième de l'unité où $n \in \mathbb{N}^*$ est une extension finie. On remarque que $\mathbb{Q}(\mu_n) = \mathbb{Q}[\mu_n]$ car $\mu_n^n = 1$. On dit que $\mathbb{Q}(\mu_n)/\mathbb{Q}$ est une *extension cyclotomique*.

(2) $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est finie.

(3) $K(X)/K$ est de type fini, mais pas finie.

(4) $K(X_n \mid n \in \mathbb{N})/K$ n'est pas de type fini. $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$ ne le sont pas non plus. On verra cela en utilisant des bases de transcendance.

1.2 Extensions algébriques et transcendantes

Définition 1.13. Soit L/K une extension de corps. Un élément $\alpha \in L$ est dit *algébrique sur K* s'il existe $P \in K[X] \setminus \{0\}$ tel que $P(\alpha) = 0$. Sinon, il est dit *transcendant sur K*. L'extension L/K est dite *algébrique* si tout élément de L est algébrique sur K. Sinon, on dira qu'elle est *transcendante*.

Exemple 1.14.

(1) e est transcendant dans $\mathbb{C}/\mathbb{Q}$ (Hermite 1873). π est transcendant dans $\mathbb{C}/\mathbb{Q}$ (Lindemann 1882).

(2) $\sqrt{2}$ et $\sqrt[n]{n}$ sont algébriques dans $\mathbb{C}/\mathbb{Q}$.

(3) $2^{\sqrt{2}}$ est transcendant dans $\mathbb{R}/\mathbb{Q}$ (Gelfond-Schneider 1934).

(4) On ne sait pas si $e + \pi$ ou $e - \pi$ sont transcendants.

Théorème 1.15. *Soit $\alpha \in L$. Soit* $E_\alpha : \begin{array}{ccc} K[X] & \to & L \\ P(X) & \mapsto & P(\alpha) \end{array}$ *. C'est un K-morphisme d'anneaux.*

De plus :

(1) *L'élément α est transcendant dans L/K si et seulement si E_α est injectif. Dans ce cas, il induit un isomorphisme de K-algèbres $K[X] \simeq K[\alpha]$ qui se prolonge en un K-isomorphisme $K(X) \to K(\alpha)$. Dans ce cas, $\dim_K K[\alpha]$ et $\dim_K K(\alpha)$ sont infinies.*

(2) *L'élément α est algébrique dans L/K si et seulement si E_α n'est pas injectif. Dans ce cas, il existe un unique polynôme unitaire P_α dans $K[X]$ de degré minimal tel que $P_\alpha(\alpha) = 0$. Ce polynôme est irréductible sur K. De plus, $K[\alpha] = K(\alpha) \simeq K[X]/(P_\alpha)$ et $[K(\alpha) : K] = \deg P_\alpha$.*

Définition 1.16. Le polynôme $P_\alpha \in K[X]$ issu du théorème précédent est appelé le *polynôme minimal de $\alpha \in L$ sur K.*

Preuve du théorème 1.15.

(1) L'élément α est transcendant si et seulement si E_α est injectif par définition. Alors, $E_\alpha(K[X]) \simeq \mathrm{Im}(E_\alpha) = K[\alpha]$, donc E_α induit un K-isomorphisme $K[X] \xrightarrow{\sim} K[\alpha]$ et il se prolonge à $K(X) \xrightarrow{\sim} K(\alpha)$ par $\frac{P}{Q} \mapsto P(\alpha)Q(\alpha)^{-1}$ (bien défini car $Q(\alpha) \neq 0$ pour $Q \in K[X] \setminus \{0\}$).

(2) L'élément α est algébrique si et seulement si $\ker E_\alpha \neq \{0\}$ par définition. Comme $K[X]$ est principal, $\ker E_\alpha = (P_\alpha)$ pour un certain polynôme $P_\alpha \in K[X]$ qu'on peut choisir unitaire. Ce polynôme est de degré minimal dans $\ker E_\alpha \setminus \{0\}$. De plus, $\ker E_\alpha$ est premier, donc P_α est irréductible. Comme $K[X]$ est principal, $\ker E_\alpha$ est maximal, donc $K[X]/(\ker E_\alpha)$ est un corps, isomorphe à $K[\alpha]$ par théorème d'isomorphisme. En particulier, $K(\alpha) = K[\alpha]$. En notant $n = \deg P_\alpha$, $\{1, \alpha, \dots, \alpha^{n-1}\}$ est une base de $K[\alpha]/K$. En effet, elle est libre, sinon on aurait un polynôme de $K[X]$ annulateur de α de degré strictement plus petit que $\deg P_\alpha$. De plus, pour $x \in K[\alpha]$, il existe $T \in K[X]$ tel que $x = T(\alpha)$. Par division euclidienne, on a $T = QP_\alpha + R$ avec $\deg R < n$, donc $T(\alpha) = R(\alpha)$, donc $x \in \mathrm{Vect}(1, \alpha, \dots, \alpha^{n-1})$. On a donc $[K(\alpha) : K] = \dim_K K[\alpha] = \deg P_\alpha$.

