I.I Norme dans une extension algébrique

Soit K un corps. Soit L/K une extension finie de K. Soit $\alpha \in L$, on note $\pi_{K,\alpha} = X^m + \sum_{i=0}^{m-1} a_i X^i$ le polynôme minimal de α sur K et $m_\alpha : \begin{array}{ccc} L & \to & L \\ x & \mapsto & \alpha x \end{array}$ la multiplication par α dans L.
On appelle norme de α et on note $N_{L/K}(\alpha)$ le déterminant de m_α vu comme K-endomorphisme de L.

Théorème 17:

1. Soit K un corps. Soit L/K une extension finie de K. Soit $\alpha \in L$. Alors dans la K-base $\left(1, \alpha, \dots, \alpha^{m-1}\right)$ de $K(\alpha)$ (où $m = \deg(\pi_{K,\alpha})$) la matrice de m_α est la matrice compagnon associée au polynôme $\pi_{K,\alpha}$.
   Donc
   $$\pi_{K,\alpha} = \chi_{m_\alpha}$$
   et :
   $$N_{K(\alpha)/K}(\alpha) = (-1)^m a_0$$
   Si de plus L contient un corps de décomposition de $\pi_{K,\alpha}$, alors :
   $$N_{K(\alpha)/K}(\alpha) = \prod_{i=1}^{m} x_i$$
   où $x_1, \dots, x_n \in L$ sont les racines de $\pi_{K,\alpha}$.
2. Il existe une K-base de L telle que la matrice de l'endomorphisme m_α dans cette base soit diagonale par blocs de la forme :
   $$\underbrace{\begin{pmatrix} C_\alpha & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & C_\alpha & \cdots & \mathbf{O} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{O} & \cdots & \mathbf{O} & C_\alpha \end{pmatrix}}_{[L:K(\alpha)] \text{ blocs}}$$
   où C_α est la matrice compagnon évoquée dans le premier point.
   De plus :
   $$\forall \alpha \in L, \quad N_{L/K}(\alpha) = \left(N_{K(\alpha)/K}(\alpha)\right)^{[L:K(\alpha)]}$$

Démonstration. 1. La famille $\left(1, \alpha, \dots, \alpha^{m-1}\right)$ est une K-base de $K(\alpha)$. En effet :
— Elle est libre par minimalité du polynôme minimal :
si $\sum_{i=0}^{m-1} \lambda_i \alpha^i = 0$ avec les $\lambda_i \in K$, alors $\sum_{i=0}^{m-1} \lambda_i X^i$ est un polynôme annulateur pour α, mais alors par définition du polynôme minimal ce polynôme est nulle ;
— Elle est génératrice car $K(\alpha) \simeq K[X]/\pi_{K,\alpha}$ est un K-e.v. de dimension $\deg(\pi_{K,\alpha})$.
La matrice de l'endomorphisme m_α dans cette base est alors :

$$C_\alpha := \begin{pmatrix} 0 & 0 & 0 & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{m-1} \end{pmatrix}$$

Alors :

$$\chi_{m_\alpha} = \begin{vmatrix} X & 0 & 0 & \cdots & a_0 \\ -1 & X & 0 & \cdots & a_1 \\ 0 & -1 & X & \cdots & a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & X + a_{m-1} \end{vmatrix}$$

et en faisant la combinaison $L_1 \longleftarrow L_1 + XL_2 + \dots X^{m-1}L_m$ puis en développant suivant la première ligne, on obtient :

$$\chi_{m_\alpha} = \begin{vmatrix} 0 & 0 & 0 & \cdots & \pi_{K,\alpha} \\ -1 & X & 0 & \cdots & a_1 \\ 0 & -1 & X & \cdots & a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & X + a_{m-1} \end{vmatrix} = (-1)^{m+1}\pi_{K,\alpha} \begin{vmatrix} -1 & X & 0 & \cdots & 0 \\ 0 & -1 & X & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & X \\ 0 & 0 & \cdots & 0 & -1 \end{vmatrix} = (-1)^{m+1}\pi_{K,\alpha}(-1)^{m-1} = \pi$$

On a donc obtenu que $\pi_{K,\alpha} = \chi_{m_\alpha}$ et les relations coefficients/racines fournissent en outre $N_{K(\alpha)/K}(\alpha) = \det(m_\alpha) = (-1)^m a_0$.

Si de plus L contient un corps de décomposition de $\pi_{K,\alpha}$ alors :

$$N_{K(\alpha)/K}(\alpha) = \prod_{i=1}^{m} x_i$$

2. Soit $d := [L : K(\alpha)]$, si $(e_1, \dots, e_d)$ est une $K(\alpha)$-base de L, alors d'après le théorème de la base télescopique $\left(e_1, \alpha e_1, \dots, \alpha^{m-1}e_1, e_2, \dots, \alpha^{m-1}e_2, \dots, e_d, \dots, \alpha^{m-1}e_d\right)$ est une K-base de L. Il s'en suit que la matrice dans cette base de m_α est

$$\begin{pmatrix} C_\alpha & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & C_\alpha & \cdots & \mathbf{O} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{O} & \cdots & \mathbf{O} & C_\alpha \end{pmatrix}$$

Alors $\chi_{m_\alpha} = (\chi_{C_\alpha})^d = (\pi_{K,\alpha})^d$. De cela résulte $N_{L/K}(\alpha) = N_{K(\alpha)/K}(\alpha)^d$.

