Algèbre et théorie de Galois - TD7

Exercice 1 : (Entiers quadratiques) Si $K/\mathbb{Q}$ est une extension finie, on note O_K son anneau d'entiers.

a) Montrer que toute extension quadratique $K/\mathbb{Q}$ peut s'écrire $K = \mathbb{Q}(\sqrt{d})$ avec $d \neq 0, 1$ et d sans facteur carré.

b) Soit $K = \mathbb{Q}(\sqrt{d})$. Montrer que

i) $O_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ si $d \cong 4 \mod 4$,

ii) $O_K = \mathbb{Z}[\sqrt{d}]$ sinon.

c) Quels sont les morphismes de K dans $\mathbb{C}$? En déduire l'expression de la norme et la trace de $z = x + y\sqrt{d} \in K$. Montrer que $z \in O_K$ si et seulement si sa norme et sa trace sont dans O.

d) Déterminer le groupe des inversibles $O_K^\times$ de O_K (appelé groupe des unités) lorsque d est négatif.

e) Monter que le groupe des unités de $\mathbb{Z}[\sqrt{2}]$ est infini (c'est ce qui rend les corps quadratiques réels plus difficiles à étudier).

f) Trouver tous les rationnels x tels que $\cos(2\pi x)$ soit rationnel.

Exercice 2 : Déterminer si les éléments suivants $x \in \mathbb{C}$ sont des entiers algébriques dans leur corps de définition $\mathbb{Q}(x)$:

a) $\frac{\sqrt{3}+\sqrt{5}}{2}$,

b) $\frac{\sqrt{3}+\sqrt{7}}{2}$,

c) $\frac{\sqrt{5}+\sqrt{7}}{2}$,

d) $\frac{1+i\sqrt{3}+i\sqrt{7}-\sqrt{21}}{4}$.

Exercice 3 : (Racines quinzièmes de l'unité) On pose $\zeta = e^{\frac{2i\pi}{15}}$, $\eta = e^{\frac{2i\pi}{5}}$, $j = e^{\frac{2i\pi}{3}}$. On rappelle que $\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{2}$.

a) Quel est le degré de $\mathbb{Q}(\zeta)/\mathbb{Q}$? Calculer son polynôme minimal et donner la décomposition en facteurs irréductibles dans $\mathbb{Q}[X]$ de $X^15 - 1$. On note $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ et on note σ_k l'élément du groupe G tel que $\sigma_k(\zeta) = \zeta^k$.

b) Quelles sont les valeurs possibles pour k ?

c) Décrire G et calculer les ordres de ses éléments.

d) Montrer que $\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\eta)$ et que $\mathbb{Q}(\zeta)$ est une extension de degré 2 de $\mathbb{Q}(\cos\frac{2\pi}{15})$.

e) Montrer que les extensions $\mathbb{Q}(j)$, $\mathbb{Q}(\eta)$, $\mathbb{Q}(\sqrt{5})$ et $\mathbb{Q}(j, \sqrt{5})$ sont contenues dans $\mathbb{Q}(\zeta)$ et déterminer le sous-groupe de G qui les fixe.

f) Déterminer les corps des invariants de $\langle\sigma_{14}\rangle$ et $\langle\sigma_2\rangle$.

g) Donner explicitement la correspondance de Galois entre les deux treillis de la situation.

h) Calculer une expression algébrique de $\cos\frac{2\pi}{15}$ en utilisant le groupe

$$\mathrm{Gal}(\mathbb{Q}(\cos\frac{2\pi}{15})/\mathbb{Q}(\sqrt{5})).$$

i) Dire si le polygone régulier à 15 cotés de rayon 1 est constructible à la règle et au compas.

Exercice 4 : (Groupes de Galois cyclotomiques) Soient n un entier naturel $f_n(X) = X^n - 1$. On note $L/\mathbb{Q}$ le corps de décomposition de f_n.

a) Calculer le groupe de Galois G de $L/\mathbb{Q}$.

b) Montrer que si $H \subset G$ est un sous-groupe, on a un morphisme naturel $H(p) \to G(p)$ entre les composantes p-primaires (éléments annulés par une puissance de p) pour tout p premier.

c) En déduire une méthode pour simplifier la classification des sous-groupes de G.

d) Classifier les idéaux de l'anneau $\mathbb{Z}/p^k\mathbb{Z}$ et en déduire une suite naturel de quotients de $(\mathbb{Z}/p^k\mathbb{Z})^\times$.

e) Pour p premier et k naturel, montrer les congruences

$$(1+p)^{p^k} \equiv 1 + p^{k+1} \mod (p^{k+2})$$

et

$$5^{2^k} \equiv 1 + 2^{k+2} \mod (2^{k+3}).$$

f) Montrer qu'on a une suite exacte

$$0 \to 1 + (p) \to (\mathbb{Z}/p^k\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \to 1$$

si p est premier impair avec $1 + (p) \cong \mathbb{Z}/p^{k-1}\mathbb{Z}$ et que si $k > 2$, on a une suite exacte

$$1 \to 1 + (4) \to (\mathbb{Z}/2^k\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times \to 0$$

avec $1 + (4) \cong \mathbb{Z}/2^{k-1}\mathbb{Z}$.

g) En déduire une description explicite du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ et des sous-groupes de $(\mathbb{Z}/p^k\mathbb{Z})^\times$.

h) Déterminer tous les sous-groupes de G pour $n = 3^2.7$.

i) Même question pour $n = 3^2.5^2$.