□

Remarque.

(1) On a aussi montré que $[K[X]/(P_\alpha) : K] = \deg P_\alpha$ et que $K[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \mid a_i \in K\}$, où $\alpha \in L$ est algébrique sur K et $n = \deg P_\alpha$.

(2) Si P est un polynôme irréductible dans $K[X]$, alors (P) est un idéal maximal, donc $L = K[X]/(P)$ est un corps et L/K une extension. Soit $\alpha = X + (P) \in L$. Alors, le morphisme projection $\begin{array}{ccc} K[X] & \to & L \\ X & \mapsto & \alpha \end{array}$ coïncide avec E_α. Dans ce cas, $P_\alpha = uP$ où $u \in K^\times$ est tel que P_α soit unitaire. On a alors $[L : K] = \deg P$.

(3) Pour $\alpha \in L$ algébrique sur K et $Q \in K[X]$, on a $Q(\alpha) = 0$ si et seulement si $P_\alpha \mid Q$ dans $K[X]$.

Exemple 1.17.

(1) Dans $\mathbb{C}/\mathbb{R}$, tout polynôme minimal d'un élément de $\mathbb{C}$ est de degré au plus 2.

(2) Dans $K(X)/K$, l'élément transcendant X est transcendant sur K.

(3) Dans $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, le polynôme minimal de $a + b\sqrt{2}$ avec $b \neq 0$ est $(X - a)^2 - 2b^2 \in \mathbb{Q}[X]$.

Proposition 1.18. *Tout extension de corps finie est algébrique.*

Démonstration. Soit L/K une extension finie. Soit $\alpha \in L$. Alors, $K(\alpha)/K$ est aussi finie, donc α est algébrique. □

Exemple 1.19. On verra plus tard que $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algébrique dans } \mathbb{C}/\mathbb{Q}\}$ est dénombrable. Remarquons que par définition, $\overline{\mathbb{Q}}/\mathbb{Q}$ est algébrique. De plus, on démontrera que $\overline{\mathbb{Q}}/\mathbb{Q}$ n'est pas finie et donc pas de type fini.

Corollaire 1.20. *Soit L/K une extension de type fini. Si L est engendré par des éléments algébriques, alors L/K est finie et algébrique.*

Démonstration. Soit $L/E/K$ une tour de corps telle que E/K soit finie et algébrique et $x \in L$ algébrique sur K. Alors, x est algébrique sur E donc $E(x)/E$ est finie donc $E(x)/K$ est finie (donc algébrique) par le théorème 1.10. Le corollaire suit par récurrence sur le cardinal de l'ensemble générateur. □

Corollaire 1.21. *La somme et le produit de deux éléments algébriques de L/K sont algébriques. L'ensemble des éléments algébriques de L/K est une sous-extension, notée $\overline{K}^L$ et appelée* clôture algébrique de K dans L. *De plus, $\overline{K}^L/K$ est algébrique.*

Démonstration. Soient $x, y \in L$ algébriques sur K. Alors, $K(x,y)/K$ est une extension algébrique par ce qui précède. Comme $x - y, xy \in K(x,y)$ (et $y^{-1} \in K(x,y)$ si $y \neq 0$), ces éléments sont algébriques sur K. Le reste en découle. □

Exemple 1.22.

(1) L'extension $\mathbb{R}/\mathbb{Q}$ n'est ni algébrique, ni de type fini.
(2) L'extension $K(X)/K$ est de type fini mais pas algébrique.
(3) L'extension $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est algébrique et finie.
(4) L'extension $\overline{\mathbb{Q}}/\mathbb{Q}$ où $\overline{\mathbb{Q}}$ est la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ n'est pas de type fini ou finie mais est algébrique.

Définition 1.23. Soit L/K une extension. Si $\overline{K}^L = K$, on dit que K *est algébriquement clos dans* L. Remarquons qu'alors l'extension $L/\overline{K}^L$ est totalement transcendante.

