Théorie de Galois L3, 2018-2019 Durée : 3h00 B. Calmès

Correction de l'examen de première session

Exercice 1. Le problème suivant était un des grands problèmes de l'antiquité : peut-on "dupliquer le cube" à la règle et au compas, c'est-à-dire, étant donné un segment représentant le côté d'un cube, peut-on construire à la règle et au compas celui d'un cube de volume double.
Ramener cette question à une question de constructibilité au sens du cours, et la résoudre par la négative.

Solution. Quitte à changer l'unité de mesure, on peut supposer le cube de côté 1 et donc de volume 1. Un cube de volume double a alors pour côté $\sqrt[3]{2}$. La question est donc de savoir si $\sqrt[3]{2}$ est constructible. Mais $\mathbb{Q}[\sqrt[3]{2} : \mathbb{Q}] = 3$ puisque le polynôme minimal de $\sqrt[3]{2}$ est $X^3 - 2$ (évidemment irréductible sur $\mathbb{Q}$, sa seule racine réelle étant irrationnelle). Si $\sqrt[3]{2}$ était constructible, il serait inclus dans une extension L de degré 2^n pour un $n \in \mathbb{N}$; c'est impossible, par multiplicativité des degrés, on aurait $3|2^n$.

Exercice 2. Soit $\xi = \sqrt{13 + 2\sqrt{13}}$ et $L = \mathbb{Q}[\xi] \subset \mathbb{R}$.

(1) Montrer que l'extension $L/\mathbb{Q}$ est une extension de corps algébrique finie.

(2) Déterminer le polynôme minimal P de ξ sur $\mathbb{Q}$.

(3) Déterminer le degré de L.

(4) Trouver toutes les racines de P (exprimées à l'aide de racines carrées réelles, comme l'est ξ ci-dessus).

(5) Montrer que $\mathbb{Q}[\sqrt{13}]$ est inclus dans L.

(6) Montrer que L est un corps de décomposition de P (indication : penser au produit par la quantité conjuguée).

(7) Montrer que $L/\mathbb{Q}$ est normale.

(8) Quel est le cardinal de $\mathrm{Gal}(L/\mathbb{Q})$? Quels sont donc a priori les deux seuls groupes possibles pour ce groupe de Galois (à isomorphisme près, bien sûr).

(9) Notons $\bar{\xi} = \sqrt{13 - 2\sqrt{13}}$. Justifier qu'il existe un unique élément σ du groupe de $\mathrm{Gal}(L/\mathbb{Q})$ tel que $\sigma(\xi) = \bar{\xi}$.

(10) Déterminer $\sigma(\sqrt{13})$ puis l'image par σ des autres racines de P.

(11) Quel est l'ordre de σ ?

(12) Parmi les deux possibilités de la question (8), laquelle est la bonne ?

(13) Déterminer toutes les sous-extensions de $L/\mathbb{Q}$.

Solution. (1) On a $\xi^2 - 13 = 2\sqrt{13}$, donc $(\xi^2 - 13)^3 - 4 \times 13 = 0$. Le polynôme $(X^2-13)^2-52 = X^4-26X^2+9\times 13$ annule donc ξ, qui est donc algébrique. Le sous-anneau $\mathbb{Q}[\xi]$ de $\mathbb{R}$ est donc isomorphe à $\mathbb{Q}[X]/(P)$ où P est le polynôme minimal de ξ. C'est donc une extension finie de corps (cours : I.2.21).

(2) Le polynôme $P = X^4 - 26X^2 + 117$ annule ξ, et il est irréductible sur $\mathbb{Q}$ par le critère d'Eisenstein pour le nombre premier 13. C'est donc le polynôme minimal de ξ.

(3) Puisque $L \simeq \mathbb{Q}[X]/(P)$, on a donc $[L : \mathbb{Q}] = 4$.

(4) En factorisant $P = (X^2 - 13)^2 - 4 \times 13$, on voit immédiatement que les racines de P sont $\pm\sqrt{13 \pm 2\sqrt{13}}$ (les quatres signes possibles). Si l'on note $\bar{\xi} = \sqrt{13 - 2\sqrt{13}}$, ces racines sont donc $\pm\xi$ et $\pm\bar{\xi}$.

(5) On a $\xi^2 = 13 + 2\sqrt{13}$, donc $\sqrt{13} \in \mathbb{Q}[\xi] = L$, donc $\mathbb{Q}[\sqrt{13}] \subset L$.

(6) On a bien entendu $-\xi \in \mathbb{Q}[\xi]$. De plus $\xi\bar{\xi} = 3\sqrt{13}$ donc $\bar{\xi} = 3\sqrt{13}/\xi \in \mathbb{Q}[\sqrt{13}, \xi] = \mathbb{Q}[\xi]$ par la question précédente. On a donc également $-\bar{\xi} \in \mathbb{Q}[\xi]$. Finalement, $L = \mathbb{Q}[\xi]$ contient toutes les racines de P et est minimale pour cette propriété (puisqu'une telle extension doit contenir au moins contenir ξ). C'est donc un corps de décomposition de P.

(7) L'extension $L/\mathbb{Q}$ est normale puisque c'est une extension de décomposition (cours : I.6.2).

