2.5 L'algèbre linéaire au service de la théorie des corps : la norme (125, 127, 144, 149) [22]

Dans ce développement, pour K un corps et L une extension finie de K, je propose d'étudier l'application, pour $\alpha \in L$ fixé :

$$\begin{array}{rccc} \mu_\alpha & : & L & \longrightarrow & L \\ & & x & \longmapsto & \alpha x. \end{array}$$

Son déterminant, appelé "norme" est un outil puissant de théorie des corps dont nous allons montrer quelques propriétés élémentaires et une application pour caractériser les carrés dans les corps finis.

Définition 2.13 (Norme)**.** Soient K un corps, L une extension finie de K de degré n et $\alpha \in L$. L'application μ_α définie ci-dessus est un endomorphisme K-linéaire de L. On appelle alors *norme de α relativement à K*, notée $N_{L/K}(\alpha)$ la quantité :

$$N_{L/K}(\alpha) = \det(\mu_\alpha) \in K.$$

Proposition 2.14. 1. Soit L/K une extension finie et $\alpha \in L$. Alors, en notant :

$$\pi_{K,\alpha} = X^m + \sum_{i=0}^{m-1} a_i X^i$$

on a :

$$\mathrm{Mat}_{\mathscr{B}(\alpha)}(\mu_\alpha) = C_{\pi_{K,\alpha}}$$

où $\mathscr{B}(\alpha)$ désigne la K-base $(1, \alpha, \ldots, \alpha^{m-1})$ de $K(\alpha)$. En particulier :

$$\pi_{K,\alpha} = \chi_{\mu_\alpha}$$

et :

$$N_{K(\alpha)/K}(\alpha) = (-1)^m a_0.$$

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

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

en notant $x_1, \ldots, x_n \in L$ les racines de $\pi_{K,\alpha}$.

2. De façon plus générale, il exsite une K-base de L telle que l'endomorphisme μ_α ait pour matrice dans cette base :

$$\underbrace{\begin{pmatrix} C_{\pi_{K,\alpha}} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & C_{\pi_{K,\alpha}} & \cdots & \mathbf{O} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{O} & \cdots & \mathbf{O} & C_{\pi_{K,\alpha}} \end{pmatrix}}_{[L:K(\alpha)] \text{ blocs}}$$

En particulier, si $M/L/K$ est une tour d'extensions finies, alors :

$$\forall \alpha \in L, \quad N_{M/K}(\alpha) = \left(N_{L/K}(\alpha)\right)^{[M:L]}.$$

Démonstration. 1. Justifions que $\mathscr{B}(\alpha)$ est bien une K-base de $K(\alpha)$. Il s'agit d'une famille K-libre de $K(\alpha)$:

si $(\lambda_0, \ldots, \lambda_{m-1}) \in K^m$ sont tels que :

$$\sum_{i=0}^{m-1} \lambda_i \alpha^i = 0$$

alors le polynôme :

$$P = \sum_{i=0}^{m-1} \lambda_i X^i$$

annule α. Ainsi, par définition du polynôme minimal, on a :

$$\pi_{K,\alpha} \mid P.$$

Or, $\deg(\pi_{K,\alpha}) = m > \deg(P)$. Ainsi, $P = 0$ et donc $\lambda_0 = \ldots = \lambda_{m-1} = 0$. Et il s'agit bien d'une famille génératrice d'après l'isomorphisme :

$$K(\alpha) \simeq \frac{K[X]}{(\pi_{K,\alpha})}.$$

Dans cette base, l'endomorphisme μ_α a alors pour matrice :

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

On en conclut donc que $\pi_{K,\alpha} = \chi_{\mu_\alpha}$ et donc $N_{K(\alpha)/K}(\alpha) = (-1)^m a_0$. En effet, on a :

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

et, en effectuant l'opération élémentaire :

$$L_1 \longleftarrow L_1 + XL_2 + \ldots X^{m-1} L_m,$$

on obtient :

