Le théorème de la base normale

in ~/MATHS/GALOIS/

Voici une preuve extrêmement simple du théorème de la base normale (trouvée chez Artin E., "Galois theory", Notre Dame Mathematical Lectures, n°2).

(1) Théorème (de la base normale)

Soit L une extension galoisienne d'un corps **infini** *K, x un élément primitif de L sur K : $L = K(x)$ et $f \in K[X]$ le polynôme minimal de x sur K. Alors pour $\lambda \in K \setminus \{$partie finie$\}$, l'élément :*

$$y = \frac{f(\lambda)}{(\lambda - x)f'(x)}$$

est un élément normal de L sur K i.e. les $\sigma(y)$ pour $\sigma \in \mathrm{Gal}(L/K)$ forment une base de L sur K.

On notera que $f'(x) \neq 0$ car la séparabilité de L/K assure la séparabilité du polynôme f ; en particulier, x est une racine simple de f et l'on a bien $f'(x) \neq 0$.

Pour la commodité du lecteur, on rappelle quelques résultats classiques : dans les deux lemmes ci-dessous, on dispose d'une extension galoisienne L de degré n d'un corps quelconque K (non supposé infini, pour l'instant) et on note $\mathrm{Gal}(L/K) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$.

(2) Lemme

Soient $x_1, x_2, \ldots, x_n$ n éléments de L ; pour que $\{x_1, x_2, \ldots, x_n\}$ soit une base de L sur K, il faut et il suffit que $\det(\sigma_i(x_j)) \neq 0$

Preuve du lemme

Notons A la matrice définie par $a_{ij} = \sigma_i(x_j)$. Supposons $\det(A)$ non nul ; d'une relation $\sum_j \lambda_j x_j = 0$, $\lambda_j \in K$, il vient en appliquant σ_i :

$$\sum_j \lambda_j \sigma_i(x_j) = 0 \quad \text{c'est à dire} \quad A \begin{pmatrix} \lambda_1 \\ \\ \vdots \\ \lambda_n \end{pmatrix} = 0$$

Cela entraîne $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$; par conséquent $\{x_1, x_2, \ldots, x_n\}$ est une famille libre sur K, donc une base de L sur K.
Réciproquement, supposons que $\{x_1, x_2, \ldots, x_n\}$ soit une base de L sur K et montrons que les lignes de A sont linéairement indépendantes. Soit une combinaison linéaire (à coefficients dans K) des lignes de A, i.e. des scalaires $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$ tels que :

$$\sum_{i=1}^{n} \lambda_i \sigma_i(x_j) = 0, \qquad \text{pour } j = 1, \ldots, n$$

Par linéarité, il vient :

$$\sum_{i=1}^{n} \lambda_i \sigma_i(x) = 0, \text{ pour tout } x \in L \quad \text{c'est à dire} \quad \sum_{i=1}^{n} \lambda_i \sigma_i = 0,$$

Le théorème de l'indépendance linéaire des homomorphismes (théorème de Dedekind) entraîne $\lambda_i = 0$ pour $1 \leq i \leq n$.

Dans le contexte galoisien ci-dessus, on définit la trace de L sur K par :

$$\mathrm{tr}_{L/K}(y) = \sum_{\sigma \in \mathrm{Gal}(L/K)} \sigma(y), \qquad \mathrm{tr}_{L/K} : L \to K$$

On peut montrer que cette définition coïncide avec la définition plus générale (dans le cadre d'une extension finie L/K quelconque non nécessairement galoisienne) qui consiste à définir la trace (sur K) de $x \in L$ comme la trace du K-endomorphisme "multiplication par x".

(3) Lemme

Pour $x_1, x_2, \ldots, x_n \in L$, on a $\det(\mathrm{tr}_{L/K}(x_i x_j)) = \Big(\det(\sigma_i(x_j))\Big)^2$

Preuve du lemme

Soit A la matrice $(\sigma_i(x_j))_{ij}$ et B la matrice $(\mathrm{tr}_{L/K}(x_i x_j))_{ij}$. L'égalité :

$$\mathrm{tr}_{L/K}(x_i x_j) = \sum_{k=1}^{n} \sigma_k(x_i)\sigma_k(x_j)$$

prouve que $B_{ij} = ({}^t AA)_{ij}$ i.e. $B = {}^t AA$ d'où l'égalité pour les déterminants.

Preuve du théorème de la base normale

Le premier lemme dit qu'un élément $y \in L$ engendre une base normale si et seulement si :

$$\det\Big(\sigma\tau(y)_{\sigma,\tau}\Big) \neq 0$$

Notons $G = \mathrm{Gal}(L/K)$ le groupe de Galois de L sur K et pour $\sigma \in G$, définissons $g_\sigma, g \in L[X]$ par :

$$g_\sigma(X) = \frac{f(X)}{(X - \sigma(x))\, f'(\sigma(x))} \qquad \text{et} \qquad g(X) = g_{\mathrm{Id}}(X)$$

Cette définition est valide car $f'(x) \neq 0$ donc $f'(\sigma(x)) \neq 0$ pour tout $\sigma \in G$.
Il est clair que ${}^\tau g_\sigma = g_{\tau\sigma}$ et :

$$(\star) \qquad g_\sigma(x) = \begin{cases} 0 & \text{si } \sigma \neq \mathrm{Id} \\ 1 & \text{si } \sigma = \mathrm{Id} \end{cases}$$

En effet, x étant un élément primitif de L sur K, on a $\tau(x) \neq \sigma(x)$ pour $\tau \neq \sigma$.
Introduisons le polynôme $h \in L[X]$ défini par :

$$h(X) = \det\left(\sum_{\sigma \in G} g_{\sigma\tau}(X) g_{\sigma\tau'}(X)\right)_{\tau,\tau'}$$

Pour $\boxed{\lambda \in K}$, on a $\sigma(g_\tau(\lambda)) = g_{\sigma\tau}(\lambda) = \sigma\tau(g(\lambda))$ donc :

$$h(\lambda) = \det\Big(\mathrm{tr}(g_\tau(\lambda) g_{\tau'}(\lambda))\Big) = \det\Big(\sigma(g_\tau(\lambda))\Big)^2 = \det\Big(\sigma\tau(g(\lambda))\Big)^2$$

Le polynôme $h \in L[X]$ n'est pas identiquement nul puisqu'il vérifie $h(x) = 1$ d'après $(\star)$ (merci à toi, Lionel). En conclusion, pour $\lambda \in K$ non racine du polynôme h, le déterminant $\det\big(\sigma\tau(g(\lambda))\big)$ n'est pas nul, ce qui exprime que :

$$g(\lambda) = \frac{f(\lambda)}{(\lambda - x) f'(x)}$$

est un élément normal de L sur K.