(8) Puisque $L/\mathbb{Q}$ est une extension normale en caractéristique 0, on a $\#\mathrm{Gal}(L/\mathbb{Q}) = [L : \mathbb{Q}] = 4$. Il est donc isomorphe à $\mathbb{Z}/4$ ou à $\mathbb{Z}/2 \times \mathbb{Z}/2$ qui sont les deux seuls groupes de cardinal 4 (à isomorphisme près).

(9) Puisque $L \simeq \mathbb{Q}[X]/(P)$ (en envoyant ξ sur X), étant donné une racine de P (en l'occurrence $\bar{\xi}$), il existe un unique élément de $\mathrm{Gal}(L/\mathbb{Q})$ qui envoie ξ sur cette racine (cours : II.2.4).

(10) On a $\sigma(\xi) = \bar{\xi}$, donc $\sigma(\xi^2) = \bar{\xi}^2$, donc $\sigma(13 + 2\sqrt{13}) = 13 - 2\sqrt{13}$, ou encore $13+2\sigma(\sqrt{13} = 13-2\sigma(\sqrt{13})$ donc $\sigma(\sqrt{13}) = -\sqrt{13}$. Alors $\sigma(\xi)\sigma(\bar{\xi}) = \sigma(\xi\bar{\xi}) = \sigma(3\sqrt{13}) = -3\sqrt{13}$, donc $\sigma(\bar{\xi}) = -\sqrt{13 + 2\sqrt{13}} = -\xi$. Bien évidemment, on a $\sigma(-\xi) = -\sigma(\xi) = -\bar{\xi}$ et $\sigma(-\bar{\xi}) = -\sigma(\bar{\xi}) = \xi$.

(11) On a $\sigma(\xi) = \bar{\xi}$, donc $\sigma^2(\xi) = \sigma(\bar{\xi}) = -\xi$, donc $\sigma^3(\xi) = \sigma(-\xi) = -\bar{\xi}$, et $\sigma^4 = \mathrm{id}$ (car dans un groupe d'ordre 4). L'élément σ est donc d'ordre 4.

(12) $\mathbb{Z}/2 \times \mathbb{Z}/2$ ne contient pas d'élément d'ordre 4, donc la seule possibilité est $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/4$.

(13) Le seul sous-groupe non-trivial de $\mathbb{Z}/4 \simeq \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$ est $\{1, \sigma^2\} \simeq \mathbb{Z}/2$. La correspondance de Galois nous dit donc que, hormis L et $\mathbb{Q}$, il n'y a qu'un seul sous-corps F de L (contenant $\mathbb{Q}$, mais c'est automatique). Il vérifie $[L : F] = \#\mathbb{Z}/2 = 2$ et nous l'avons déjà trouvé, c'est $F = \mathbb{Q}[\sqrt{13}]$.

Exercice 3. Soit K un corps de caractéristique 0. Soit E/K une extension de corps normale finie de groupe de Galois G. Étant donné un élément a de E, on note $G_a = \{g \in G \text{ t.q. } g(a) = a\}$.

(1) Montrer que G_a est un sous-groupe de G.

(2) Montrer que par la correspondance de Galois, G_a correspond à $K[a]$.

(3) Montrer que $K[a] = E$ si et seulement si $G_a = \{\mathrm{id}\}$.

(4) Soit b un élément de E tel que $G_a \subset G_b$. Démonter qu'il existe un polynôme $P \in K[X]$ tel que $P(a) = b$.

(5) Montrer que pour tout sous-groupe H de G, il existe un élément $a \in E$ tel que $H = G_a$.

Solution. (1) C'est évident : l'élément neutre de $\mathrm{id} \in G$ vérifie $\mathrm{id}(a) = a$. Si $g \in G_a$ et $h \in G_a$, alors $g(a) = a$ et $h(a) = a$, donc $gh(a) = g(a) = a$ et $gh \in G_A$. Si $g(a) = a$, alors $a = g^{-1}g(a) = g^{-1}(a)$, donc $g \in G_a$ implique $g^{-1} \in G_a$.

(2) Par la correspondance de Galois, $K[a]$ correspond à

$$\mathrm{Gal}(E/K[a]) = \{g \in G \text{ t.q. } g_{|K[a]} = \mathrm{id}\}.$$

Or $g_{|K[a]} = \mathrm{id}$ si et seulement si $g(a) = a$, puisque tout élément de $K[a]$ s'exprime comme un polynôme en a à coefficients dans K. Donc $\mathrm{Gal}(E/K[a]) = G_a$ (au passage, on a $E^{G_a} = K[a]$).

(3) Toujours par la correspondance de Galois, on a $K[a] = E$ si et seulement si $G_a = \mathrm{Gal}(E/E) = \{\mathrm{id}\}$.

(4) La correspondance de Galois étant décroissante, on a $G_a \subset G_b$ si et seulement si $K[b] \subset K[a]$. Or $b \in K[b]$, donc $b \in K[a]$ et $b = P(a)$ pour un polynôme $P \in K[X]$.

(5) Par la correspondance de Galois, H correspond à une sous-extension F/K de E/K. Par le théorème de l'élément primitif, il existe $a \in F$ tel que $F = K[a]$. Par la question (2), on a donc $H = G_a$.