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

et donc, en développant selon la première ligne, on obtient :

$$\chi_{\mu_\alpha} = (-1)^{m+1} \pi_{K,\alpha} \begin{vmatrix} -1 & X & 0 & \cdots & 0 \\ 0 & -1 & X & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 & X \\ 0 & 0 & \cdots & 0 & -1 \end{vmatrix} = (-1)^{m+1} \pi_{K,\alpha} (-1)^{m-1} = \pi_{K,\alpha}.$$

Ainsi, on a :

$$\pi_{K,\alpha} = X^m - \mathrm{tr}(\mu_\alpha)X^{m-1} + \ldots + (-1)^m \det(\mu_\alpha).$$

D'où, en identifiant les coefficients :

$$N_{K(\alpha)/K}(\alpha) = (-1)^m a_0.$$

De plus, si L contient un corps de décomposition de $\pi_{K,\alpha}$, on peut écrire :

$$\pi_{K,\alpha} = \prod_{i=1}^{m}(X - x_i)$$

on a directement, en identifiant les coefficients :

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

2. D'après le théorème de la base téléscopique, en notant $d = [L : K(\alpha)]$, si $(e_1, \ldots, e_d)$ est une $K(\alpha)$-base de L, alors la famille :

$$\mathscr{B} = (e_1, \alpha e_1, \ldots, \alpha^{m-1}e_1, e_2, \ldots, \alpha^{m-1}e_2, \ldots, e_d, \ldots, \alpha^{m-1}e_d)$$

est une K-base de L. Dans cette base, on a bien :

$$\mathrm{Mat}_{\mathscr{B}}(\mu_\alpha) = \begin{pmatrix} C_{\pi_{K,\alpha}} & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & C_{\pi_{K,\alpha}} & \cdots & \mathbf{O} \\ \vdots & \ddots & \ddots & \vdots \\ \mathbf{O} & \cdots & \mathbf{O} & C_{\pi_{K,\alpha}} \end{pmatrix}.$$

Ainsi, on a :

$$\chi_{\mu_\alpha} = (\pi_{K,\alpha})^d$$

et donc :

$$N_{L/K}(\alpha) = \left(N_{K(\alpha)/K}(\alpha)\right)^d.$$

Ainsi, si $M/L/K$ est une tour d'extensions finies de K, on a, pour tout $\alpha \in L$:

$$\begin{aligned} N_{M/K}(\alpha) &= \left(N_{K(\alpha)/K}(\alpha)\right)^{[M:K(\alpha)]} \\ &= \left(N_{K(\alpha)/K}(\alpha)\right)^{[M:L]\times[L:K(\alpha)]} \\ &= \left(\left(N_{K(\alpha)/K}(\alpha)\right)^{[L:K(\alpha)]}\right)^{[M:L]} \\ &= \left(N_{L/K}(\alpha)\right)^{[M:L]}. \end{aligned}$$

□

On est prêt à montrer la formule dans le cadre des corps finis.

Théorème 2.15 (Norme d'un élément dans un corps fini)**.** Soit p un nombre premier et $q = p^n$ avec $n \in \mathbb{N}^*$. On a :

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

où φ désigne l'automorphisme de Frobenius.

Corollaire 2.16 (Les carrés dans $\mathbb{F}_q$)**.** Avec les mêmes notations que précédemment, $\alpha \in \mathbb{F}_q$ est un carré si et seulement si $N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$ est un carré dans $\mathbb{F}_p$.

