Remarque sur les extensions galoisiennes

Soit K/k une extension finie de corps. On dit que K/k est *galoisienne* s'il existe G un sous-groupe de $\mathrm{Aut}(K)$, le groupe des automorphismes de K tel que $k = K^G = \{x \in K \ : \ ^\forall \phi \in G, \phi(x) = x\}$.

Dans ce cas, on sait que $G = \mathrm{Aut}_k(K)$, le groupe des $k-$automorphismes de K et $[K : k] = |G|$ et que tout $k-$plongement $\phi : K \to \Omega$ de K dans un corps algébriquement clos Ω laisse stable K et $\phi \in G$. On dit que G est le groupe de Galois de l'extension.

Réciproquement, on a :

Proposition : *Soit k un corps contenu dans un corps algébriquement clos Ω. On suppose que k est fini ou de caractéristique nulle. Soit $(f_i)_i$ une famille de polynômes à coefficients dans k. On note K le corps de décomposition des f_i sur k (dans Ω). C'est le sous-corps de Ω engendré par k et les racines des f_i. Si K/k est finie (par exemple si l'ensemble des f_i est fini), alors K est une extension galoisienne de k de groupe de Galois le groupe $G = \mathrm{Aut}_k(K)$.*

démo : Comme K/k est finie, le groupe $G = \mathrm{Aut}_k(K)$ est fini (de cardinal au plus $[K : k]$. Il suffit donc de montrer que $K^G = k$. Il y a une inclusion évidente. Pour l'autre inclusion : soit $x \in K^G$, montrons que $x \in k$. Si $x \notin k$, alors le polynôme minimal P de x sur k est de degré ≥ 2. Or P est irréductible sur k donc scindé à racines simples dans Ω (*cf.* le lemme ci-dessous). Donc P admet au moins une racine $x' \neq x$ dans Ω. Il existe un $k-$morphisme de corps : $\phi : k[x] \to \Omega$ tel que $\phi(x) = x'$. Le morphisme ϕ s'étend en un $k-$morphisme $\widetilde{\phi} : K \to \Omega$ car Ω est algébriquement clos. On a $\widetilde{\phi}(K) = K$. En effet, il suffit de montrer que $\widetilde{\phi}$ laisse stable l'ensemble des racines des f_i ce qui est immédiat :

$$f_i(z) = 0 \Rightarrow \widetilde{\phi}(f_i(z)) = f_i(\widetilde{\phi}(z)) = 0 \ .$$

Puisque K est un $k-$espace vectoriel de dimension finie, $\widetilde{\phi}$ est un $k-$automorphisme de K *i.e.* $\widetilde{\phi} \in G$; d'où la contradiction car $x \in K^G$ et $\widetilde{\phi}(x) = x' \neq x$.

Lemme : *Soit P un polynôme irréductible sur un corps k fini ou de caractéristique nulle. Alors, pour toute extension Ω algébriquement close de k, le polynôme P est scindé à racines simples dans Ω.*

démo : il suffit de vérifier que P et son polynôme dérivé P' sont premiers entre eux (si $P(X) = (X - t_1)^{m_1}...(X - t_r)^{m_r}$ pour certains $t_i \in \Omega$ deux à deux distincts et certains entiers $m_i \geq 1$, alors le pgcd de P et P' est le polynôme : $(X - t_1)^{m_1-1}...(X - t_n)^{m_n-1})$. Si tel n'était pas le cas, comme P est irréductible, on aurait P divise P' donc, pour des raisons de degrés, $P' = 0$. Cela n'est possible que si k est de caractéristique p et si $P(X) = Q(X^p)$ pour un certain :

$$Q = a_0 + ... + a_d X^d \in k[X] \ .$$

Mais alors, k est un corps fini $\mathbb{F}_q$ avec q une puissance de p. On a alors $x = x^q$ pour tout $x \in k$. En particulier, $a_i = b_i^p$ pour tout i et pour certains $b_i \in k$. Comme k est de caractéristique p, on a :

$$P(X) = a_0 + ... + a_d (X^p)^d$$

$$= b_0^p + ... + b_d^p X^{pd}$$
$$= (b_0 + ... + b_d X^d)^p$$

ce qui contredit l'irréductibilité de $P(X)$.

Remarque : Dans la proposition, on peut remplacer l'hypothèse k fini ou de caractéristique nulle par l'hypothèse :« l'extension K/k est séparable » *i.e.* tous les éléments de K sont des racines d'un polynôme à racines simples dans Ω.

Dans la proposition on utilise en fait que tous les $k-$plongements de K dans Ω laisse stable K. On dit qu'une extension qui vérifie cette propriété est *normale*. Tout corps de décomposition est une extension normale et réciproquement, toute extension normale est le corps de décomposition de l'ensemble de ses polynômes non constants.