École Polytechnique 2009-2010

Théorie de Galois

Corrigé de la Feuille d'exercices 3

Exercice 1.

(i) Soit $\phi : k[X] \to K$ le morphisme de k-algèbres défini dans l'énoncé. Par définition de Π_x, on a $\mathrm{Ker}(\phi) = (\Pi_x)$. De plus l'image de ϕ est $k[x]$. Donc ϕ induit un isomorphisme de k-algèbres $(k[X]/\mathrm{Ker}(\phi)) \simeq \mathrm{Im}(\phi)$, c'est à dire $(k[X]/(\Pi_x)) \simeq k[x]$.

(ii) Soit Ψ l'application de $\mathrm{Hom}_{k-alg}(k[x], L)$ vers L définie pas $\Psi(\phi) = \phi(x)$. Comme x est une racine de $\Pi_x \in k[X]$, l'image de Ψ est contenue dans l'ensemble R des racines de Π_x dans L. De plus un morphisme $\phi \in \mathrm{Hom}_{k-alg}(k[x], L)$ est entièrement déterminé par $\phi(x)$. Donc Ψ est injective. Maintenant soit $y \in R$. On a un morphisme de k-algèbres naturel de $\tilde{\phi} : k[X] \to L$ défini par $\tilde{\phi}(P) = P(y)$. Comme $y \in R$, on a $(\Pi_x) \subset \mathrm{Ker}(\tilde{\phi})$. Donc $\tilde{\phi}$ induit un morphisme de k-algèbres $\phi : (k[X]/(\Pi_x)) \to L$. D'après (i), ϕ est un élément de $\mathrm{Hom}_{k-alg}(k[x], L)$. Donc Ψ est surjective.

Si L est un corps, Π_x a au plus $\deg(\Pi_x) = [k[x] : k]$ racines dans L, d'où l'inégalité.

(iii) Soit $R \in k[X]$ non constant irréductible qui divise P. Alors $k[X]/(R)$ est un corps et la classe de X dans ce corps est une racine de R. Montrons le deuxième résultat par récurrence sur le degré de P. Si P est de degré 1, P est déjà scindé dans k. En général, on commence par construire une extension $k \subset k_1$ comme ci-dessus tel que P a une racine x dans k_1. Alors dans $k_1[X]$, P se factorise sous la forme $P(X) = (X - x)P_1(X)$. En utilisant l'hypothèse de récurrence, on obtient une extension $k_1 \subset k_2$ dans laquelle P_1 est scindé. Donc P est scindé dans k_2.

Exercice 2. Soit $\phi : K \to K$ un morphisme de k-algèbres.

(i) Le noyau de ϕ est un idéal de K non égal à K (car $\phi(1) \neq 0$). Comme K est un corps, $\mathrm{Ker}(\phi) = \{0\}$ et ϕ est injective. Maintenant un endomorphisme linéaire injectif en dimension fini est un automorphisme.

(ii) Soit $x \in K$ et K_x le sous-corps de K engendré par les racines $\{x_1, \cdots, x_N\}$ de Π_x dans K. On a $\phi(\{x_1, \cdots, x_N\}) \subset \{x_1, \cdots, x_N\}$, donc K_x est stable par ϕ. De plus

$$[K_x : k] \leq [k[x_n] : k][k[x_{n-1}] : k] \cdots [k[x_1] : k] \leq (\deg(\Pi_x))^{\deg(\Pi_x)} < \infty.$$

Donc K_x est de dimension finie sur k, et d'après (i), ϕ induit un isomorphisme de K_x. Donc $K_x \subset \mathrm{Im}(\phi)$ et $x \in \mathrm{Im}(\phi)$. Donc ϕ est surjective, donc ϕ est un automorphisme.

Exercice 3.

(i) Par définition, $\overline{\mathbf{Q}}$ est algébrique sur $\mathbf{Q}$. Maintenant, soit $P(X) = \sum_{0 \leq i \leq n} a_i X^i \in \overline{\mathbf{Q}}$. Alors pour $K = \mathbf{Q}[x_1, \cdots, x_n]$, on a

$$[K : \mathbf{Q}] \leq [\mathbf{Q}(x_n) : \mathbf{Q}] \cdots [\mathbf{Q}(x_1) : \mathbf{Q}].$$

Donc $[K : \mathbf{Q}] < \infty$. Alors pour x une racine de P dans $\mathbf{C}$, on a $[\mathbf{Q}(x) : \mathbf{Q}] \leq [K[x] : K][K : \mathbf{Q}] < \infty$. Donc $x \in \overline{\mathbf{Q}}$. Comme P est scindé dans $\mathbf{C}$, il est scindé dans $\overline{\mathbf{Q}}$.

