Annexes sur les extensions de corps et limites directes/inverses

HAJASOA Fanantenana M1 MAFI

Annexe A - Extensions de corps

1. Corps et sous-corps

Dans tout ce cours, nous entendrons par corps un anneau commutatif K vérifiant $K^* = K \setminus \{0\}$.

Définition 1 (A.1.1)**.** *Soit K un corps. Une extension de K est un couple (L, j) où L est un corps et $j : K \to L$ un homomorphisme de corps.*

Comme un homomorphisme de corps est injectif (les seuls idéaux de K sont l'idéal nul et K), on peut identifier K et $j(K)$ et considérer K comme un sous-corps de L. Ainsi, dans toute la suite, une extension d'un corps K est un corps L tel que $L \supseteq K$. On écrit aussi L/K pour dire que L est une extension de K.

Il est clair que si L est une extension de K alors L est un K-espace vectoriel et aussi une K-algèbre.

Définition 2 (A.1.2)**.** *On appelle degré de l'extension L/K et on note $[L : K]$ la dimension de L en tant que K-espace vectoriel.*

Définition 3 (A.1.3)**.** *On dit que le corps K est premier s'il n'admet pas de sous-corps propre.*

Exemple 1 (A.1.4)**.** — *L'intersection des sous-corps de K est un corps premier. C'est le sous-corps premier de K.*

— *Le corps $\mathbb{Q}$ des rationnels est un corps premier. En effet, un sous-corps de $\mathbb{Q}$ contient le sous-anneau de $\mathbb{Q}$ engendré par 1. Donc il contient $\mathbb{Z}$.*

— *Pour p premier, d'après le théorème de Lagrange, le corps $\mathbb{Z}/p\mathbb{Z}$ est premier.*

Proposition 1 (A.1.5)**.** *Soit K un corps.*

(a) Si car$(K) = 0$ alors le sous-corps premier de K est isomorphe à $\mathbb{Q}$.

(b) Si car$(K) = p$ (premier) alors le sous-corps premier de K est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Démonstration. Il suffit de considérer l'homomorphisme d'anneaux $\mathbb{Z} \to K$ tel que $f(n) = n \cdot 1$ en se rappelant que la caractéristique d'un anneau intègre est, soit nulle, soit un nombre premier p (voir [Raz25a]). D'après le premier théorème d'isomorphisme, K contient, soit un sous-corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$, soit un sous-anneau isomorphe à $\mathbb{Z}$. $\square$

Définition 4 (A.1.6)**.** *Soit l'extension L/K. Un K-automorphisme de L est un automorphisme de L en tant que K-algèbre. C'est donc un automorphisme du corps L qui laisse invariant les éléments de K. On note Gal(L/K) l'ensemble des K-automorphismes de L. C'est un groupe pour la loi de composition des applications. On l'appelle le groupe de Galois de l'extension L/K.*

Proposition 2 (A.1.7)**.** *Soient K un corps et P son sous-corps premier. On a $Aut(K) = Gal(K/P)$.*

Démonstration. Il est clair que $\mathrm{Gal}(K/P) \subseteq \mathrm{Aut}(K)$.

Soit $f \in \mathrm{Aut}(K)$. On a $K^f = \{x \in K, f(x) = x\}$ est un sous-corps de K. Ainsi $P \subseteq K^f$ et $f \in \mathrm{Gal}(K/P)$. $\square$

Exemple 2 (A.1.8)**.** *On a $Aut(\mathbb{R}) = Gal(\mathbb{R}/\mathbb{Q}) = \{id_{\mathbb{R}}\}$.*

En effet, d'après la proposition précédente, on a déjà $Aut(\mathbb{R}) = Gal(\mathbb{R}/\mathbb{Q})$. Soit $x \in \mathbb{R}$ avec $x > 0$. Si $f \in Gal(\mathbb{R}/\mathbb{Q})$ alors $f(x) = f(\sqrt{x^2}) = f(\sqrt{x})^2 \geq 0$. Comme f est injectif, on a $f(x) > 0$. Il vient que si $a - b > 0$ alors $f(a - b) = f(a) - f(b) > 0$ et f est strictement croissant.

