Fiche XIV : théorème d'Artin-Schreier

Soit K/k une extension finie séparable. Soit $a \in K$ tel que : $K = k(a)$. L'extension $K(X)/k(X)$ est encore finie et séparable. On note N la norme $N_{K(X)/k(X)}$.

a) Soit f le polynôme minimal de a sur k. Fixons un corps algébriquement clos Ω qui contient $K(X)$. Tout $k-$plongement σ de K dans Ω se prolonge en un $k(X)-$plongement (encore noté σ) de $K(X)$ dans Ω : il suffit de poser $\sigma(X) := X$. Si on note $\sigma_1, ..., \sigma_n$ les $k-$plongements de K dans Ω, leurs prolongements $\sigma_1, ..., \sigma_n$ sont les $k(X)-$plongements de $K(X)$ dans Ω. Donc comme $K(X) = k(X)(a)$, on a :

$$N(X-a) = \prod_i \sigma_i(X-a) = \prod_i X - \sigma_i(a) = f(X) \in k(X) \ .$$

b) Soit $g \in k[X]$. Soit $g(X) - a = \prod_{j=1}^{d} g_j$ la décomposition en facteurs irréductibles de $g - a$ dans $K[X]$.

Comme la norme est multiplicative, on a :

$$N(g-a) = \prod_j N(g_j)$$

or :

$$N(g-a) = \prod_i \sigma_i(g-a) = \prod_i g - \sigma_i(a) = f(g) \ .$$

Donc :

$$f(g(X) = \prod_j N(g_j) \ .$$

Remarque : comme $g_j \in K[X]$ est entier sur $k[X]$, $N(g_j) \in k(X)$ est entier sur $k[X]$. Comme l'anneau $k[X]$ est principal, on a forcément, $N(g_j) \in k[X]$.

c) Soit p un facteur irréductible de $f(g(X)$ dans $k[X]$. Alors, $p|N(g_j)$ pour un certain j. Notons K' la clôture normale de K dans Ω (K' est le corps engendré par tous les $\sigma_i(K)$). Comme $N(g_j) = \prod_i \sigma_i(g_j)$, il existe un i tel que $\sigma_i(g_j)$ n'est pas premier à p. Mais alors g_j n'est pas premier à p non plus (si g_j était premier à p, alors $\sigma_i(g_j)$ serait premier à $\sigma_i(p) = p$ (il suffit d'appliquer σ_i à une relation de Bezout)). Or g_j est irréductible dans $K[X]$ donc $g_j|p$ dans $K[X]$. On en déduit que $\sigma_i(g_j)|p$ dans $K'[X]$.

Comme a est séparable sur k, $\sigma_i(a) \neq a$ si $\sigma_i \neq \mathrm{Id}$. Donc les polynômes : $g - \sigma_i(a)$ et $g - a$ sont premiers entre eux. Or : $g - \sigma_i(a) = \prod_j \sigma_i(g_j)$. Donc les $\sigma_i(g_j)$, $1 \leq i \leq n$, sont premiers entre eux deux à deux.

On a donc $\prod_i(\sigma_j) = N(g_j)|p$ dans $K'[X]$. Comme $p|N(g_j)$, on a :

$$N(g_j) = p$$

(à multiplication par une constante près).

Vérifions que tous les $N(g_{j'})$ sont irréduictibles sur k.

Soit $j' \neq j$. Si $N(g_{j'}) = N(g_j)$, alors $N(g_{j'})$ est irréductible sur k. Si $N(g_{j'}) \neq N(g_j)$, soit p un diviseur irréductible de $N(g_{j'})$. D'apès ce qui précède, $p = N(g_{j''})$ pour un certain j''. Mais alors, $N(g_{j''})$ et $N(g_{j'})$ ne sont pas premiers entre eux. On a donc $N(g_{j''})|N(g_{j'})$. Donc $g_{j''}$ n'est pas premier avec un $\sigma_i(g_{j'})$ pour un certain i. On a forcément $\sigma_i = \mathrm{Id}$ sinon $g - a = \prod_j g_j$ serait premier avec $g - \sigma_i(a) = \prod_j \sigma_i(g_j)$. Donc $\sigma_i(g_{j'}) = g_{j'}$ et $g_{j'} = g_{j''}$ car $g_{j'}$ et $g_{j''}$ sont irréductibles sur K.

On adonc montré que $f(g(X)) = \prod_{j=1}^{d} N(g_j)$ est la décomposition de $f(g(X))$ en facteurs irréductibles.

En particulier, $f(g(X))$ est irréductible sur $k \Leftrightarrow g - a$ est irréductible sur $K \Leftrightarrow d = 1$.

Lemme 1 *Soient k un corps et $0 \neq a \in k$. Soit p un nombre premier impair. Si $a \notin k^p$, alors pour tout $n \geq 1$, $X^{p^n} - a$ est irréductible sur k.*

Démonstration : Si k n'est pas de caractéristique p.

