Groupe de Galois

Samuel Rochetin

Jeudi 1er juin 2017

Problème. *On considère le polynôme suivant :* $P(X) = X^4 + 1$.

1. *Démontrer que* P *est irréductible dans* $\mathbb{Q}[X]$.
2. *Démontrer que les racines de* P *sont de la forme* $\{\alpha, \alpha^3, \alpha^5, \alpha^7\}$*, où* α *est un nombre complexe bien choisi.*
3. *En déduire que l'extension de corps* $\mathbb{Q} \to \mathbb{Q}(\alpha)$ *est finie, normale et séparable, et donner* $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ *et* $|Gal(\mathbb{Q}(\alpha) : \mathbb{Q})|$.
4. *Démontrer que tout* $\sigma \in Gal(\mathbb{Q}(\alpha) : \mathbb{Q})$ *est déterminé par l'image* $\sigma(\alpha)$ *de* α.
5. *Indiquer les valeurs prises par les* $\sigma(\alpha)$ *et décrire les automorphismes du corps* $\mathbb{Q}(\alpha)$.
6. *Démontrer que* $Gal(\mathbb{Q}(\alpha) : \mathbb{Q})$ *est isomorphe à* $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$.

Corrigé.

1. Le critère d'Eisenstein appliqué à $P(X+1) = X^4+4X^3+6X^2+4X+2$ montre que P est irréductible dans $\mathbb{Q}[X]$.
2. Les racines de P sont $\exp\left(\frac{i\pi}{4}\right), \exp\left(\frac{3i\pi}{4}\right), \exp\left(\frac{5i\pi}{4}\right), \exp\left(\frac{7i\pi}{4}\right)$ donc en posant $\alpha := \exp\left(\frac{i\pi}{4}\right)$, les racines de P sont de la forme $\{\alpha, \alpha^3, \alpha^5, \alpha^7\}$.
3. $\mathbb{Q} \to \mathbb{Q}(\alpha)$ est normale comme corps de décomposition de P, finie, de degré $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = \deg P$, et séparable car de caractéristique nulle. Le groupe de Galois est d'ordre 4.
4. Soit $\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\alpha) : \mathbb{Q})$. Pour tout $k \in \mathbb{Z}, \sigma\left(\alpha^k\right) = \sigma(\alpha)^k$, donc σ est déterminé par $\sigma(\alpha)$.
5. $\sigma(\alpha)$ peut prendre pour valeurs $\alpha, \alpha^3, \alpha^5, \alpha^7$. Un automorphisme σ_k du corps $\mathbb{Q}(\alpha)$, où $k = 1, 3, 5$ ou 7, est déterminé par $\sigma_k(\alpha) = \alpha^k$.
6. Un groupe d'ordre 4 est isomorphe à $(\mathbb{Z}/4\mathbb{Z}, +)$ s'il existe un élément d'ordre 4 ou à $(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}, +)$ sinon. Or, $\sigma_3(\alpha)^2 = \sigma_3 \circ \sigma_3(\alpha) = \sigma_3\left(\alpha^3\right) = \left(\alpha^3\right)^3 = \alpha$ donc $\sigma_3^2 = Id$, de même pour σ_5 et σ_7. Donc les automorphismes sont d'ordre 2, donc $\mathrm{Gal}\,(\mathbb{Q}(\alpha) : \mathbb{Q})$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$.

□