École Polytechnique 2009-2010

Théorie de Galois

Feuille d'exercices 3

Pour $k \subset K$ une extension de corps et $x \in K$ algébrique sur k, on note $\Pi_x \in k[X]$ le polynôme minimal de x sur k.

Exercice 1. (Rappels de cours) (i) Soient $k \subset K$ une extension de corps et $x \in K$ algébrique sur k. Montrer que l'application $k[X] \to K$, $P \mapsto P(x)$, induit un isomorphisme de k-algèbres $k[X]/(\Pi_x) \xrightarrow{\sim} k[x]$.

(ii) En déduire que pour toute k-algèbre L, $\mathrm{Hom}_{k-alg}(k[x], L)$ est en bijection naturelle avec l'ensemble des racines de Π_x dans L. En particulier, vérifier que si L est un corps alors $|\mathrm{Hom}_{k-alg}(k[x], L)| \leq [k[x] : k]$.

(iii) Soient k un corps et $P \in k[X]$ un polynôme non constant. Montrer qu'il existe un corps contenant k dans lequel P admet une racine (resp. dans lequel P est scindé).

Pour $k \subset K$ une extension de corps, on notera $\mathrm{Aut}_k(K)$ l'ensemble des automorphismes k-linéaires du corps K. C'est un groupe pour la composition.

Exercice 2. Soit $k \subset K$ une extension algébrique. On veut montrer que tout morphisme de k-algèbre $K \to K$ est un élément de $\mathrm{Aut}_k(K)$.

(i) Le démontrer quand $[K : k] < \infty$.

(ii) En déduire le cas général. Pour $x \in K$, on pourra considérer le sous-corps de K engendré par les racines de Π_x dans K.

Exercice 3. Soit $\overline{\mathbf{Q}} \subset \mathbf{C}$ le sous-corps des nombres algébriques sur $\mathbf{Q}$.

(i) Rappeler pourquoi $\overline{\mathbf{Q}}$ est une clôture algébrique de $\mathbf{Q}$. Montrer que $\mathrm{Hom}_{\mathbf{Q}-\mathrm{alg}}(\overline{\mathbf{Q}}, \mathbf{C}) = \mathrm{Hom}_{\mathbf{Q}-\mathrm{alg}}(\overline{\mathbf{Q}}, \overline{\mathbf{Q}}) = \mathrm{Aut}_{\mathbf{Q}}(\overline{\mathbf{Q}})$.

On rappelle qu'un ensemble X est dit dénombrable si il existe une surjection $\mathbf{N} \to X$. On admettra qu'un ensemble de la forme $X = \cup_{i \in I} X_i$, avec I et les X_i dénombrables, est dénombrable.

(ii) Montrer que $\overline{\mathbf{Q}}$ est dénombrable.

On munit $\mathbf{C}$, ainsi que ses parties, de la distance usuelle $d(z, z') = |z - z'|$.

(iii) Montrer que si $\sigma \in \mathrm{Aut}_{\mathbf{Q}}(\overline{\mathbf{Q}})$ est continu alors soit $\sigma = \mathrm{id}$, soit σ est la conjugaison complexe.

(iv) En revanche, montrer que $\mathrm{Aut}_{\mathbf{Q}}(\overline{\mathbf{Q}})$ est infini. On pourra par exemple démontrer, en utilisant le théorème de prolongement, que pour tout entier n et toute racine nième de l'unité ζ il existe $\sigma \in \mathrm{Aut}_{\mathbf{Q}}(\overline{\mathbf{Q}})$ tel que $\sigma(\sqrt[n]{2}) = \zeta \sqrt[n]{2}$.

Pour $k \subset K$ une extension de corps et $H \subset \mathrm{Aut}_k(K)$ une partie de $\mathrm{Aut}_k(K)$, par exemple un sous-groupe, on note K^H l'ensemble des points fixes de H dans K, c'est à dire $\{x \in K, \sigma(x) = x \ \forall \sigma \in H\}$. C'est un sous-corps de K.

Exercice 4. Soit $d \in \mathbf{Z}$ qui n'est pas un carré.

(i) Montrer que $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{Q}[\sqrt{d}])$ est un groupe à deux éléments, constitué de l'identité et de l'application σ définie par $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$ pour tout $a, b \in \mathbf{Q}$.

(ii) Soit $d' \in \mathbf{Z}$ qui n'est pas un carré. En utilisant σ, montrer que $\sqrt{d'} \in \mathbf{Q}[\sqrt{d}]$ si, et seulement si, d'/d est le carré d'un nombre rationnel.

(iii) Si $z \in \mathbf{Q}[\sqrt{d}]$, on pose $N(z) = z\sigma(z) \in \mathbf{Q}$ (justifier). Montrer que

$$\forall z, z' \in \mathbf{Q}[\sqrt{d}], \ \ N(zz') = N(z)N(z').$$

En déduire que les nombres rationels non nuls de la forme $a^2 - db^2$ avec $a, b \in \mathbf{Q}$ forment un sous-groupe de $\mathbf{Q}^*$ pour la multiplication. (Exemple classique : $d = -1$)

Exercice 5. Soient $K = \mathbf{Q}[\sqrt{2}, \sqrt{3}]$ et $G = \mathrm{Aut}_{\mathbf{Q}}(K)$. On se propose de déterminer la structure du groupe G ainsi que tous les sous-corps de K.

(i) Montrer que $[K : \mathbf{Q}] = 4$ et donner trois sous-corps stricts[1] de K. Montrer que $|G| \leq 4$.

(ii) Soit $x \in \{\sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Montrer que $\mathrm{Aut}_{\mathbf{Q}[x]}(K)$ a deux éléments et les décrire.

(iii) En déduire que $|G| = 4$. Lister les éléments de G et décrire K^σ pour chaque $\sigma \in G$.

(iv) Montrer que $G \simeq (\mathbf{Z}/2\mathbf{Z})^2$. On pourra soit raisonner directement, soit montrer que l'application $G \to \{\pm 1\} \times \{\pm 1\}$:

$$\sigma \mapsto (\sigma(\sqrt{2})/\sqrt{2}, \sigma(\sqrt{3})/\sqrt{3}),$$

est un isomorphisme de groupes.

(v) Soit $L \subset K$ un sous-corps strict. Montrer que $\mathrm{Aut}_L(K)$ est un sous-groupe à deux éléments de G. (On pourra d'abord montrer que $K = L[x]$ pour $x \in \{\sqrt{2}, \sqrt{3}, \sqrt{6}\}$ bien choisi.)

(vi) En déduire que L est l'un des trois corps trouvés au (i).

(vii) Soit $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, $a, b, c, d \in \mathbf{Q}$. Montrer que $\mathbf{Q}[x] = K$ si, et seulement si, deux au moins des nombres b, c et d sont non nuls (de tels x, sont appelés *éléments primitifs de K sur $\mathbf{Q}$*).

(viii) Vérifier que l'application qui à un sous-groupe H de $G = \mathrm{Aut}_{\mathbf{Q}}(K)$ associe le sous-corps K^H de K induit une bijection entre sous-groupes de G et sous-corps de K.

[1] C'est à dire différents de $\mathbf{Q}$ et de K.