On raisonne par récurrence sur $n \geq 1$. Si $n = 1$: soit α une racine de $X^p - a$. Soit N la norme de l'extension $k(\alpha)/k$ (extension séparable car $X^p - a$ est séparable). On a :

$$\alpha^p = a \Rightarrow N(\alpha)^p = N(a) = a^d$$

où $d := [k(\alpha)/k]$. Si d était premier à p, on aurait $du + pv = 1$ pour certains u, v entiers. Mais alors :

$$a = a^{du+pv} = N(\alpha)^{pu} a^{pv} \in k^p$$

contradiction ! Donc $p|d$. Or $d \leq p$ donc $d = p = [k(\alpha) : k]$. En particulier, $X^p - a$ est le polynôme minimal de α sur k et $X^p - a$ est irréductible sur k.

Si $n > 1$: on pose $f = X^p - a$. Soit α une racine de f. Soit $g := X^{p^{n-1}}$. Alors : $f(g(X)) = X^{p^n} - a$ est irréductible si et seulement si : $g - \alpha = X^{p^{n-1}} - \alpha$ est irréductible sur $k(\alpha)$. Or, $\alpha \notin k(\alpha)^p$. En effet, sinon :

$$\alpha = \lambda^p$$

pour un certain $\lambda \in k(\alpha)$ donc si on note N la norme de l'extension $k(\alpha)/k$, on a :

$$N(\alpha) = N(\lambda)^p \in k^p$$

ce qui est impossible car $N(\alpha) = a$ (puisque $X^p - a$ est le polynôme minimal de α sur k et p impair).

Donc par hypothèse de récurrence :

$$\alpha \notin k(\alpha)^p \Rightarrow X^{p^{n-1}} - \alpha \text{ irréductible sur } k(\alpha) \ .$$

Si k est de caractéristique p.

On raisonne encore par récurrence sur $n \geq 1$. Si $n = 1$, alors $X^p - a = (X - \alpha)^p$ où $\alpha^p = a$ avec $\alpha \notin k$. Si $X^p - a$ est réductible, il existe $1 < d < p$ tel que $(X - \alpha)^d \in k[X]$. Le coefficient de degré $d - 1$ de $(X - \alpha)^d$ est alors $-d\alpha \in k \Rightarrow \alpha \in k$ *absurdo* !

Si $n > 1$, soit α tel que $\alpha^{p^n} = a$. On a $\alpha^{p^{n-1}} \notin k(\alpha^{p^{n-1}})^p = k(\alpha^{p^n}) = k$. Donc par hypothèse de récurrence, $X^{p^n-1} - \alpha^{p^{n-1}}$ est irréductible sur $k(\alpha^{p^{n-1}})$. Donc :

$$[k(\alpha) : k] = [k(\alpha) : k(\alpha^{p^{n-1}})][k(\alpha^{p^{n-1}}) : k] = p^n$$

et $X^{p^n} - a$ est irréductible sur k. *q.e.d.*

Remarque : en caractéristique $p > 0$, le lemme est aussi vrai si $p = 2$.

Nous allons utiliser ce lemme pour démontrer le

Théorème 0.1 *Soit k un corps. Si $0 \neq a \in k$ et si $n \geq 1$, alors $X^n - a$ est réductible sur $k \Leftrightarrow$:*

$$i) {}^{\exists} b \in k,\ a = b^d \text{ pour un diviseur } 1 < d \text{ de } n \text{ ou bien :}$$

$$ii) 4|n \text{ et } a = -4c^4 \text{ pour un } c \in k$$

Démonstration :

Si i) ou ii) est vrai, il est facile de voir que $X^n - a$ est réductible. Réciproque :

On raisonne par récurrence sur n.

1er cas : $n = p^r q$ pour un nombre premier impair p, $r \geq 1$ et q un entier premier à p

Si $a \in k^p$, $i)$ est vérifié. Sinon, $X^{p^r} - a$ est irréductible sur k. Posons $f := X^{p^r} - a$, α une racine de f et $g := X^q$. Supposons k de caractéristique $\neq p$. Alors $f(g) = X^n - a$ est réductible $\Rightarrow g - \alpha$ est réductible sur $k(\alpha)$. Donc par hypothèse de récurrence, on a $(*)$ $\alpha \in k(\alpha)^d$ pour un $1 \neq d|q$ ou $(**)$ $4|q$ et $\alpha \in -4k(\alpha)^4$. Posons $N := N_{k(\alpha)/k}$. On a $N(\alpha) = a$ (car p^r est impair) et on en déduit $(*) \Rightarrow i)$ et $(**) \Rightarrow ii)$.