On a clairement $\mathrm{Aut}_{\mathbf{Q}}(\overline{\mathbf{Q}}) \subset \mathrm{Hom}_{\mathbf{Q}-\mathrm{alg}}(\overline{\mathbf{Q}}, \overline{\mathbf{Q}}) \subset \mathrm{Hom}_{\mathbf{Q}-\mathrm{alg}}(\overline{\mathbf{Q}}, \mathbf{C})$. Maintenant, l'image d'un élément algébrique sur $\mathbf{Q}$ par un morphisme de $\mathbf{Q}$-algèbre est algébrique sur $\mathbf{Q}$. Donc $\mathrm{Hom}_{\mathbf{Q}-\mathrm{alg}}(\overline{\mathbf{Q}}, \overline{\mathbf{Q}}) = \mathrm{Hom}_{\mathbf{Q}-\mathrm{alg}}(\overline{\mathbf{Q}}, \mathbf{C})$. L'égalité $\mathrm{Aut}_{\mathbf{Q}}(\overline{\mathbf{Q}}) = \mathrm{Hom}_{\mathbf{Q}-\mathrm{alg}}(\overline{\mathbf{Q}}, \overline{\mathbf{Q}})$ se déduit de l'exercice 2.

(ii) On a $\overline{\mathbf{Q}} = \cup_{P \in \mathbf{Q}[X]}\{\text{Racines de } P\}$. Comme les $\{\text{Racines de } P\}$ sont finis, il suffit de montrer que $\mathbf{Q}[X]$ est dénombrable. Mais

$$\mathbf{Q}[X] = \cup_{n \geq 0}\{\text{Polynômes de } \mathbf{Q}[X] \text{ de degré } \leq n\}.$$

On peut conclure car l'ensemble des polynômes de $\mathbf{Q}[X]$ de degré $\leq n$ est dénombrable étant en bijection avec $\mathbf{Q}^{n+1}$ (et $\mathbf{Q}$ est dénombrable).

(iii) $\sigma(i)$ est une racine de $X^2 - 1$ donc $\sigma(i) \in \{i, -i\}$. Si $\sigma(i) = i$, σ coïncide avec l'identité sur $\mathbf{Q} \oplus \mathbf{Q}i$. Cet espace est dense dans $\overline{\mathbf{Q}}$. Par continuité de σ, σ est l'identité sur $\overline{\mathbf{Q}}$. Le cas $\sigma(i) = -i$ est traité de la même manière.

(iv) Soit n un entier. Notons d'abord que $\sqrt[n]{2}$ est une racine de $X^n - 2 \in \mathbf{Q}[X]$. En utilisant le critère d'Eisenstein avec $p = 2$, on obtient que $X^n - 2$ est irréductible sur $\mathbf{Q}$. Donc c'est le polynôme minimal de $\sqrt[n]{2}$ sur $\mathbf{Q}$. Soit ζ une racine nème de l'unité. Alors $\zeta\sqrt[n]{2}$ est une racine de $X^n - 2$. Donc d'après l'exercice 1, on a un (unique) morphisme de $\mathbf{Q}$-algèbre $\phi : \mathbf{Q}[\sqrt[n]{2}] \to \overline{\mathbf{Q}}$ tel que $\phi(\sqrt[n]{2}) = \zeta\sqrt[n]{2}$. Le théorème de prolongement des morphisme donne un plongement de la $\mathbf{Q}[\sqrt[n]{2}]$-algèbre $\overline{\mathbf{Q}}$ dans $\overline{\mathbf{Q}}$, c'est à dire un prolongement $\tilde{\phi}$ de ϕ à $\overline{\mathbf{Q}}$. D'après (i), $\tilde{\phi}$ est un élément de $\mathrm{Aut}_{\mathbf{Q}}(\overline{\mathbf{Q}})$. On obtient ainsi n éléments différents de $\mathrm{Aut}_{\mathbf{Q}}(\overline{\mathbf{Q}})$, et ce pour tout n. Donc $\mathrm{Aut}_{\mathbf{Q}}(\overline{\mathbf{Q}})$ est infini.