Soit alors $x \in \mathbb{R} \setminus \mathbb{Q}$. Si $f(x) < x$ alors il existe $r \in \mathbb{Q}$ tel que $f(x) < r < x$. Dans ce cas, $f(f(x)) < f(r) = r < f(x)$. Ce qui est absurde. De la même manière, on ne peut pas avoir $f(x) > x$.

Définition 5 (A.1.9)**.** *Soit l'extension L/K et soit $A \subseteq L$. On désigne par $K(A)$ le sous-corps de L engendré par K et A. On dit aussi que $K(A)$ est le sous-corps de L engendré par A sur K. C'est l'intersection des sous-corps de L contenant K et A.*

Si $A = \{\alpha_1, ..., \alpha_r\}$, on écrit simplement $K(\alpha_1, ..., \alpha_r)$ et on dit que $K(\alpha_1, ..., \alpha_r)/K$ est une extension de type fini. Si $A = \{\alpha\}$, on dit que $K(\alpha)$ est une extension simple de K.

2. Éléments algébriques, éléments transcendants

Soit une extension $K \subseteq L$ et soit $\alpha \in L$. Le plus petit sous-anneau de L contenant K et α est l'ensemble $K[\alpha]$ des expressions polynomiales en α. Son corps des fractions, noté $K(\alpha)$, est le plus petit sous-corps de L contenant K et α. Soit X une indéterminée et soit l'homomorphisme d'anneaux

$$\varepsilon_\alpha : K[X] \longrightarrow K[\alpha]$$

défini par $\varepsilon_\alpha(a) = a$ si $a \in K$ et $\varepsilon_\alpha(X) = \alpha$. Il est clair que ε_α est surjectif. Deux cas peuvent se présenter selon que $\ker(\varepsilon_\alpha)$ est nul ou non.

Définition 6 (A.2.1)**.** *On dit que α est transcendant sur K si $\ker(\varepsilon_\alpha) = (0)$, et α est algébrique sur K si $\ker(\varepsilon_\alpha) \neq (0)$.*

(a) Si α est transcendant sur K, il n'existe pas de polynôme non nul de $K[X]$ qui admet α comme racine. Dans ce cas, ε_α est un isomorphisme d'anneaux principaux $K[X] \longrightarrow K[\alpha]$.

(b) Si α est algébrique sur K, il existe un polynôme non nul de $K[X]$ qui s'annule en α. Soit P un générateur de $\ker(\varepsilon_\alpha)$ dans l'anneau principal $K[X]$. Puisque $K[X]/(P)$ est isomorphe à l'anneau intègre $K[\alpha]$, l'idéal (P) est un idéal premier, donc maximal, de $K[X]$ et P est un élément irréductible de $K[X]$. Il s'ensuit que $K[\alpha]$ est un corps et $K[\alpha] = K(\alpha)$.

Définition 7 (A.2.2)**.** *Si α est algébrique sur K, on appelle polynôme minimal de α sur K et on note $m_{\alpha,K}$, ou simplement m_α si le contexte est clair, le générateur unitaire de $\ker(\varepsilon_\alpha)$. Le degré de α est le degré de son polynôme minimal.*

Proposition 3 (A.2.3)**.** *Soit l'extension L/K et soit $\alpha \in L$. Les assertions suivantes sont équivalentes :*

(a) L'élément α est algébrique sur K.

(b) On a l'égalité $K[\alpha] = K(\alpha)$.

(c) Le K-espace vectoriel $K(\alpha)$ est de dimension finie.

Plus précisément, si $[K(\alpha) : K]$ est fini alors $[K(\alpha) : K] = \deg \alpha$.

Démonstration. On a déjà (1)implique(2). Réciproquement, si $K[\alpha] = K(\alpha)$ alors l'homomorphisme ε_α n'est pas injectif et α est algébrique sur K.

(1)implique(3) Soit $x = F(\alpha)$ avec $F \in K[X]$. On a $F(X) = Q(X)m_\alpha(X) + R(X)$ avec $\deg R < \deg m_\alpha$ ou $R = 0$. Ainsi $x = R(\alpha)$ et $(1, \alpha, ..., \alpha^{\deg \alpha - 1})$ est un système générateur de $K(\alpha)$.

(3)implique (1) Si $[K(\alpha) : K] = n$, fini, la famille $(1, \alpha, ..., \alpha^n)$ n'est pas libre sur K. A partir d'une relation de dépendance linéaire entre les éléments de cette famille on obtient un polynôme non nul de $K[X]$, de degré n, qui s'annule en α.

