Théorème de l'élément primitif :

Théorème : Soit $\mathbb{L}/\mathbb{K}$ une extension finie où $\mathbb{K}$ est un corps fini ou $\mathrm{car}(\mathbb{K})=0$. Alors $\mathbb{L}/\mathbb{K}$ est monogène.

Preuve : • Si $\mathbb{K}=\mathbb{F}_q$ avec $q=p^n$: $[\mathbb{L}:\mathbb{K}]=m\in\mathbb{N}^*$ donc $\mathbb{L}\overset{\text{ev}}{\simeq}\mathbb{K}^m$

→ $\mathbb{L}$ est fini donc $\mathbb{L}$ est un corps fini, donc $\mathbb{L}^\times$ est cyclique, engendré par $\alpha\in\mathbb{L}$. Alors $\mathbb{K}(\alpha)\subset\mathbb{L}$ d'une part. Et d'autre part $\mathbb{L}^\times\subset\mathbb{F}_p(\alpha)\subset\mathbb{K}(\alpha)$ donc $\mathbb{L}=\mathbb{K}(\alpha)$: $\mathbb{L}/\mathbb{K}$ est monogène.

• Si $\mathrm{car}(\mathbb{K})=0$: alors $\mathbb{K}$ est infini.

On traite d'abord le cas $\mathbb{L}=\mathbb{K}(x,y)$. Soient Π_x et Π_y les polynômes minimaux de x et y sur $\mathbb{K}$. Soit $\mathbb{M}$ un corps de décomposition de $\Pi_x\Pi_y$, comme $\mathrm{car}(\mathbb{K})=0$, Π_x et Π_y sont à racines simples sur $\mathbb{M}$:

$$\Pi_x(X)=(X-x)\prod_{i=1}^{n}(X-x_i) \quad\text{et}\quad \Pi_y(X)=(X-y)\prod_{j=2}^{m}(X-y_j)$$

avec les x_i ($\sup y_j$) distincts dans $\mathbb{L}$.

Alors $\exists t\in\mathbb{K}$ tq $x+ty\neq x_i+ty_j$, $\forall (i,j)\in[\![2,n]\!]\times[\![2,m]\!]$.

En effet, $x+ty=x_i+ty_j \iff t=\dfrac{x-x_i}{y_j-y}$ on prend qu'un nombre fini de valeurs.

Soit donc $z=x+ty$, on va montrer que $\mathbb{L}=\mathbb{K}(z)$:

Soit $\widetilde{\mathbb{K}}=\mathbb{K}(z)$ et $F(X)=\Pi_x(z-tX)\in\widetilde{\mathbb{K}}[X]$ par composition.

Alors F est scindé sur $\mathbb{M}$: $F(X)=(z-tX-x)\prod_{i=2}^{n}(z-tX-x_i)$

$$=t(y-X)\prod_{i=2}^{n}((x-x_i)+t(y-X))$$

Or par définition de t, $F(y_j)\neq 0$ $\forall y_j\in[\![2,m]\!]$

Donc dans $\mathbb{M}[X]$, $\mathrm{PGCD}(F,\Pi_y)=X-y$ donc aussi dans $\widetilde{\mathbb{K}}[X]$

En effet, si $D_1=\mathrm{PGCD}(F,\Pi_y)$ dans $\widetilde{\mathbb{K}}[X]$, $\begin{matrix}F=AD_1\\ \Pi_y=BD_1\end{matrix}$ avec $A,B\in\widetilde{\mathbb{K}}[X]$ premiers entre eux

donc $\exists U,V\in\widetilde{\mathbb{K}}[X]$ tq $UA+VB=1$, or $U,V\in\mathbb{M}[X]$ donc A et B sont premiers entre eux dans $\mathbb{M}[X]$, donc D_1 est le PGCD de F et Π_y dans $\mathbb{M}[X]$.

