Théorème de l'élément primitif (+ contre-exemple)

Soit K/k extension séparable. $\exists z \in K$ tq $K = k(z)$

Thm : Supposons k infini.

- Supposons que $K = k(x,y)$.

  Montrons : $\exists z \in K$ tq $K = k(z)$.

Soient P_x, P_y les poly min de x, y sur k.

Soit M un corps de décomp de $P_x P_y$.

Dans $M[X]$, $P_x(X) = \prod_{i=1}^{n} (X - x_i)$ $\quad P_y(X) = \prod_{j=1}^{m} (X - y_j)$

$x_1 = x$, $x_2, \dots, x_n \in M$ $\quad y_1 = y$, $y_2, \dots, y_m \in M$

x_i distincts, y_j distincts car K/k séparable.

Soit $\mathcal{E} := \left\{ \frac{x - x_i}{y - y_j},\ 2 \le i \le n \right\} \subset M$. On a $\#(\mathcal{E}) \in (n-1)(m-1)$, donc $\exists t \in k^*$ tq $t \notin \mathcal{E}$.

Ainsi, $\forall i \ge 1$, $\forall j \ge 2$, $x - t y \neq x_i - t y_j$

Posons $F(X) = P_x(z + tX) \in k(z)[X]$.

On a $F(X) = \prod_{i=1}^{n} (z + tX - x_i) = \prod_{i=1}^{n} ((x - x_i) - t(y - X))$

Donc $F(y_j) \neq 0$ $\forall j \ge 2$

$F(y) = 0$ car $x_1 = x$

Donc $F(X) \wedge P_y = X - y \Rightarrow X - y \in k(z)[X]$

$\Rightarrow y \in k(z)[X]$

$\Rightarrow x = z + ty \in k(z)[X]$

$\Rightarrow k(z) = k(x,y)$.

- Dans le cas général, écrivons $K = k(x, x_1, \dots, x_n)$, $x, x_1, \dots, x_n \in k$, $n \in \mathbb{N}^*$ et procédons par récurrence sur n.

$n = 1$ ok

Supposons HR_n vraie. Soit $K = k(x, x_1, \dots, x_n, x_{n+1})$

Alors $K = k(z, x_{n+1}) = k(z')$ (HR$_n$, HR$_1$) $\square$

Supposons k fini.

- Alors K est fini. $\exists q$ tq $K = \mathbb{F}_q$, $q = p^r$ p premier.

$\mathbb{F}_q^\times$ est cyclique, $\exists \alpha \in \mathbb{F}_q^\times$ tq $\mathbb{F}_q^\times = \langle \alpha \rangle \Rightarrow K = k(\alpha)$.

Sur $\mathbb{F}_q$, $X^{q-1}-1$ est scindé à racines simples, ses racines étant les $x \in \mathbb{F}_q^*$.

Donc $\forall d | q-1$, X^d-1 est scindé à racines simples.

Soit $d | q-1$. Supposons avoir x d'ordre d. Alors les x^k sont d'ordre au plus d, et on en a d.
Ce sont donc toutes les racines de x^d-1. Ceux qui sont d'ordre exactement d sont donc les x^k tels que $k \wedge d = 1$.
On en a $\varphi(d)$.

Sinon, il n'y a pas d'élément d'ordre d.

On a donc : $\#\{x \in \mathbb{F}_q \mid \mathrm{ord}(x) = d\} \in \{0, \varphi(d)\}$ Or, $q-1 = \sum_{d | q-1} \#\{x \in \mathbb{F}_q \mid \mathrm{ord}(x) = d\}$

$= \sum_{d | q-1} \varphi(d)$

Donc $\forall d | q-1$, $\#\{x \in \mathbb{F}_q \mid \mathrm{ord}(x) = d\} = \varphi(d)$

Comme $\varphi(d) \neq 0$, en particulier $\varphi(q-1)$, on a un élément d'ordre $q-1$. □

Cours d'Algèbre 1
1ère année ENS de Lyon

Contre-exemple :

$k = \mathbb{F}_p(X, Y) = \mathrm{Frac}(\mathbb{F}_p[X, Y])$

K corps de décomposition de $T^p - X$ et $T^p - Y$

Soit $\alpha \in_K \alpha^p = X$, $\beta \in_K \beta^p = Y$

On a : $k(\alpha, \beta)$ / $k(\alpha)$ / $k(\beta)$ / k ; $[k(\alpha):k] = p$, $[k(\beta):k] = p$

$T^p - X = (T - \alpha)^p$ non séparable (irréd par Eisenstein dans $\mathbb{F}_p[X, Y]$)

$T^p - Y = (T - \beta)^p$

Soit $z \in K$, $z^p \in k$ ... car $(\alpha^i \beta^j)^p = \alpha^{pi} \beta^{pj} = X^i Y^j$

Donc il n'y a aucun $z \in K$ tq $K = k(z)$, car $\deg(\mathrm{Irr}(z, k)) \leq p$ $\forall z \in K$.

Démo : $[k(\alpha, \beta) : k] = p^2$:

$\beta \notin k(\alpha)$ car si $\left(\sum_{i=0}^{p-1} \frac{P_i(X)}{Q_i(X)} \alpha^i\right)^p = Y$ alors $\sum_{i=0}^{p-1} P_i(X^p) \times \prod_{j \neq i} Q_j(X^p, Y^p) X^i = Y \times \prod_{j=0}^{p-1} Q_j(X^p, Y^p)$ car $P(X, Y)^p = P(X^p, Y^p)$ dans $\mathbb{F}_p[X, Y]$.

mais $\deg_Y(\ldots) = 0 [p]$ $\neq$ $\deg_Y(\cdot) = 1 [p]$ contradiction

$\begin{cases} p \mid [k(\alpha, \beta) : k] \mid p^2 \\ [k(\alpha, \beta) : k] > [k(\alpha) : k] \text{ car } \beta \notin k(\alpha) \end{cases}$

$\Rightarrow [k(\alpha, \beta) : k] = p^2$