Enfin, si $[K(\alpha) : K]$ est fini, le système générateur $(1, \alpha, ..., \alpha^{\deg \alpha - 1})$ est un système libre sinon il existerait un polynôme non nul $F \in K[X]$ tel que $\deg F < \deg m_\alpha$ et $F \in (m_\alpha) = \ker(\varepsilon_\alpha)$. $\square$

3. Extensions finies

Définition 8 (A.3.1)**.** *L'extension L/K est dite finie si la dimension de L en tant que K-espace vectoriel est finie.*

Remarque 1 (A.3.2)**.** *Une extension de type fini n'est pas nécessairement finie. Si $L = K(X)$, le corps des fractions rationnelles en l'indéterminée X alors X n'est pas algébrique sur K de sorte que la dimension de L en tant que K-espace vectoriel n'est pas finie.*

Définition 9 (A.3.3)**.** *On appelle corps de nombres toute extension finie du corps des rationnels $\mathbb{Q}$.*

Proposition 4 (A.3.4)**.** *Si L/K et K/H sont des extensions finies alors L/H est une extension finie et $[L : H] = [L : K][K : H]$.*

Démonstration. Soient $(k_i)_{1 \leq i \leq m}$ une H-base de K et $(l_j)_{1 \leq j \leq n}$ une K-base de L. Si $\gamma \in L$ alors

$$\gamma = \sum_{j=1}^{n} \alpha_j l_j \quad \text{avec } \alpha_j \in K,$$

$$\alpha_j = \sum_{i=1}^{m} \alpha_{ij} k_i \quad \text{avec } \alpha_{ij} \in H.$$

Et, en regroupant

$$\gamma = \sum_{j=1}^{n} \sum_{i=1}^{m} \alpha_{ij} k_i l_j.$$

Ainsi, $(k_i l_j)_{1 \leq i \leq m, 1 \leq j \leq n}$ est un système générateur de L sur H.

Si $\sum_{i,j} \alpha_{ij} k_i l_j = \sum_j (\sum_i \alpha_{ij} k_i) l_j = 0$ alors, comme $\sum_i \alpha_{ij} k_i \in K$, pour tout j on a $\sum_i \alpha_{ij} k_i = 0$. Donc $\alpha_{ij} = 0$ pour tout i, j et $(k_i l_j)_{1 \leq i \leq m, 1 \leq j \leq n}$ est une H-base de L. □

Corollaire 1 (A.3.5). *Si $[L : K] = n$, fini, alors tout élément de L est algébrique sur K et de degré un diviseur de n.*

Démonstration. Si $x \in L$, alors la famille $(1, x, ..., x^n)$ est K-liée. On obtient alors un élément non nul de $K[X]$ qui s'annule en x. Il suffit alors de remarquer que $n = [L : K] = [L : K(x)][K(x) : K]$.

Soit l'extension finie L/K. Si $\alpha \in L$, on considère le K-endomorphisme δ_α de L défini par $\delta_\alpha(x) = \alpha x$. □

Définition 10 (A.3.6). *On appelle trace (resp. norme) de α relativement à L/K et on note $Tr_{L/K}(\alpha)$ (resp. $N_{L/K}(\alpha)$) la trace (resp. le déterminant) de δ_α.*

$$Tr_{L/K}(\alpha) = Tr(\delta_\alpha) \quad N_{L/K}(\alpha) = \det(\delta_\alpha).$$

Définition 11 (A.3.7). *On appelle polynôme caractéristique de α relativement à L/K et on note $c_{\alpha,L/K}$ (ou c_α quand le contexte est clair) le polynôme caractéristique de δ_α,*

$$c_{\alpha,L/K}(X) = \det(X id - \delta_\alpha).$$

Proposition 5 (A.3.8). *On a*

$$c_{\alpha,L/K}(X) = m_{\alpha,K}(X)^{[L:K(\alpha)]}.$$

Démonstration. Supposons d'abord que $L = K(\alpha)$. D'après le théorème de Cayley-Hamilton, $c_\alpha(\delta_\alpha) = 0$. On a alors $c_\alpha(\alpha) = 0$ et $m_\alpha \mid c_\alpha$. Comme ces polynômes sont unitaires et de même degré, $c_\alpha = m_\alpha$.