Si k est de caractéristique p : on note β une racine de $X^n - a$. On a :

$$[k(\beta) : k] = [k(\beta) : k(\beta^q)][k(\beta^q) : k] < p^r q = n$$

car $X^n - a$ est réductible sur k. Donc $X^q - \beta^q$ est réductible sur $k(\beta^q)$ ou $X^{p^r} - a$ est réductible sur k. Si $X^{p^r} - a$ est réductible sur k, alors $a \in k^p$ d'où i. Si $X^q - \beta^q$ est réductible sur $k(\beta^q)$, alors par hypothèse de récurrence, soit il existe $d > 1$ tel que $d|q$ et $\beta^q \in k(\beta^q)^d \Rightarrow a = \beta^{p^r q} \in k(\beta^q)^{dp^r} = k(\beta^{qp^r})^d = k^d \Rightarrow i$. Soit $4|q$ et $\beta^q \in -4k(\beta^q)^4 \Rightarrow a = \beta^{p^r q} \in -4k^4 \Rightarrow ii$.

2eme cas : si $n = 2^r$

Si k est de caractéristique 2, on a $a \in k^2$ d'après la remarque qui suit le lemme ci-dessus. Donc i est vraie.

Si k est de caractéristique différente de 2, le polynôme $X^{2^r} - a$ est séparable sur k.

Si $r > 1$, c'est facile si $r > 1$, supposons $a \notin k^2$ (sinon i est déjà vérifiée). Soit α tel que $\alpha^2 = a$. Soit N la norme relative à l'extension $k(\alpha)/k$ (qui est séparable). Soient $f := X^2 - a$ et $g := X^{2^{r-1}}$. On a : $f(g(X)) = X^{2^r} - a$ réductible sur $k \Rightarrow X^{2^{r-1}} - \alpha$ réductible sur $k(\alpha)$. Donc par hypothèse de récurrence, $\alpha \in k(\alpha)^2$ ou $\alpha \in -4k(\alpha)^4$. Dans tous les cas, $N(\alpha) \in k^2$. Or $N(\alpha) = -\alpha^2 = -a$. Donc il existe $b \in k$ tel que $a = -b^2 = \alpha^2 \Rightarrow \alpha = ib$ où i est une racine carrée de -1. Donc $k(\alpha) = k(i)$ et $i \notin k$.

Soient $\lambda, \mu \in k$ tels que $\alpha = (\lambda + i\mu)^2$.

On a :

$$\alpha = ib \Rightarrow \lambda^2 = \mu^2 \text{ et } 2\lambda\mu = b$$

$$\Rightarrow \alpha^2 = -b^2 = -4\lambda^4$$

donc ii est vraie.

q.e.d.

Théorème 0.2 (Artin-Schreier) *Soit K/k une estension finie de corps de degré > 1 telle que K est algébriquement clos. Alors, k est de caractéristique 0, il existe $i \in K$ tel que $i^2 = -1$ et $K = k(i)$. En particulier K/k est de degré 2.*

Exemple : $K = \overline{Q}$ le corps des nombres algébriques sur $\mathbb{Q}$ et $k = \overline{\mathbb{Q}} \cap \mathbb{R}$ le corps des nombres algébriques réels.

Démonstration : L'extension K/k est séparable.

En effet, sinon, il existerait $a \in K$ tel que a est algébrique non séparable sur k. Si on note p la caractéristique de k, $P \in k[X]$ le polynôme minimal de a sur k, alors $P' = 0$ donc $P \in k[X^p]$. Soit $Q \in k[X]$ tel que $P(X) = Q(X^p)$. Comme P est irréductible sur k, $Q \notin k^p[X]$ *i.e.* il existe $q_i \neq 0$ un coefficient

de Q tel que $q_i \notin k^p$. Mais alors le polynôme $X^{p^r} - q_i$ est irréductible sur k pour tout $r \geq 1$ d'après le lemme. Donc : $[K : k] \geq p^r$ pour tout r : *absurde !*

Comme K est algébriquement clos, l'extension K/k est aussi normale (si $\alpha \in K$, tous les conjugués de α sur k sont aussi dans K). Donc l'extension K/k est galoisienne finie. Notons G le groupe de Galois de K/k. Soit p un nombre premier qui divise $|G|$. D'après le *lemme de Cauchy*, il existe un sous-groupe H de G (cyclique) d'ordre p.

Soit σ un générateur de H. Les racines $p-$ièmes de l'unité sont dans K^H. En effet, si $\alpha \in K$ et si $\alpha^p = 1$, alors :

$$[K : K^H(\alpha)][K^H(\alpha) : K^H] = [K : K^H] = p \ .$$

Comme p est premier, $[K^H(\alpha) : K^H] = 1$ ou p. Puisque $\alpha = 1$ ou $1 + ..; + \alpha^{p-1} = 0$, on a $[K^H(\alpha) : K^H] < p$ et donc $[K^H(\alpha) : K^H] = 1$ et $\alpha \in K^H$.

