Corrigé Devoir 3

Exercice 1 — Autour de Dedekind. Soient k un corps, K une extension de k (pas nécessairement de dimension finie) et $\sigma \in \mathrm{Gal}(\mathrm{K}/k)$.

a) On suppose que σ vérifie $\sigma(x) + \sigma^2(x) = x + \sigma^3(x)$ pour tout $x \in \mathrm{K}$. Montrer que $\sigma^2 = \mathrm{id}$.

b) Montrer que l'équivalence des propriétés suivantes :

(i) σ est d'ordre fini dans le groupe $\mathrm{Gal}(\mathrm{K}/k)$;
(ii) le k-endomorphisme σ de K admet un polynôme minimal non nul ;
(iii) l'algèbre $k[\sigma]$ est de dimension finie.

c) On suppose que les conditions de la question **b** sont vérifiées. Déterminer le polynôme minimal de σ.

d) Montrer que les conditions de la question **b** sont vérifiées si $[\mathrm{K} : k] < +\infty$. En déduire qu'un k-automorphisme de K ne peut être d'ordre infini que si $[\mathrm{K} : k] = +\infty$.

e) Reprendre la question **a** en utilisant les résultats des questions **b** et **c**.

Corrigé

a) La relation $\sigma(x)+\sigma^2(x) = x+\sigma^3(x)$ pour tout $x \in \mathrm{K}$ dit que la famille de k-endomorphismes $(\mathrm{id}_\mathrm{K}, \sigma, \sigma^2, \sigma^3)$ est liée. Le lemme de Dedekind assure qu'il existe $i \neq j$ avec $i, j \in \{0, 1, 2, 3\}$ tel que $\sigma^i = \sigma^j$. On peut supposer que $i < j$. On a donc $\sigma^{j-i} = \mathrm{id}_\mathrm{K}$ avec $j - i \in \{1, 2, 3\}$. Si $j - i = 1$ alors $\sigma = \mathrm{id}_\mathrm{K}$ et donc $\sigma^2 = \mathrm{id}_\mathrm{K}$. Si $j - i = 2$, on a le résultat souhaité. Supposons que $j - i = 3$ alors $\sigma^3 = \mathrm{id}_\mathrm{K}$ et donc $\sigma(x) + \sigma^2(x) = 2x$ pour tout $x \in \mathrm{K}$. On a une relation de dépendance linéaire entre $(\mathrm{id}_\mathrm{K}, \sigma, \sigma^2)$ et donc, encore grâce au lemme de Dedekind, on a $\sigma = \mathrm{id}_\mathrm{K}$ ou $\sigma^2 = \mathrm{id}_\mathrm{K}$ ou $\sigma = \sigma^2$ ce qui donne $\sigma = \mathrm{id}_\mathrm{K}$.

b) $(i) \Rightarrow (ii)$. Notons n l'ordre de σ. Le polynôme $\mathrm{X}^n - 1$ est un polynôme annulateur de σ. Ainsi l'idéal annulateur de σ n'est pas réduit à 0 et σ admet donc un polynôme minimal qui est un diviseur de $\mathrm{X}^n - 1$.

$(ii) \Rightarrow (iii)$. On note I l'idéal annulateur de σ. Par définition le polynôme minimal π_σ de σ est le polynôme unitaire vérifiant $\mathrm{I} = \langle \pi_\sigma \rangle$. et on a $k[\sigma] = k[\mathrm{X}]/\pi_\sigma$ dont la dimension est le degré de π_σ.

$(iii) \Rightarrow (i)$. Si l'idéal annulateur de σ est réduit à 0 alors $k[\sigma] = k[\mathrm{X}]$ n'est pas de dimension finie. On en déduit qu'il existe un polynôme annulateur non nul pour σ. On obtient ainsi une relation de dépendance linéaire entre les puissances de σ. Le lemme de Dedekind assure qu'il existe $i \neq j$ (on suppose $i < j$) tel que $\sigma^i = \sigma^j$ et donc $\sigma^{j-i} = \mathrm{id}_\mathrm{K}$. Ainsi σ est d'ordre fini.

c) On note n l'ordre de σ. Le polynôme $\mathrm{X}^n - 1$ est un polynôme annulateur de σ. Ainsi le polynôme minimal π_σ de σ est un diviseur de $\mathrm{X}^n - 1$. En particulier, il est de degré $d \leqslant n$. La relation $\pi_\sigma(\sigma) = 0$ donne alors une relation de dépendance linéaire portant sur la famille $(\mathrm{id}_\mathrm{K}, \sigma, \ldots, \sigma^d)$. Le lemme de Dedekind assure alors qu'il existe $i \neq j$ avec $i, j \in [\![0 , d]\!]$ tel que $\sigma^i = \sigma^j$. En supposant $i < j$, on obtient $\sigma^{j-i} = \mathrm{id}_\mathrm{K}$ avec $j - i \in [\![1 , d]\!]$. Ainsi, l'ordre n de σ est un diviseur de d et donc en particulier $n \leqslant d$. Finalement $d = n$. Comme $\pi_\sigma \mid \mathrm{X}^n - 1$, la relation sur les degrés assure que $\pi_\sigma = \mathrm{X}^n - 1$.

d) Si $[\mathrm{K} : k] < +\infty$ alors $\mathrm{End}_k(\mathrm{K})$ est de dimension finie et $k[\sigma] \subset \mathrm{End}_k(\mathrm{K})$ aussi. Le point (iii) est donc vérifié. La contraposée de cette affirmation donne le deuxième résultat.

e) Le polynôme $\mathrm{X}^3 - \mathrm{X}^2 - \mathrm{X} + 1 = (\mathrm{X}^2 - 1)(\mathrm{X} - 1)$ est un polynôme annulateur (non nul) de σ. On est donc dans les conditions de la question **b**. Le polynôme minimal de σ est donc diviseur de $(\mathrm{X}^2 - 1)(\mathrm{X} - 1)$ de la forme $\mathrm{X}^n - 1$ (d'après la question **c**). On en déduit que $n = 1$ ou $n = 2$.