Dans le cas général, soit (k_i) une K-base de $K(\alpha)$ et soit (l_j) une $K(\alpha)$-base de L. Comme dans la preuve du théorème A.3.4, la famille $(k_i l_j)$ est une K-base de L.

On a $\delta_\alpha(k_i) = \sum_j a_{ij}k_j$ et d'après la première partie, le polynôme caractéristique de la matrice $A = (a_{ij})$, qui est une matrice carrée $[K(\alpha) : K] \times [K(\alpha) : K]$, n'est autre que m_α. Maintenant, $\delta_\alpha(k_i l_j) = \alpha k_i l_j = \sum_j a_{ij}k_j l_j$, de sorte que la matrice de δ_α dans la base $(k_i l_j)$ est formée de $[L : K(\alpha)]$ blocs diagonaux tous égaux à A. D'où le résultat. □

4. Extensions algébriques

Définition 12 (A.4.1)**.** *L'extension L/K est dite algébrique si tout élément de L est algébrique sur K. Dans le cas contraire, on dit que l'extension L/K est transcendante.*

On a déjà vu que si l'extension L/K est finie alors elle est algébrique (voir corollaire A.3.5).

Proposition 6 (A.4.2)**.** *Soit $L = K(\alpha_1, \ldots, \alpha_n)$ une extension de type fini de K. Si les α_i sont algébriques sur K alors L/K est finie (donc algébrique) et $L = K[\alpha_1, \ldots, \alpha_n]$.*

Démonstration. On raisonne par récurrence sur n. On a déjà vu le résultat pour $n = 1$. Supposons alors $n > 1$ et posons $H = K(\alpha_1, \ldots, \alpha_{n-1})$. Par hypothèse de récurrence, H/K est fini et $H = K[\alpha_1, \ldots, \alpha_{n-1}]$. Puisque α_n est algébrique sur H, on a $H(\alpha_n)/H$ fini et $L = H(\alpha_n) = H[\alpha_n]$. Il vient que $[L : K] = [L : H][H : K]$ est fini. □

Proposition 7 (A.4.3)**.** *Si L/K et K/H sont algébriques alors L/H est algébrique.*

Démonstration. Soit $\alpha \in L$ et soit $m_{\alpha,K}(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$ son polynôme minimal sur K. Considérons alors le corps $M = H(a_0, \ldots, a_{n-1})$. Puisque les a_i sont algébriques sur H (ils appartiennent à K), l'extension M/H est finie. Comme α est évidemment algébrique sur M, l'extension $M(\alpha)/M$ est finie et $[M(\alpha) : H] = [M(\alpha) : M][M : H]$ est fini. Ce qui montre que α est algébrique sur H. □

En examinant les résultats précédents, une question se pose. Soit $K(\alpha_1, \ldots, \alpha_n)$ une extension de type fini de K. Si $K(\alpha_1, \ldots, \alpha_n) = K[\alpha_1, \ldots, \alpha_n]$, peut-on dire que les α_i sont algébriques sur K ?

Remarque 2 (A.4.4)**.** *Nous dirons que l'extension L de K est une K-algèbre de type fini s'il existe $\alpha_1, \ldots, \alpha_n \in L$ tels que $L = K[\alpha_1, \ldots, \alpha_n]$.*

Si l'extension L/K est de type fini, L n'est pas nécessairement une K-algèbre de type fini. C'est le cas par exemple du corps des fractions rationnelles en l'indéterminée X. En effet, si $K(X) = K[\tau_1, \ldots, \tau_n]$ et si D est un dénominateur commun des τ_j alors pour tout $z \in K(X)$ il existe $N \in \mathbb{N}$ tel que $D^N z \in K[X]$.

Ce qui est évidemment impossible en prenant $z = 1/c$ avec $c = 1 + d_1 d_2 \cdots d_t$ où les d_i sont les diviseurs irréductibles de D dans l'anneau factoriel $K[X]$.

Theoreme 1 (A.4.5 (Zariski))**.** *Soit l'extension L/K. Si L est une K-algèbre de type fini alors l'extension L/K est finie (donc algébrique).*

Démonstration. Supposons que $L = K[\alpha_1, \ldots, \alpha_n]$ et raisonnons par récurrence sur n. Le cas $n = 1$ est résolu par la proposition A.2.3. Supposons alors $n > 1$ et le résultat vrai pour toute extension engendrée par $t \leq n - 1$ éléments en tant qu'algèbre sur un corps quelconque. Posons $K_1 = K(\alpha_1)$. Par hypothèse de récurrence, $L = K_1[\alpha_2, \ldots, \alpha_n]$ est algébrique sur K_1. Si α_1 est algébrique sur K alors on a le résultat. Supposons alors α_1 transcendant sur K.

