Théorie de Galois

Contrôle du 11 avril 2022. Durée 1h00.

Pas de documents autorisés.

Exercice 1. Soit $f := X^5 - 3 \in \mathbb{Q}[X]$. On note $K_f \subset \overline{\mathbb{Q}}$ son corps de décomposition et G_f son groupe de Galois.

i. Montrer que $\mathbb{Q}(\sqrt[5]{3}) \subset K_f$ et $\mathbb{Q}(\mu_5) \subset K_f$.

   Par définition, K_f est engendré par les racines de f qui sont les $\zeta\sqrt[5]{3}$, où ζ parcourt μ_5. On a donc $\sqrt[5]{3} \in K_f$ et $\mu_5 \subset K_f$.

ii. Montrer que $[K_f : \mathbb{Q}] = 20$, et en déduire que f reste irréductible dans $\mathbb{Q}(\mu_5)$ et que Φ_5 est irréductible dans $\mathbb{Q}(\sqrt[5]{3})(X)$.

   On a $4 = [\mathbb{Q}(\mu_5) : \mathbb{Q}] | [K_f : \mathbb{Q}]$ et $5 = [\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] | [K_f : \mathbb{Q}]$, donc $20 | [K_f : \mathbb{Q}]$. Par ailleurs, on a $[K_f : \mathbb{Q}(\mu_5)] \leqslant 5$ puisque $K_f = \mathbb{Q}(\mu_5)(\sqrt[5]{3})$ et le polynôme minimal de $\sqrt[5]{3}$ dans $\mathbb{Q}(\mu_5)[X]$ divise f. Par l'égalité $[K_f : \mathbb{Q}] = [K_f : \mathbb{Q}(\mu_5)][\mathbb{Q}(\mu_5) : \mathbb{Q}]$, on en déduit que $[K_f : \mathbb{Q}] \leqslant 20$. En mettant ensemble les deux inégalités obtenues, on obtient $[K_f : \mathbb{Q}] = 20$. On en déduit aussi que $[K_f : \mathbb{Q}(\mu_5)] = 5$, donc que f est encore le polynôme minimal de $\sqrt[5]{3}$ sur $\mathbb{Q}(\mu_5)$, et en particulier f reste irréductible dans $\mathbb{Q}(\mu_5)[X]$. De même, à l'aide de l'égalité $[K_f : \mathbb{Q}] = [K_f : \mathbb{Q}(\sqrt[5]{3})][\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}]$ on voit que le polynôme minimal $\Phi_5 = 1 + X + X^2 + X^3 + X^4$ d'une racine primitive 5-ème de 1 sur $\mathbb{Q}$ reste irréductible sur $\mathbb{Q}(\sqrt[5]{3})$.

iii. Montrer que G_f est le produit semi-direct de son sous-groupe distingué $G_1 := \mathrm{Gal}(K_f/\mathbb{Q}(\mu_5))$ par son sous-groupe $G_2 := \mathrm{Gal}(K_f/\mathbb{Q}(\sqrt[5]{3}))$.

   On sait que l'extension $\mathbb{Q}(\mu_5)/\mathbb{Q}$ est Galoisienne, donc le sous-groupe G_1 de G_f est bien distingué, et le sous-ensemble $G_1G_2 := \{h \in G, \exists g_1 \in G_1, g_2 \in G_2, h = g_1g_2\}$ de G est un sous-groupe. De plus, les éléments de l'intersection $G_1 \cap G_2$ fixent $\sqrt[5]{3}$ et μ_5 qui engendrent K_f, donc cette intersection est $\{\mathrm{id}\}$, et G_1G_2 est un produit semi-direct de G_1 par G_2. On a alors $|G_1G_2| = |G_1||G_2| = 4 \times 5 = |G|$, donc $G_1G_2 = G$.

iv. Construire explicitement un isomorphisme de groupes $G_f \xrightarrow{\sim} \mu_5 \rtimes (\mathbb{Z}/5\mathbb{Z})^\times$.

   Cf cours et TD. On envoie σ sur (ζ_σ, a_σ) où $\zeta_\sigma = \frac{\sigma(\sqrt[5]{3})}{\sqrt[5]{3}}$ et a_σ est tel que $\sigma(\zeta) = \zeta^{a_\sigma}$ pour tout $\zeta \in \mu_5$.

v. Trouver un élément primitif de K_f.

On doit trouver un élément de degré $[K_f : \mathbb{Q}]$, i.e. dont l'orbite sous G_f est de cardinal $|G_f|$, i.e. dont le stabilisateur dans G_f est trivial. Regardons par exemple $\alpha := \sqrt[5]{3}+\zeta$ pour $\zeta \in \mu_5 \setminus \{1\}$. On a $\sigma(\alpha) = \zeta_\sigma \sqrt[5]{3} + \zeta^{a_\sigma}$. Donc $\alpha = \sigma(\alpha) \Leftrightarrow (1-\zeta_\sigma)\sqrt[5]{3} = \zeta^{a_\sigma} - \zeta$. Puisque $\sqrt[5]{3} \notin \mathbb{Q}(\mu_5)$, on en déduit que $\alpha = \sigma(\alpha) \Leftrightarrow (\zeta_\sigma = 1 \text{ et } \zeta^{a_\sigma} = \zeta)$ et donc $\alpha = \sigma(\alpha) \Leftrightarrow \sigma = \mathrm{id}$.

vi. Montrer qu'il n'y a pas de corps strictement compris entre $\mathbb{Q}(\mu_5)$ et K_f.

L'extension $K_f \supset \mathbb{Q}(\mu_5)$ est de degré 5. Toute extension intermédiaire a donc degré 1 ou 5, donc est égale à $\mathbb{Q}(\mu_5)$ ou à K_f.

vii. Montrer qu'il y a un unique corps strictement compris entre $\mathbb{Q}(\sqrt[5]{3})$ et K_f. Le décrire (donner des générateurs).

Puisque $K_f = \mathbb{Q}(\sqrt[5]{3})(\mu_5)$ et Φ_5 est irréductible dans $\mathbb{Q}(\sqrt[5]{3})[X]$, on sait que le caractère cyclotomique $\mathrm{Gal}(K_f/\mathbb{Q}(\sqrt[5]{3})) \longrightarrow \mathrm{Aut}(\mu_5) \simeq \mathbb{Z}/4\mathbb{Z}$ est un isomorphisme. Le groupe $\mathbb{Z}/4\mathbb{Z}$ contient un unique sous-groupe propre et non-trivial, à savoir $H = 2\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z}$. Par la correspondance de Galois, il existe donc un unique corps strictement compris entre $\mathbb{Q}(\sqrt[5]{3})$ et K_f, à savoir $(K_f)^H$. Pour le calculer explicitement, on peut remarquer que H est le groupe engendré par la conjugaison complexe (qui est bien un élément d'ordre 2 de $\mathrm{Gal}(K_f/\mathbb{Q}(\sqrt[5]{3}))$ et qui est le seul élément d'ordre 2 de ce groupe). En particulier $(K_f)^H$ contient $\cos(2\pi/5)$, qui est un élément de degré 2 sur $\mathbb{Q}$, donc non contenu dans $\mathbb{Q}(\sqrt[5]{3})$ (qui est de degré 5). On en déduit que $(K_f)^H = \mathbb{Q}(\sqrt[5]{3}, \cos(2\pi/5))$.