L'endomorphisme de K^H-espace vectoriel : $\sigma : K \to K$ vérifie $\sigma^p = \mathrm{Id}$.

Le corps k n'est pas de carctéristique p

En effet, sinon ... D'abord, k contient $\mathbb{F}_p$. Puis, comme l'extension est séparable, on peut trouver un élément $a \in K$ tel que : $\mathrm{Tr}a = 1$ (il s'agit de la trace de l'extension K/K^H) car les automorphismes :

$$\mathrm{Id}, \sigma, ..., \sigma^{p-1}$$

sont K linéairement indépendants et $\mathrm{Tr} = \mathrm{Id} + ... + \sigma^{p-1} \neq 0$.

On a alors :

$$\mathrm{Tr}(a^p - a) = \mathrm{Tr}(a)^p - \mathrm{Tr}(a) = 1 - 1 = 0 \ .$$

Donc il existe $\alpha \in K$ tel que $\sigma\alpha - \alpha = a^p - a$ (il suffit de poser $a := -b\sigma(a) - (b + \sigma(b))\sigma^2(a) - ... - (b + \sigma(b) + ... + \sigma^{p-2}(b))\sigma^{p-1}(a)$ avec $b := a^p - a$). Mais alors, puisque K est algébriquement clos, il existe $x \in K$ tel que $x^p - x - \alpha = 0$. Or :

$$\begin{gathered} x^p - x - \alpha = 0 \Rightarrow \sigma(x)^p - \sigma(x) - \sigma(\alpha) = x^p - x - \alpha \\ \Rightarrow \sigma(x)^p - x^p = \sigma(x) - x + a^p - a \\ \Rightarrow (\sigma(x) - x - a)^p = \sigma(x) - x - a \\ \Rightarrow \sigma(x) - x - a \in \mathbb{F}_p \\ \Rightarrow \mathrm{Tr}(\sigma(x) - x - a) = 0 \\ \Rightarrow \mathrm{Tr}(a) = 0 \end{gathered}$$

car $\mathrm{Tr}(\sigma(x)) = \mathrm{Tr}(x)$, d'où la contradiction !

Comme K^H n'est pas de caractéristique p et contient les racines $p-$èmes de l'unité, le polynôme $X^p - 1$ est scindé à racines simples sur K^H. Donc $\sigma : K \to K$ est un K^H-endomorphisme diagonalisable. Il existe donc $a \in K$ un vecteur propre de valeur propre $\epsilon \neq 1$ telle que $\epsilon^p = 1$. On a $\sigma(a) = \epsilon a \Rightarrow \sigma(a^p) = a^p$. Donc d'une part $a \notin K^H$ et d'autre part $a^p \in K^H$. Donc $a^p \in K^H \setminus (K^H)^p$ et $K = K^H(a^p)$.

Si p est impair, alors le polynôme $X^{p^n} - a^p$ est irréductible sur K^H pour tout n et alors :

$$[K : K^H] \geq p^n$$

pour tout n : *impossible !*

On a donc $[K : k] = 2^r$ pour un certain $r \geq 1$. On a même montré qu'il existe $k \subseteq K' \subseteq K$ tel que $[K : K'] = 2$ et $K = K'(a)$ avec $a^2 \in K'$. Soit $b \in K$ tel que $a = b^2$. On a $N(a) = N(b)^2$ où N est la norme relative à l'extension K/K'. Mais $N(a) = -a^2$. Donc : $N(b)^2 = -a^2 \Rightarrow a = iN(b)$ où i est une racine carrée de -1. Puisque $N(b) \in K'$, on a :

$$K = K'(a) = K'(i)$$

et en particulier, $i \notin K'$. Si $k \neq K'$, $k(i) \neq K$ et il existe K'' tel que :

$$k(i) \subseteq K'' \subseteq K$$

et $[K : K''] = 2$ e $K = K''(i)$: *absurde !*.

donc $[K : k] = 2$ et $K = k(i)$.

Il reste à vérifier que k est de caractéristique nulle.

Soient $a, b \in k$. Il existe $u, v \in k$ tels que $(u + iv)^2 = a + ib$ (car $k(i) = K$ est algébriquement clos). En prenant la norme relative à K/k, on a :

$$N((u + iv)^2) = N(a + ib) \Leftrightarrow (u^2 + v^2)^2 = a^2 + b^2$$

et donc toute somme de carrés de k est un carré de k. Si k était de caractéristique $l > 0$. On aurait :

$$-1 = \underbrace{1 + ... + 1}_{l-1 \text{ fois}}$$

et -1 serait un carré dans k et donc on aurait $i \in k$ et $K = k(i) = k$ *absurde !*

q.e.d.