Corollaire 1.24. *Une extension de corps engendrées par des éléments algébriques est algébrique.*

Démonstration. Soit L/K une extension de corps et $S \subseteq L$ où S contient uniquement des éléments algébriques sur K tel que $L = K(S)$. Alors, $S \subseteq \overline{K}^L$ et L/K est algébrique. □

Proposition 1.25. *Soit $M/L/K$ une tour de corps. Alors, M/K est algébrique si et seulement si M/L et L/K le sont.*

Démonstration. Le sens direct est clair. Supposons donc M/L et L/K algébriques. Soit $\alpha \in M$. On dispose de $P = \sum_{i=0}^{n} a_i X^i \in L[X]$ non nul tel que $P(\alpha) = 0$. Alors, α est algébrique dans $M/K(a_1, \ldots, a_n)$. Alors, $[K(a_0, \ldots, a_n)(\alpha) : K(a_0, \ldots, a_n)] < \infty$. De plus, les éléments a_i sont algébriques sur K car L/K est algébrique, donc $[K(a_0, \ldots, a_n) : K] < \infty$. Le théorème 1.10 donne $[K(a_0, \ldots, a_n)(\alpha) : K] < \infty$, ce qui démontre que α est algébrique sur K. Ainsi, M/K est algébrique. □

1.3 Degré de transcendance

Définition 1.26. Soit L/K une extension de corps. Une famille $(\alpha_i)_{i\in I}$ d'éléments de L est dite *algébriquement indépendante* sur K si le morphisme de K algèbres $\begin{array}{ccc} K[X_i \mid i \in I] & \to & L \\ X_i & \mapsto & \alpha_i \end{array}$ est injectif. L'extension L/K est dite *transcendante pure* si elle est engendrée par une famille algébriquement indépendante. Cela est équivalent à demander que L soit K-isomorphe à $K(X_i \mid i \in I)$.

Remarque.

(1) La famille d'éléments $(\alpha_i)_{i\in I}$ de L/K est algébriquement indépendante si et seulement si pour tout $\{i_1, \ldots, i_n\} \subseteq I$ et pour tout $P(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, on a $P(\alpha_{i_1}, \ldots, \alpha_{i_n}) \neq 0$.

(2) Si $(\alpha_i)_{i\in I}$ est algébriquement indépendante dans L/K, le K-morphisme $\begin{array}{ccc} K[X_i \mid i \in I] & \to & L \\ X_i & \mapsto & \alpha_i \end{array}$ est injectif et se prolonge donc à un K-morphisme de corps $\begin{array}{ccc} K(X_i \mid i \in I) & \to & L \\ \frac{P(X_{i_1},\ldots,X_{i_n})}{Q(X_{j_1},\ldots,X_{j_m})} & \mapsto & \frac{P(\alpha_{i_1},\ldots,\alpha_{i_n})}{Q(\alpha_{j_1},\ldots,\alpha_{j_m})} \end{array}$ qui a pour image $K(\alpha_i \mid i \in I)$.

Lemme 1.27. *Soit L/K une extension de corps et $S \subseteq L$ un ensemble algébriquement indépendant dans L/K. Soit $x \in L \setminus S$. Alors $S \cup \{x\}$ est algébriquement indépendant dans L/K si et seulement si x est transcendant dans $L/K(S)$.*

Démonstration. Supposons x algébrique dans $L/K(S)$. Soit $P \in K(S)[X] \setminus \{0\}$ tel que $P(x) = 0$. On écrit $P = \sum_{i=0}^{n} a_i X^i$ avec $a_i \in K(S)$. On dispose alors de $\exists b_i, c_i \in K[S]$ tels que $a_i = \frac{b_i}{c_i}$ avec les c_i non nuls. En multipliant P par $\prod_i c_i$, on obtient un polynôme $P_1 \in K[S][X] \setminus \{0\}$ qui annule x. Comme S est algébriquement indépendant, le morphisme $\begin{array}{ccc} K[X_s \mid s \in S] & \to & K[S] \\ X_s & \mapsto & s \end{array}$ est injectif. Par l'absurde, si $S \cup \{x\}$ est algébriquement indépendant, on a

$$\begin{array}{ccccc} K[X, X_s \mid s \in S] & \hookrightarrow & K[S][X] & \hookrightarrow & L \\ X_s & \longmapsto & s & \longmapsto & s \\ X & \longmapsto & X & \longmapsto & x \end{array}$$

Ce qui contredit l'existence de $P_1 \in K[S][X] \setminus \{0\}$ qui annule x.
Réciproquement, supposons x transcendant dans $L/K(S)$. Comme S est algébriquement indépendant, le K-morphisme $\begin{array}{ccc} K[X_s \mid s \in S] & \to & K(S) \\ X_s & \mapsto & s \end{array}$ est injectif. La transcendance de x implique que le $K(S)$-morphisme $\begin{array}{ccc} K(S)[X] & \to & L \\ X & \mapsto & x \end{array}$ est injectif. Donc, le K-morphisme

$$\begin{array}{ccc} K[X, X_s \mid s \in S] & \to & L \\ X_s & \mapsto & s \\ X \mapsto x & & \end{array}$$

est injectif, d'où $S \cup \{x\}$ est algébriquement indépendant dans L/K. □

Exemple 1.28.