Démonstration du théorème. Soit $\alpha_0 \in \mathbb{F}_q^\times$ un générateur du groupe multiplicatif $\mathbb{F}_q^\times$. On a alors clairement que $\mathbb{F}_q = \mathbb{F}_p(\alpha_0)$ (théorème de l'élément primitif dans les corps finis, très facile à voir). De plus, $\pi_{\mathbb{F}_p,\alpha_0}$ est scindé dans $\mathbb{F}_q$ et ses racines sont les $\left(\varphi^i(\alpha_0)\right)_{0\leqslant i\leqslant n-1}$. En effet, puisque $\mathbb{F}_q = \mathbb{F}_p(\alpha_0)$, $\pi_{\mathbb{F}_p,\alpha_0}$ est de degré n, donc admet au plus n racines dans $\mathbb{F}_q$. Or, puisque φ fixe le corps $\mathbb{F}_p$, on a :

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

Ainsi, pour tout $i \in [\![0, n-1]\!]$, $\varphi^i(\alpha_0)$ est racine de $\pi_{\mathbb{F}_p,\alpha_0}$. Or, ces éléments sont tous distincts dans $\mathbb{F}_q$. En effet, si $i, j \in [\![0, n-1]\!]$ sont tels que $i < j$ et $\alpha_0^{p^i} = \alpha_0^{p^j}$, alors :

$$\alpha_0^{p^j - p^i} = 1.$$

Or, $p^j - p^i \in [\![1, p^{n-1} - 1]\!]$ **ABSURDE** car α_0, par son caractère générateur, est d'ordre $p^n - 1$. Ainsi, d'après le point 1 de la proposition 2.14, on a :

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

On en déduit donc :

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

et donc, puisque α_0 est un générateur de $\mathbb{F}_q^\times$:

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

Le résultat est évidemment vrai également pour $\alpha = 0$ et cela conclut la preuve ! □

Preuve du corollaire. Si $\alpha = 0$, l'équivalence est directe. Supposons donc $\alpha \in \mathbb{F}_q^\times$. Si α est un carré dans $\mathbb{F}_q$, alors il exsite $\beta \in \mathbb{F}_q^\times$ tel que $\alpha = \beta^2$. On a alors :

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

ce qui veut dire, étant donné que $N_{\mathbb{F}_q/\mathbb{F}_p}$ est à valeurs dans $\mathbb{F}_p$, que $N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$ est un carré dans $\mathbb{F}_p$. Réciproquement, si $N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$ est un carré dans $\mathbb{F}_p$, alors :

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

car $N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$ est un carré dans $\mathbb{F}_p$. Ainsi, α est un carré dans $\mathbb{F}_q$, cela conclut donc la preuve ! □

Autre démonstration du théorème. Je propose une autre démonstration qui met plus en valeur l'aspect théorie des corps, pas juste le fait que $\mathbb{F}_q^\times$ est cyclique. Si $\alpha \in \mathbb{F}_q^\times$, même s'il n'est pas un élément primitif de $\mathbb{F}_q$, on peut retrouver la formule en observant que le sous-corps $\mathbb{F}_p(\alpha)$ de $\mathbb{F}_q$ est égal à un sous-ensemble fixe par une certaine puissance du Frobenius. Plus précisément, si $d = \deg\left(\pi_{\mathbb{F}_p,\alpha}\right)$, alors on a :

$$\mathbb{F}_p(\alpha) = \mathrm{Fix}\left(\varphi^d\right) := \left\{x \in \mathbb{F}_q \;\middle|\; \varphi^d(x) = x\right\}.$$

En effet, $\mathbb{F}_p(\alpha)$ est isomorphe en tant que $\mathbb{F}_p$-espace vectoriel à $\mathbb{F}_p^d$. C'est donc un sous-corps de $\mathbb{F}_q$ à p^d éléments. C'est donc le corps de décomposition du polynôme $X^{p^d} - X \in \mathbb{F}_p[X]$. De même, $\mathrm{Fix}\left(\varphi^d\right)$ est un sous-corps de $\mathbb{F}_q$ possédant les racines de $X^{p^d} - X$, au nombre de p^d car $X^{p^d} - X$ est premier avec son polynôme dérivé, qui est -1 et, puisque d divise n (multiplicativité des degrés), on a que $X^{p^d} - X$ divise $X^{p^n} - X$. Il est donc scindé dans $\mathbb{F}_q$. Or, par le même argument que pour la première preuve, on a :

$$N_{\mathbb{F}_{p(\alpha)}/\mathbb{F}_p}(\alpha) = \prod_{i=0}^{d-1} \varphi^i(\alpha).$$

