Lemme de Dedekind et application

S. Francinou, H. Gianella, *Exercices pour l'agrégation, Algèbre 1*, Masson. Exercice B.4 page 243.

Recasage : 125, 151, 162.

Lemme 1 (*Dedekind*)

Soient K, L deux corps. Soient $f_1, \dots, f_n : K \to L$ des morphismes de corps distincts. Alors $f_1, \dots, f_n$ sont linéairement indépendants sur K.

▷ Supposons par l'absurde que la famille $(f_1, \dots, f_n)$ est liée. Parmi l'ensemble non vide des combinaisons linéaires nulles non triviales, on en choisit une de taille minimale, que l'on écrit, quitte à réordonner les f_i :

$$a_1 f_1 + \cdots + a_k f_k = 0 \tag{1}$$

avec $a_1, \dots, a_k \in K^\times$. Comme $f_1 \neq f_k$, il existe $z \in K$ tel que $f_1(z) \neq f_k(z)$. Alors,

$$\forall x \in K, \qquad a_1 f_1(xz) + \cdots + a_k f_k(xz) = 0$$

d'où

$$a_1 f_1(z) f_1 + \cdots + a_k f_k(z) f_k = 0. \tag{2}$$

L'opération $(2) - f_1(z) \times (1)$ donne :

$$a_2(f_2(z) - f_1(z))f_2 + \cdots + a_k(f_k(z) - f_1(z))f_k = 0$$

qui est une relation de liaison non triviale puisque $f_k(z) \neq f_1(z)$, ce qui contredit la minimalité de k. □

Théorème 2

Soient K un corps et G un groupe fini d'automorphismes de K. Notons $K^G = \{x \in K, \forall g \in G, g(x) = x\}$. Alors K^G est un sous-corps de K et $[K : K^G] = |G|$.

▷ Notons $n = |G|$ et $g_1 = e, g_2, \dots, g_n$ les éléments de G.

– *Étape 1 : Supposons par l'absurde que* $[K : K^G] < n$. Soit alors $x_1, \dots, x_p$ $(p < n)$ une base de K en tant que K^G-espace vectoriel. Considérons l'application linéaire $f : K^n \to K^p$ ayant pour matrice dans les bases canoniques : $(g_j(x_i))_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}}$. Comme $p < n$, d'après le théorème du rang, $\operatorname{Ker} f \neq (0)$ donc il existe $z_1, \dots, z_n \in K$ tels que

$$\forall 1 \leq i \leq p, \qquad z_1 g_1(x_i) + \cdots + z_n g_n(x_i) = 0.$$

Soit $a \in K$. Il existe $\lambda_1, \dots, \lambda_p \in K^G$ tels que $a = \sum_{i=1}^{p} \lambda_i x_i$. Alors,

$$\begin{aligned} \sum_{j=1}^{n} z_j g_j(a) &= \sum_{j=1}^{n} z_j \sum_{i=1}^{p} g_j(\lambda_i) g_j(x_i) \\ &\underset{\lambda_i \in K^G}{=} \sum_{i=1}^{p} \lambda_i \underbrace{\left(\sum_{j=1}^{n} z_j g_j(x_i) \right)}_{=0} = 0. \end{aligned}$$

Ainsi, $z_1 g_1 + \cdots + z_n g_n \equiv 0_K$ ce qui contredit le lemme de Dedekind.

– *Étape 2 : Supposons par l'absurde qu'il existe* $x_1, \dots, x_{n+1}$ $n+1$ *éléments de* K *linéairement indépendants sur* K^G. Pour $1 \leq i \leq n+1$, posons

$$X_i = \begin{pmatrix} g_1(x_i) \\ \vdots \\ g_n(x_i) \end{pmatrix}.$$

On dispose donc d'une famille $(X_1, \dots, X_{n+1})$ de $(n+1)$ vecteurs de K^n, qui est donc liée : en considérant une combinaison linéaire non triviale nulle de taille minimale, et quitte à réordonner les X_i, on peut écrire

$$z_1 X_1 + \cdots + z_k X_k = 0 \tag{3}$$

avec $z_1, \dots, z_k \in K^\times$. Considérons l'action de G sur K^n définie par

$$\forall g \in G, \forall (u_1, \dots, u_n) \in K^n, \qquad g \cdot \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \begin{pmatrix} g(u_1) \\ \vdots \\ g(u_n) \end{pmatrix}.$$

Comme la translation $\begin{array}{ccc} G & \to & G \\ h & \mapsto & gh \end{array}$ est une bijection, un élément $g \in G$ agit sur X_i par permutation des lignes. En faisant agir $g \in G$ sur (3), on obtient

$$g(z_1) g \cdot X_1 + \cdots + g(z_n) g \cdot X_k = 0$$

soit, après réorganisation des lignes,

$$g(z_1) X_1 + \cdots + g(z_k) X_k = 0. \tag{4}$$

En effectuant l'opération (3) $\times\, g(z_1) -$ (4) $\times\, z_1$ on obtient :

$$(z_2 g(z_1) - z_1 g(z_2)) X_2 + \cdots + (z_k g(z_1) - z_1 g(z_k)) X_k = 0.$$

Par minimalité de k, chacun des coefficients doit être nul, pour tout g, donc

$$\forall g \in G, \forall 1 \leq i \leq k, \qquad g(z_i z_1^{-1}) = z_i z_1^{-1}$$

ie. $\lambda_i = z_i z_1^{-1} \in K^G$ $\forall i$. Alors, l'équation (3) s'écrit

$$z_1 \lambda_1 X_1 + \cdots + z_1 \lambda_k X_k = 0$$

soit, comme $z_1 \neq 0$,

$$\lambda_1 X_1 + \cdots + \lambda_k X_k = 0$$

d'où

$$\forall 1 \leq j \leq n, \qquad g_j \left(\sum_{i=1}^{k} \lambda_i x_i \right) = 0$$

et donc

$$\sum_{i=1}^{k} \lambda_i x_i = 0$$

ce qui contredit la liberté de $(x_1, \dots, x_{n+1})$.

– *Conclusion.* L'extension K/K^G est donc finie et $[K : K^G] = n = |G|$. □