École Polytechnique 2009-2010

Théorie de Galois

Feuille d'exercices 4

Exercice 1. Soient $K = \mathbf{Q}[\sqrt{2}, \sqrt{3}] \subset \mathbf{C}$.

(i) Montrer que $[K : \mathbf{Q}] = 4$.

(ii) Soit $x = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, $a, b, c, d \in \mathbf{Q}$. Montrer que x est un élément primitif de K si, et seulement si, deux au moins des nombres b, c et d sont non nuls.

(iii) Décrire tous les sous-corps de K.

Notations : Si $k \subset K$ est 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. Si $H \subset \mathrm{Aut}_k(K)$ est 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 2. Soient $x = \sqrt[3]{2}, j = e^{2i\pi/3}$, $K = \mathbf{Q}(x, j) \subset \mathbf{C}$ et $G = \mathrm{Aut}_{\mathbf{Q}}(K)$.

(i) Montrer que $[K : \mathbf{Q}] = 6$ et donner 4 sous-corps stricts de K.

(ii) Montrer que $|G| \leq 6$.

(iii) Déterminer $\mathrm{Aut}_L(K)$ pour $L = \mathbf{Q}(j)$ et $L = \mathbf{Q}(x)$. Vérifier que ce sont des sous-groupes de G.

(iv) En déduire que $G \simeq \mathfrak{S}_3$. On pourra considérer l'ensemble R des racines de $X^3 - 2$ dans K et montrer que pour tout $\sigma \in G$ on a $\sigma(R) = R$, de sorte que $\sigma \mapsto \sigma_{|R}$ induit un morphisme de groupes

$$G \longrightarrow \mathfrak{S}(R) \simeq \mathfrak{S}_3.$$

(v) Soit $L \subsetneq K$ un sous-corps. Montrer qu'il existe $\sigma \in G \backslash \{\mathrm{id}\}$ tel que $\sigma(x) = x$ pour tout x dans L.

(vi) Décrire tous les sous-corps de K ainsi que tous les éléments primitifs.

(vii) 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.

Remarquer qu'il existe un unique sous-corps strict $L \subset K$ tel que $\sigma(L) = L$ pour tout $\sigma \in G$, et qu'il correspond à l'unique sous-groupe distingué de G (voir l'exercice suivant pour la définition).

Exercice 3. Soient k un corps et $\overline{k}$ une clôture algébrique de k. Si $x \in \overline{k}$, on rappelle que les conjugués de x sur k dans $\overline{k}$ sont les racines dans $\overline{k}$ du polynôme minimal de x sur k. On note $\mathrm{conj}_k(x) \subset \overline{k}$ l'ensemble des conjugués de x.

(i) (rappel de cours) Montrer que

$$\mathrm{conj}_k(x) = \{\sigma(x), \sigma \in \mathrm{Aut}_k(\overline{k})\} = \{\sigma(x), \sigma \in \mathrm{Hom}_k(K, \overline{k})\},$$

où $k \subset K \subset \overline{k}$ est n'importe quelle extension contenant x.

(ii) Montrer que si $x, y \in \overline{k}$, alors

$$\mathrm{conj}_k(x+y) \subset \{a+b, a \in \mathrm{conj}_k(x), b \in \mathrm{conj}_k(y)\}.$$

Donner un exemple où cette inclusion est stricte.

(iii) Donner un exemple où $\mathrm{conj}_k(x)$ n'est pas inclus dans $k[x]$.

(iv) Supposons k parfait et $x \in \overline{k}$. Montrer que les propriétés suivantes sont équivalentes:

- $x \in k$,

- $\mathrm{conj}_k(x) = \{x\}$,

- $\forall \sigma \in \mathrm{Aut}_k(\overline{k})$, $\sigma(x) = x$.

Exercice 4. (Rappel sur les groupes quotients) Soit $H \subset G$ un sous-groupe. Si $g \in G$, on note

$$gH = \{gh, h \in H\} \subset G$$

le translaté de H à gauche par g et on désigne par $G/H \subset \mathcal{P}(G)$ l'ensemble des gH, $g \in G$. On a une définition analogue pour Hg, et plus généralement si X et Y sont des parties de G, on pose $XY = \{xy, x \in X, y \in Y\} \subset G$. On rappelle que H est dit *distingué* (ou *normal*) dans G si $gH = Hg$ pour tout g dans G, on note $H \lhd G$.

(i) Montrer que $H \lhd G$ si, et seulement si, $\forall g, g' \in H$, $(gH)(g'H) = gg'H$.

(ii) En déduire que si $H \lhd G$, la loi de composition sur G/H définie par $(gH, g'H) \mapsto gg'H$ est une loi de groupe de neutre H. De plus, l'application $\pi : G \to G/H$, $g \mapsto gH$, est un morphisme de groupes, surjectif et de noyau H.

(iii) Supposons $H \lhd G$. Montrer que l'application qui à un sous-groupe $X \subset G/H$ associe le sous-groupe $\pi^{-1}(X) \subset G$ est une bijection de l'ensemble des sous-groupes de G/H dans ceux de G contenant H. Si G est fini, vérifier que $|\pi^{-1}(X)| = |X||H|$.

(iv) Donner un exemple de groupe G ayant un sous-groupe distingué H tel que G n'est pas isomorphe au groupe produit $H \times (G/H)$.

Exercice 5. Soient $p_1, \ldots, p_r$ des éléments de $\mathbf{Q}^*$ et

$$K = \mathbf{Q}[\sqrt{p_1}, \sqrt{p_2}, \cdots, \sqrt{p_r}].$$

(i) Montrer que la structure de groupe abélien sur le quotient $\mathbf{Q}^*/(\mathbf{Q}^*)^2$ s'étend naturellement en une structure de $\mathbf{Z}/2\mathbf{Z}$-espace vectoriel. Vérifier que la famille $\overline{-1}$, $\overline{p}$, où p parcourt les nombres premiers, en est une base.

(ii) On suppose que les images de $p_1, \ldots, p_r$ dans le $\mathbf{Z}/2\mathbf{Z}$-espace vectoriel $\mathbf{Q}^*/(\mathbf{Q}^*)^2$ sont linéairement indépendantes. Démontrer que $[K : \mathbf{Q}] = 2^r$ (on pourra raisonner par récurrence sur r).

(iii) Montrer que ceci s'applique au cas où $p_1, \ldots, p_r$ sont des nombres premiers distincts.

(iv) En déduire que $\sqrt{2} + \sqrt{3} + \sqrt{4} + \cdots + \sqrt{n}$ n'est jamais entier pour n entier ≥ 2.

Exercice 6. (plus difficile) Montrer que $\mathrm{Aut}_{\mathbf{Q}}(\overline{\mathbf{Q}})$ est en bijection avec $\mathbf{R}$ (en particulier, il n'est pas dénombrable).