Et donc, par le point 2 de la propriété 2.14 :

$$N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \left(\prod_{i=0}^{d-1} \varphi^i(\alpha)\right)^{\frac{n}{d}} = \prod_{i=0}^{d-1} \varphi^i(\alpha) \times \prod_{i=d}^{2d-1} \varphi^i(\alpha) \times \ldots \times \prod_{i=n-d}^{n-1} \varphi^i(\alpha)$$

puisque α est fixé par φ^d. On obtient donc bien :

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

□

Remarque 2.5.1. *La formule*

$$N_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \prod_{i=0}^{n-1} \varphi^i(\alpha)$$

peut se généraliser dans certains cas. En effet, si L/K est une extension finie ***normale et séparable****, c'est-à-dire que tout élément $\alpha \in L$ a son polynôme minimal sur K scindé et à racines simples dans L, alors :*

- $\mathrm{Gal}(L/K) := \left\{\sigma \in \mathrm{Aut}(L) \;\middle|\; \sigma_{|K} = id_K\right\}$ *est un sous-groupe de* $\mathrm{Aut}(L)$ *d'ordre exactement* $[L : K]$*, appelé "groupe de Galois de L/K ",*
- *Pour tout $\alpha \in L$, on a :*

$$N_{L/K}(\alpha) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(\alpha).$$

Pour le premier point, on montre que si L/K est une extension séparable, alors, si Ω est un corps algébriquement clos et $\sigma_0 : K \longrightarrow \Omega$ un morphisme de corps, alors le nombre de morphismes de corps $\sigma : L \longrightarrow \Omega$ tels que $\sigma_{|K} = \sigma_0$ ne dépend pas du couples (σ_0, Ω) et est égal à $[L : K]$. Et étant donné que dans une extension normale, pour tout morphisme de corps $\sigma : L \longrightarrow \overline{L}$, où $\overline{L}$ est une clôture algébrique de L, $\sigma(L) = L$, on a, en prenant σ_0 un morphisme de corps fixant K (par exemple l'injection canonique $K \longrightarrow \overline{L}$), que l'ensemble des morphismes de corps de L dans $\overline{L}$ prolongeant σ_0 sont exactement les automorphismes de L fixant K et il y en a donc $[L : K]$. Le deuxième point est plus technique mais repose sur la transitivité de la norme, prouvée en point 2 :

$$N_{M/K}(\alpha) = \left(N_{L/K}(\alpha)\right)^{[M:L]}$$

si $M/L/K$ est une tour d'extensions finies.

Bonus, peut-être plus adapté pour la leçon 127 :

Corollaire 2.17 (Les inversibles d'un entier de corps de nombres)**.** Soit K un corps de nombres, c'est-à-dire une extension finie du corps $\mathbb{Q}$. On note $\mathfrak{O}_K$ les *entiers* du corps K, c'est-à-dire les éléments de K annulés par un polynôme unitaire à coefficients dans $\mathbb{Z}$. Alors :

$$\mathfrak{O}_K^\times = \left\{ z \in \mathfrak{O}_K \;\middle|\; N_{K/\mathbb{Q}}(z) \in \{-1, 1\} \right\}.$$

Démonstration. **Étape 1 : Les éléments de $\mathfrak{O}_K$ ont leur polynôme minimal à coefficients dans $\mathbb{Z}$**
Soit $z \in \mathfrak{O}_K$ et soit π_z son polynôme minimal sur $\mathbb{Q}$. Puisque $z \in \mathfrak{O}_K$, il existe $P \in \mathbb{Z}[X]$ unitaire annulant z. Ainsi, π_z divise P, de sorte que toute racine z' de π_z est annulée par P. Ainsi, les racines de π_z sont éléments de $\mathfrak{O}_{\mathbb{C}}$, l'ensemble des entiers algébriques sur $\mathbb{C}$. Ainsi :