Pour $i \geq 2$, on a une équation

$$\alpha_i^m + a_{i1}\alpha_i^{m-1} + \cdots + a_{im-1} = 0 \quad \text{avec } a_{ij} \in K_1.$$

Si a est un dénominateur commun des a_{ij}, on a

$$(a\alpha_i)^m + a_{i1}a(a\alpha_i)^{m-1} + \cdots + a^m a_{im-1} = 0,$$

de sorte que les $a\alpha_i$ sont entiers sur $K[\alpha_1]$. Il vient que pour tout $z \in L$, il existe $N \in \mathbb{N}$ tel que $a^N z$ soit entier sur $K[\alpha_1]$. Comme $K[\alpha_1]$ est intégralement clos (car factoriel), pour tout $z \in L = K[\alpha_1, \ldots, \alpha_n]$, il existe $N \in \mathbb{N}$ tel que $a^N z \in K[\alpha_1]$. En particulier ce résultat serait vrai pour $z \in K(\alpha_1)$. Ce qui est impossible car $K(\alpha_1)$ est isomorphe au corps des fractions rationnelles $K(X)$ et il suffit de prendre $z = 1/c$ avec c premier avec a comme dans la remarque A.4.4. □

Proposition 8 (A.4.6)**.** *Soit l'extension L/K et soit F l'ensemble des éléments de L qui sont algébriques sur K. L'ensemble F est un sous-corps de L qui contient K. C'est la fermeture algébrique de K dans L.*

Démonstration. Il est clair que $K \subseteq F \subseteq L$. Soient $\alpha, \beta \in F$. D'après la proposition A.4.2, $K(\alpha, \beta)$ est une extension algébrique de K et $\alpha \pm \beta$, $\alpha\beta, \alpha/\beta$ (si $\beta \neq 0$) sont dans $K(\alpha, \beta)$. □

5. Extensions transcendantes

Définition 13 (A.5.1)**.** *Soit l'extension L/K. Les éléments $x_1, \ldots, x_n$ de L sont algébriquement indépendants sur K s'il n'existe pas de polynôme non nul $f \in K[X_1, \ldots, X_n]$ tel que $f(x_1, \ldots, x_n) = 0$. Autrement dit, l'anneau engendré par K et les x_i est isomorphe à $K[X_1, \ldots, X_n]$.*

Dire que x est algébriquement libre sur K signifie que x est transcendant sur K.

Il est clair que si la famille des $x_1, \ldots, x_n$ est algébriquement indépendante sur K alors il en est de même de toute partie $\{x_{i_1}, \ldots, x_{i_s}\}$.

Proposition 9 (A.5.2). *Soit l'extension L/K et soient $x_1, \ldots, x_n$ des éléments deux à deux distincts de L. Soit s tel que $1 < s < n$. Alors $x_1, \ldots, x_n$ sont algébriquement indépendants sur K si et seulement si $x_1, \ldots, x_s$ sont algébriquement indépendants sur K et $x_{s+1}, \ldots, x_n$ sont algébriquement indépendants sur $K(x_1, \ldots, x_s)$.*

Démonstration. 1) Supposons $x_1, \ldots, x_n$ algébriquement indépendants sur K. Il en est de même de $x_1, \ldots, x_s$. S'il existe

$$f \in K[x_1, \ldots, x_s][Y_{s+1}, \ldots, Y_n], \quad f \neq 0$$

tel que $f(x_{s+1}, \ldots, x_n) = 0$. Il existe $h \in K[x_1, \ldots, X_s]$ tel que $h(x_1, \ldots, x_s)$ soit un dénominateur commun des coefficients de f. Soit $f_1 \in K[x_1, \ldots, X_s, Y_{s+1}, \ldots, Y_n]$ tel que $f_1(x_1, \ldots, x_s, Y_{s+1}, \ldots, Y_n) = f$. On a $0 \neq hf_1 = g \in K[x_1, \ldots, X_s, Y_{s+1}, \ldots, Y_n]$ tel que $g(x_1, \ldots, x_s, x_{s+1}, \ldots, x_n) = 0$, contrairement à notre hypothèse.