■

Application 18: Norme dans un corps fini

Soit p un nombre premier. Soit $n \in \mathbb{N}^*$. Soit $q = p^n$. Alors en notant φ le morphisme de Frobenius :

$$\forall \alpha \in \mathbb{F}_q, \quad N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \prod_{i=0}^{n-1} \varphi^i(\alpha) = \alpha^{\frac{q-1}{p-1}}$$

Démonstration. Soit $\alpha_0 \in \mathbb{F}_q^\times$ un générateur du groupe multiplicatif $\mathbb{F}_q^\times = \langle \alpha_0 \rangle$. Alors $\mathbb{F}_q = \mathbb{F}_p(\alpha_0)$ (théorème de l'élément primitif dans les corps finis, voir [7] si besoin).
Donc $\pi_{\mathbb{F}_p,\alpha_0}$ est de degré n.
Comme $\varphi_{\mathbb{F}_p} = \mathrm{id}$ et que φ est un automorphisme de corps de $\mathbb{F}_q$:

$$\forall i \in [\![0, n-1]\!], \quad 0 = \varphi^i\left(\pi_{\mathbb{F}_p,\alpha_0}(\alpha_0)\right) = \pi_{\mathbb{F}_p,\alpha_0}\left(\varphi^i(\alpha_0)\right)$$

Donc $\varphi^i(\alpha_0)$ est racine de $\pi_{\mathbb{F}_p,\alpha_0}$ pour $0 \leqslant i \leqslant n-1$.

De plus elles sont toutes distinctes car si $0 \leqslant i < j \leqslant n-1$ alors $\alpha_0^{p^i} = \alpha_0^{p^j} \iff \alpha_0^{p^j - p^i} = 1 \iff p^j - p^i \in (p^n - 1)\mathbb{Z} = (q-1)\mathbb{Z}$ car $\langle \alpha_0 \rangle = \mathbb{F}_q^\times$.
Mais $p^j - p^i \in [\![1, p^{n-1} - 1]\!]$.

Au total, on a obtenu que $\pi_{\mathbb{F}_p,\alpha_0}$ est scindé simple sur $\mathbb{F}_q$ (avec n racines distinctes).

D'après le théorème on a alors :

$$N_{\mathbb{F}_p(\alpha_0)/\mathbb{F}_p}(\alpha_0) = N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha_0) = \prod_{i=0}^{n-1} \varphi^i(\alpha_0) = \prod_{i=0}^{n-1} \alpha_0^{p^i} = \alpha_0^{\sum_{i=0}^{n-1} p^i} = \alpha_0^{\frac{p^n-1}{p-1}} = \alpha_0^{\frac{q-1}{p-1}}$$

On en déduit donc :

$$\forall k \in \mathbb{N}, \quad N_{\mathbb{F}_q/\mathbb{F}_p}\left(\alpha_0^k\right) = N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha_0)^k = \left(\alpha_0^{\frac{q-1}{q}}\right)^k = \left(\alpha_0^k\right)^{\frac{q-1}{p-1}}$$

mais donc comme α_0 engendre $\mathbb{F}_q^\times$, il sort finalement :

$$\forall \alpha \in \mathbb{F}_q^\times, \quad N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \alpha^{\frac{q-1}{p-1}} = \prod_{i=0}^{n-1} \varphi^i(\alpha)$$

Le résultat demeure pour $\alpha = 0$.

■

Corollaire 19: Les carrés dans $\mathbb{F}_q$

$\alpha \in (\mathbb{F}_q)^2 \iff N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) \in (\mathbb{F}_p)^2$.

Démonstration. Le cas $\alpha = 0$ est immédiat. Supposons donc $\alpha \in \mathbb{F}_q^\times$.

— Si $\alpha \in \left(\mathbb{F}_q^\times\right)^2$, alors il existe $\beta \in \mathbb{F}_q^\times$ tel que $\alpha = \beta^2$. La multiplicativité de la norme donne alors :

$$N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = N_{\mathbb{F}_q/\mathbb{F}_p}\left(\beta^2\right) = \left(N_{\mathbb{F}_q/\mathbb{F}_p}(\beta)\right)^2 \quad \Longrightarrow \quad N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) \in \left(\mathbb{F}_p^\times\right)^2$$

— Si $N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) \in \left(\mathbb{F}_p^\times\right)^2$, alors :

$$\alpha^{\frac{q-1}{2}} = \left(\alpha^{\frac{q-1}{p-1}}\right)^{\frac{p-1}{2}} = N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)^{\frac{p-1}{2}} = 1$$

par le lemme d'Euler car $N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$ est un carré. En conclusion α est un carré dans $\mathbb{F}_q$.

■

Remarque 20

Si vous souhaitez une autre application, il y a une très jolie application du théorème pour déterminer les inversibles d'un entier de corps de nombre sur le site de Matthias Hostein. Vous pouvez aussi regarder le super livre (quoique pas tout-à-fait récent) de Pierre Samuel [13]. Si vous choisissez cette autre application alors il faudra que vous sachiez justifier que l'ensemble des entiers d'un corps de nombre est un anneau (c'est supposé su dans le développement de Matthias), ce qui nécessite de parler de $\mathbb{Z}$-module de type fini et de savoir que le théorème de Cayley-Hamilton se généralise dans le cas des modules. Tout ceci est fait dans le livre de théorie algébrique des nombres de Pierre Samuel (il fait aussi le joli théorème de Minkowski (ça ne se refuse pas quand on l'a déjà vu en M1 en cours de théorie des nombres) très utile pour la leçon connexité dans $\mathbb{R}^n$ si on justifie bien que l'hypothèse de convexité est cruciale mais ça c'est une autre histoire).