$$\pi_z = \prod_{i=1}^{r} (X - z_i) \in (\mathbb{Q} \cap \mathfrak{O}_{\mathbb{C}})[X] = \mathbb{Z}[X]$$

car $\mathfrak{O}_{\mathbb{C}}$ est un sous-anneau de $\mathbb{C}$ et $\mathbb{Q} \cap \mathfrak{O}_{\mathbb{C}} = \mathbb{Z}$. En effet, si p, q sont deux entiers premiers entre eux tels que $\frac{p}{q}$ est annulé par un polynôme unitaire à coefficients dans $\mathbb{Z}$, alors, en notant n le degré de ce polynôme, on a :

$$q \mid p^n, \quad \text{donc} \quad q \mid p$$

car q et p sont premiers entre eux. Ainsi, les seuls entiers q tels que $q \wedge p = 1$ et $q \mid p$ sont 1 et -1, donc tout rationnel annulé par un polynôme unitaire à coefficients entiers est entier.

Étape 2 : Conclusion
Soit $z \in \mathfrak{O}_K^\times$ et soit $d \in \mathbb{N}^*$ le degré $[K : \mathbb{Q}(z)]$. On a alors $\pi_z \in \mathbb{Z}[X]$, de sorte que :

$$N_{K/\mathbb{Q}}(z) = \left(N_{\mathbb{Q}(z)/\mathbb{Q}}(z)\right)^d = \left((-1)^{\deg(\pi_z)} \pi_z(0)\right)^d \in \mathbb{Z}.$$

Ainsi, si $z' \in \mathfrak{O}_K$ est tel que $zz' = 1$, alors $N_{K/\mathbb{Q}}(z') \in \mathbb{Z}$ également et :

$$1 = N_{K/\mathbb{Q}}(1) = N_{K/\mathbb{Q}}(zz') = N_{K/\mathbb{Q}}(z) N_{K/\mathbb{Q}}(z'),$$

de sorte que $N_{K/\mathbb{Q}}(z) \in \{-1, 1\}$. Réciproquement, si $z \in \mathfrak{O}_K$ est tel que $N_{K/\mathbb{Q}}(z) = 1$, alors, puisque $\mathbb{C}$ est algébriquement clos, on a la formule liant la norme aux racines de π_z :

$$N_{\mathbb{Q}(z)/\mathbb{Q}}(z) = \prod_{i=1}^{r} z_i$$

en notant $z_1, \ldots, z_r$ les racines de π_z (on a noté $r = \deg(\pi_z)$). On a donc :

$$N_{K/\mathbb{Q}}(z) = \left(\prod_{i=1}^{r} z_i \right)^d$$

Ainsi, quitte à renuméroter on peut supposer $z_1 = z$ et on a donc :

$$z \times \left(z^{d-1} \times \prod_{i=2}^{r} z_i^d \right) = 1.$$

Ainsi, ce produit appartient à K, car c'est un corps et le polynôme :

$$P = \prod_{i=1}^{r} \left(X - \prod_{j \neq i} z_j \right)$$

est unitaire et à coefficients entiers par le théorème de structure des polynômes symétriques : les coefficients de ce polynôme sont les polynômes symétriques élémentaires en les $\prod_{j \neq i} z_j$ (au signe près), qui sont des polynômes symétriques en les z_i. Ainsi, ils s'écrivent comme polynôme en les polynômes symétriques élémentaires en les z_i, qui sont entiers car $\pi_z \in \mathbb{Z}[X]$. Ainsi :

$$\prod_{i=2}^{r} z_i \in \mathfrak{O}_K \quad \text{et donc} \quad \left(\prod_{i=2}^{r} z_i \right)^d \in \mathfrak{O}_K.$$

On a donc $z \in \mathfrak{O}_K^\times$ car son inverse est :

$$z^{d-1} \left(\prod_{i=2}^{r} z_i \right)^d \in \mathfrak{O}_K.$$

□