Théorème de Lüroth

__Lemme :__ Soient $P \in k[X]$ et $F, G, H \in k[X,Y] \setminus \{0\}$ tels que $P(X)\,F(X,Y) = G(X,Y)\,H(X,Y)$.
On écrit $G(X,Y) = \sum_{i=0}^{n} G_i(X)\,Y^i$ et $H(X,Y) = \sum_{i=0}^{p} H_i(X)\,Y^i$ avec $G_0, \dots, G_n, H_0, \dots, H_p \in k[X]$ et G_n, H_p non nuls.
On suppose les G_i premiers entre eux dans leur ensemble. Alors P divise $H_0, \dots, H_p$ (dans $k[X]$).

__Démonstration :__ On raisonne par récurrence sur $m = \deg P$.

- __$m = 0$:__ le résultat est clair.
- Soit $m \in \mathbb{N}$. On suppose le résultat vrai pour tout rang inférieur à m. Soient P, F, G, H vérifiant les hypothèses de l'énoncé, avec $\deg P = m+1$. On fixe Q un facteur irréductible de P. L'idéal (Q) de $k[X]$ étant maximal, $K := k[X]/(Q)$ est un corps. On note $\psi : \begin{array}{ccc} k[X][Y] & \longrightarrow & K[Y] \\ \sum_{i=0}^{n} U_i\,Y^i & \longmapsto & \sum_{i=0}^{n} \pi(U_i)\,Y^i \end{array}$ la réduction

modulo (Q), où $\pi : k[X] \twoheadrightarrow K$ est la projection canonique.

Comme Q divise P, on a $0 = \psi(PF) = \psi(GH) = \psi(G)\,\psi(H)$, ce qui donne, par intégrité de $K[Y]$, $\psi(G) = 0$ ou $\psi(H) = 0$. Le cas $\psi(G) = 0$ est impossible car Q ne divise pas tous les G_i, ces derniers étant premiers entre eux dans leur ensemble. On a donc $\psi(H) = 0$, ce qui signifie que Q divise tous les H_i. Pour tout $i \in [\![0, p]\!]$, on écrit alors $H_i = Q\,H_{i,1}$. On pose de plus $P = Q\,P_1$.

On a alors
$$\begin{aligned} H &= \sum_{i=0}^{p} H_i(X)\,Y^i = \sum_{i=0}^{p} Q(X)\,H_{i,1}(X)\,Y^i \\ &= Q(X) \sum_{i=0}^{p} H_{i,1}(X)\,Y^i \\ &= Q(X)\,H_1(X,Y) \end{aligned}$$

L'anneau $k[X,Y]$ étant intègre, on a $P_1(X)\,F(X,Y) = G(X,Y)\,H_1(X,Y)$. L'hypothèse de récurrence permet de conclure, car $\deg P_1 \leq m$.

__Théorème (Lüroth) :__ Soit K/k une extension transcendante pure telle que $\operatorname{degtr}_k K = 1$.
Soit L un sous-corps de K contenant strictement k. Alors L est une extension transcendante pure de k telle que $\operatorname{degtr}_k L = 1$.

Démonstration : On peut supposer que $K = k(X)$.

Soit $y \in L \setminus k$. On écrit $y = \dfrac{P_0}{Q_0}$ où $P_0, Q_0 \in k[X]$ sont premiers entre eux tels que $\max(\deg P_0, \deg Q_0) \geq 1$. L'élément $X \in K$ est racine du polynôme $P_0(T) - y\,Q_0(T) \in k(y)[T] \subset L[T]$, donc est algébrique sur L. On note $\Phi(T) = T^n + a_1 T^{n-1} + \dots + a_n$ le polynôme minimal de X sur L, avec $a_1, \dots, a_n \in L$. Comme $K = L(X)$, on a $[K : L] = n$.

De plus, pour tout $i \in [\![1, n]\!]$, $a_i \in L \subset K$, donc $a_i = A_i(X) \in k(X)$. Soit $B_0(X) \in k[X]$ un ppcm des dénominateurs des A_i, de sorte que l'on puisse écrire, pour tout $i \in [\![1, n]\!]$, $A_i(X) = \dfrac{B_i(X)}{B_0(X)}$,

avec $B_1, \dots, B_n \in k[X]$ premiers entre eux dans leur ensemble.

On pose alors $P(X,T) = B_0(X)T^n + B_1(X)T^{n-1} + \dots + B_{n-1}(X)T + B_n(X) \in k[X,T]$ et $m = \deg_X P$.

Comme X est transcendant sur k, il existe un indice i tel que $\alpha = a_i = \dfrac{B_i(X)}{B_0(X)}$ ne soit pas constant. On fixe un tel indice. On a $\deg B_i \leq m$.

$\deg B_0 \leq m$

Le polynôme $B_i(T) - a_i B_0(T) = B_i(T) - \dfrac{B_i(X)}{B_0(X)} B_0(T) \in L[T]$ admet X pour racine, ce qui le force à être divisible par Φ dans $L[T]$, et permet d'écrire $B_i - \dfrac{B_i(X)}{B_0(X)} B_0 = \Phi H$,

avec $H \in L[T]$. On pose $S(X,T) = B_i(T) B_0(X) - B_i(X) B_0(T)$,

ce qui donne $S(X,T) = \underbrace{B_0(X)\,\Phi(T)}_{= P(X,T)} H(T) = P(X,T)H(T)$. On écrit $H(T) = \sum_{i=0}^{q} \dfrac{D_i(X)}{C_0(X)} T^i$,

avec $C_0, D_0, \dots, D_q \in k[X]$. On obtient $C_0(X) S(X,T) = P(X,T) \sum_{i=0}^{q} D_i(X) T^i$. Mais les B_i sont premiers entre eux dans leur ensemble, donc, par le lemme, C_0 divise tous les D_i, ce qui donne $H \in k[X,T]$. De plus, $\deg_X P = m$ et $\deg_X S \leq m$, donc $\deg_X S = m$ et $\deg_X H = 0$, d'où $H \in k[T]$. Or $S(X,T) = -S(T,X)$, donc $H(T)P(X,T) = -H(X)P(T,X)$.

Le lemme dit que $H(X)$ divise, dans $k[X]$, les coefficients de $H(T)$ vu comme élément de $k[X][T]$, donc H est constant. On a alors $\deg_T P = \deg_X P$, donc $n = m$.

On a $B_0(X)\alpha - B_i(X) = 0$, donc X est racine de $B_0(T)\alpha - B_i(T) \in k(\alpha)[T]$.

Comme $\deg B_0 \leq m$, $\deg B_i \leq m$, on a $[k(X):k(\alpha)] \leq m$. Donc $n = m \geq [k(X):k(\alpha)] = [k(X):L][L:k(\alpha)]$,
$= n\,[L:k(\alpha)]$

d'où $[L:k(\alpha)] = 1$, ce qui donne $L = k(\alpha)$. Enfin, α est transcendant sur k, sans quoi on aurait $[k(X):k] = [k(X):k(\alpha)][k(\alpha):k] < +\infty$, ce qui serait absurde.