2) Supposons que $x_1, \ldots, x_s$ sont algébriquement indépendants sur K et que $x_{s+1}, \ldots, x_n$ sont algébriquement indépendants sur $K(x_1, \ldots, x_s)$. S'il existe $f \in K[x_1, \ldots, X_n]$ tel que $f(x_1, \ldots, x_n) = 0$ alors, si

$$g = f(x_1, \ldots, x_s, X_{s+1}, \ldots, X_n) \in K[x_1, \ldots, x_s][X_{s+1}, \ldots, X_n]$$

n'est pas nul, $x_{s+1}, \ldots, x_n$ ne seraient algébriquement indépendants sur $K(x_1, \ldots, x_s)$ car $g(x_{s+1}, \ldots, x_n) = 0$.

Donc $g = f(x_1, \ldots, x_s, X_{s+1}, \ldots, X_n) = 0$ et les coefficients de g sont tous nuls. Or les coefficients de g sont les valeurs prises en $X_1 = x_1, \ldots, X_s = x_s$ de polynômes $T_i \in K[x_1, \ldots, X_s]$. Comme $x_1, \ldots, x_s$ sont algébriquement indépendants sur K, les polynômes T_i sont tous nuls. Mais, ces polynômes T_i sont les coefficients de f en considérant f comme élément de $K[x_1, \ldots, X_s][X_{s+1}, \ldots, X_n]$. Il vient que $f = 0$. □

Définition 14 (A.5.3). *Soit l'extension L/K. Une famille $(x_1, \ldots, x_n)$ d'éléments de L est appelée base de transcendance de L sur K si*

(a) les éléments $x_1, \ldots, x_n$ sont algébriquement indépendants sur K,

(b) le corps L est algébrique sur $K(x_1, \ldots, x_n)$.

Une base de transcendance est une base de transcendance pure si elle engendre l'extension.

Exemple 3 (A.5.4). *La famille $(X_1, \ldots, X_n)$ est une base de transcendance pure de $K(X_1, \ldots, X_n)$ sur K. Par contre $\{X^2\}$ est une base de transcendance de $K(X)$ sur K (X est racine de $T^2 - X^2$) mais ce n'est pas une base de transcendance pure.*

Remarque 3 (A.5.5). *Une famille B d'éléments de L est une base de transcendance de L sur K, si et seulement si B est une famille algébriquement libre maximale.*

Proposition 10 (A.5.6). *Soit L/K une extension de type fini. Deux bases de transcendance de L sur K ont le même nombre d'éléments.*

Démonstration. Si $L = K(S)$ avec S une partie finie de L alors, une partie maximale de S formée d'éléments algébriquement indépendants sur K est une base de transcendance de L sur K. Ainsi L admet une base de transcendance sur K formée d'un nombre fini n d'éléments.

On raisonne par récurrence sur n en montrant que : pour toute extension H/F ayant une base de transcendance de cardinal n, alors toute partie de H formée d'éléments algébriquement indépendants sur F est de cardinal $\leq n$.

Si $n = 0$ alors L est algébrique sur K et on a le résultat.

Supposons alors $n \geq 1$. Soient $(x_1, \ldots, x_n)$ une base de transcendance de H sur F et $y_1, \ldots, y_m$ des éléments de H algébriquement indépendants sur F. On complète $\{y_1\}$ par des x_i pour avoir une partie maximale $\{y_1, x_{i_1}, \ldots, x_{i_s}\}$ formée d'éléments algébriquement indépendants sur F (donc une base de transcendance de H sur F). Par maximalité de la famille (x_i), on a $s \leq n - 1$. Soit le corps $F(y_1)$. La famille $(x_{i_1}, \ldots, x_{i_s})$ est une base de transcendance de H sur $F(y_1)$. Par hypothèse de récurrence, $m - 1 \leq s \leq n - 1$. Il s'ensuit que $m \leq n$. □

Définition 15 (A.5.7). *Le cardinal d'une base de transcendance d'une extension de type fini L/K s'appelle le degré de transcendance de L sur K. On le note degtr L/K. On a degtr $L/K = 0$ si et seulement si L est algébrique sur K.*

MERCI !