Ainsi $X-y\in\widetilde{\mathbb{K}}[X]\to y\in\widetilde{\mathbb{K}}$ donc en particulier on a aussi $x=z-ty\in\widetilde{\mathbb{K}}$ car $t\in\mathbb{K}$ et $z\in\widetilde{\mathbb{K}}$ donc $x,y\in\widetilde{\mathbb{K}}=\mathbb{K}(z)$

$\to\mathbb{K}(x,y)\subset\mathbb{K}(z)$: $\mathbb{K}(x,y)\subset\mathbb{K}(x+ty)$ donc $\mathbb{L}=\mathbb{K}(x,y)=\mathbb{K}(z)$

$\hookrightarrow$ $\mathbb{L}/\mathbb{K}$ est monogène.

Comme on a $\mathbb{K}(x_1,\dots,x_{n+1})=\mathbb{K}(x_1,\dots,x_n)(x_{n+1})$, on peut raisonner par récurrence sur le nombre de générateurs, ce qui achève la preuve.

Ce résultat peut être mis en défaut si $\mathbb{K}$ est infini de caractéristique non nulle.

Contre-exemple: Soit $\mathbb{K}$ un corps de caractéristique $p>0$, $\mathbb{L}=\mathbb{K}(X,T)$ et $\mathbb{L}_0=\mathbb{K}(X^p,T^p)$. Alors $[\mathbb{L}:\mathbb{L}_0]=p^2<+\infty$ mais $\mathbb{L}/\mathbb{L}_0$ n'est pas monogène.

Preuve: Considérons le polynôme $P(Y)=Y^p-X^p\in\mathbb{L}_0[Y]$

Comme X^p est irréductible dans l'anneau $\mathbb{L}_0$, par Eisenstein le polynôme P est irréductible dans $\mathbb{L}_0[Y]$. De même $Q(Y)=Y^p-T^p\in\mathbb{L}_0(Y)$ est irréductible sur $\mathbb{K}(X,Y^p)$.

Donc $[\mathbb{K}(X,Y^p):\mathbb{K}(X^p,Y^p)]=p$ $\quad\Rightarrow [\mathbb{L}:\mathbb{L}_0]=p^2$

et $[\mathbb{K}(X,Y):\mathbb{K}(X,Y^p)]=p$

Or comme $\mathrm{car}(\mathbb{K})=p$, $\forall f\in\mathbb{K}[X,T]$, $(f(X,T))^p=f(X^p,T^p)$

et donc $\forall f\in\mathbb{L}$, $f=\frac{g}{h}$ on a $(f(X,T))^p=\dfrac{g(X^p,T^p)}{h(X^p,T^p)}=f(X^p,T^p)\in\mathbb{L}_0$

Alors, si $\mathbb{L}/\mathbb{L}_0$ est monogène avec $\mathbb{L}=\mathbb{L}_0(f)$ pour $f\in\mathbb{L}$, on aurait $f^p\in\mathbb{L}_0$, et donc $[\mathbb{L}_0(f):\mathbb{L}_0]\leq p$: absurde

Donc $\mathbb{L}/\mathbb{L}_0$ n'est pas monogène

N.B.: en toute généralité, si $\mathbb{F}$ est un corps quelconque et $n\in\mathbb{N}^*$, alors $[\mathbb{F}(X):\mathbb{F}(X^n)]=n$

En effet soit $A=\mathbb{F}[X^n]\simeq\mathbb{F}[Y]$ via $\varphi:\begin{cases}\mathbb{F}[Y]\to A\\ Y\mapsto X^n\end{cases}$ isomorphisme d'anneaux.

donc A est factoriel et $a=X^n\in A$ est irréductible car ses diviseurs sont (unitaires) les X^k, $0\leq k\leq n$ qui n'appartiennent pas à A.

On peut donc appliquer le critère d'Eisenstein à $P=Y^n-X^n\in A[Y]$

Donc P est irréductible sur $\mathbb{L}=\mathbb{F}(X^n)=\mathrm{Frac}(A)$ et P est donc le polynôme minimal de X sur $\mathbb{L}$: $[\mathbb{F}(X):\mathbb{F}(X^n)]=n$ $\quad$ ($\mathbb{F}(X^n)[Y]=\mathbb{L}[Y]$).