(1) L'ensemble $\{\pi, \pi - 1\}$ n'est pas algébriquement indépendant dans $\mathbb{R}/\mathbb{Q}$.

(2) On ne sait pas si $\{\pi, e\}$ est algébriquement indépendant dans $\mathbb{R}/\mathbb{Q}$ et donc on ne sait pas si $\mathbb{Q}(\pi, e)/\mathbb{Q}$ est purement transcendante.

(3) $\{\sqrt{2}, \pi\}$ n'est pas algébriquement indépendant dans $\mathbb{R}/\mathbb{Q}$ et $\mathbb{Q}(\sqrt{2}, \pi)/\mathbb{Q}$ n'est pas transcendante pure.

(4) $K(X_1, \ldots, X_n)/K$ est transcendante pure.

(5) $\mathbb{R}(X, \sqrt{1 - X^2})/\mathbb{R}$ est transcendante pure car égale à $\mathbb{R}\left(\frac{1-X}{\sqrt{1-X^2}}\right)/\mathbb{R}$ (paramétrisation du cercle).

(6) $\mathbb{Q}(X, \sqrt{X^3 - X})/\mathbb{Q}$ n'est pas transcendante pure, même si elle est transcendante.

(7) Dans la tour $\mathbb{R}(X, Y)/\mathbb{R}(X + Y)/\mathbb{R}$, l'extension $\mathbb{R}(X, Y)/\mathbb{R}(X + Y)$ est transcendante pure.

Définition 1.29. Une *base de transcendance pour* L/K est un sous-ensemble algébriquement indépendant dans L/K maximal.

Lemme 1.30. *Un ensemble algébriquement indépendant $S \subseteq L$ est une base de transcendance de L/K si et seulement si $L/K(S)$ est algébrique.*

Démonstration. Le lemme précédent nous dit qu'on peut ajouter un élément x à S en préservant l'indépendance algébrique si et seulement si x est transcendant dans $L/K(S)$, ce qui conclut. □

Théorème 1.31. *Soit L/K une extension. Elle contient une base de transcendance. Toute les bases de transcendance de L/K ont même cardinal.*

Définition 1.32. Le cardinal commun des bases de transcendance d'une extension L/K est appelé le *degré de transcendance de* L/K et noté $\mathrm{degtr}(L/K)$.

Preuve de l'existence. Soit $E \subseteq L$ un ensemble algébriquement indépendant dans L/K. Soit $S \subseteq L$ un ensemble générateur de L/K tel que $E \subseteq S$. Soit

$$\mathcal{B} = \{U \subseteq L \mid U \text{ algébriquement indépendant}, E \subseteq U \subseteq S\}$$

C'est un ensemble non vide ordonné pour l'inclusion. Soit $(T_i)_{i \in I}$ une chaîne dans $\mathcal{B}$. Alors, $\bigcup_i T_i \in \mathcal{B}$ est un majorant de la chaîne. En effet, si des éléments $a_1, \ldots, a_n$ dans l'union sont annulés par un polynôme P, comme (T_i) est totalement ordonné pour l'inclusion, ces éléments sont contenus dans un certain T_j qui est algébriquement indépendant, donc $P = 0$, donc l'union est bien dans $\mathcal{B}$. Par le lemme de Zorn, on dispose d'un ensemble algébriquement indépendant maximal B contenu dans S.
S'il existe $t \in S \setminus B$ tel que t est transcendant sur $L/K(B)$, alors $B \cup \{t\} \subseteq S$ est algébriquement indépendant par le lemme 1.27. Cela contredit la maximalité de B, donc tout $t \in S \setminus B$ est algébrique sur $L/K(B)$, d'où $\underbrace{K(B)(S \setminus B)}_{L}/K(B)$ est algébrique et on conclut que B est une base de transcendance par le lemme 1.30. □

Remarque. La preuve précédente montre que tout ensemble générateur de l'extension L/K contient une base de transcendance.

Preuve de l'unicité des cardinaux. Soient $B_1, B_2 \subseteq L$ deux bases de transcendance de L/K. Quitte à permuter, on suppose $\mathrm{Card}(B_1) \leq \mathrm{Card}(B_2)$.
Supposons d'abord $\mathrm{Card}(B_2)$ infini. Pour $\alpha \in B_1$, il existe $B_\alpha \subseteq B_2$ fini tel que α est algébrique sur $K(B_\alpha)$. Soit $B' = \bigcup_{\alpha \in B_1} B_\alpha$. Soit $\beta \in B_2 \setminus B'$. Alors β est algébrique dans $L/K(B_1)$ et $K(B_1)/K(B')$ est algébrique. Ainsi β est algébrique dans $L/K(B')$, ce qui est absurde car $B' \cup \{\beta\} \subseteq B_2$ n'est pas algébriquement indépendante. Ainsi $B_2 = B'$, d'où B_1 est infinie et $\square$