**Université Paris 7** **25 novembre 2016**
**Algèbre**

# TD8 : correspondance de Galois

**Exercice 1 :**

Donner un élément primitif du sous corps de $L = \mathbb{Q}(\sqrt[4]{2}, i)$ fixé par le sous-groupe $\langle \sigma\tau \rangle$, avec les notations du cours.

**Exercice 2 :**

Soit $L$ le corps de décomposition de $x^4 + 1$ sur $\mathbb{Q}$.

**1.** Montrer que $i \in L$ et que $\sqrt{2} \in L$ (on pourra calculer $(\alpha + \alpha^{-1})^2$).

**2.** En déduire que $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, et donner le diagramme des sous-extensions. On rappelle que les groupes d'ordre 4 sont $\mathbb{Z}/4\mathbb{Z}$ et $(\mathbb{Z}/2\mathbb{Z})^2$.

**Exercice 3 :**

Soit $P(x) = x^4 - x^2 - 1$, et $L$ son corps de décomposition sur $\mathbb{Q}$.

**1.** Montrer que $P$ est irréductible sur $\mathbb{Q}$.

**2.** On pose $\phi = \frac{1+\sqrt{5}}{2}$. Quel est son polynôme minimal ? Déterminer $\frac{1}{\phi}$ sur la base canonique de $\mathbb{Q}(\phi)$.

**3.** Exprimer toutes les racines de $P$ en fonction d'une racine $\alpha$.

**4.** Calculer $[L : \mathbb{Q}]$.

**5.** Expliciter les éléments de $G = \mathrm{Gal}(L/\mathbb{Q})$, et en donner des générateurs.

**6.** Quels sont les sous-corps quadratiques de $L$ ?

**7.** Identifier $\mathrm{Gal}(L/\mathbb{Q}(\alpha + i/\alpha))$.

**8.** Calculer $\alpha + i/\alpha$.

**9.** Compléter le diagramme des sous-extensions de $L$.

**10.** Déterminer un élément primitif de $L$ sur $\mathbb{Q}$.

**Exercice 4 :**

Soit $L/K$ une extension galoisienne et $F, F'$ deux corps intermédiaires correspondant aux groupes $H$ et $H'$.

**1.** On note $FF'$ le plus petit corps contenant $F$ et $F'$. Montrer que $\mathrm{Gal}(L/FF') = H \cap H'$.

**2.** On note $\langle H, H' \rangle$ le sous-groupe engendré par $H$ et $H'$. Montrer que $\mathrm{Gal}(L/F \cap F') = \langle H, H' \rangle$.

**3.** Montrer que $F \subset F'$ si et seulement si $H' \subset H$ et que dans ce cas $[F' : F] = [H : H']$.

**Exercice 5 :**

Soient $x_1, \dots x_n$ des indéterminées. Montrer que $x_1 x_2^2 x_3^3 \dots x_n^n$ est un élément primitif de $\mathbb{Q}(x_1, \dots x_n)$ sur $\mathbb{Q}(\sigma_1, \dots \sigma_n)$.

## 1 Corps cyclotomiques

**Exercice 6 :**

Quels sont les corps cyclotomiques de degré $d \leqslant 10$ ?

**Exercice 7 :**

1. Soit $p$ premier, et $e \geqslant 1$. Montrer que $\Phi_{p^e}(x) = \Phi_p(x^{p^{e-1}})$.
2. Montrer que si $p$ premier ne divise pas $n$, alors $\Phi_n(x^p) = \Phi_{pn}(x)\Phi_n(x)$.
3. Calculer $\Phi_{24}(x)$.

**Exercice 8 :**

Déterminer le diagramme des sous-extensions de $\mathbb{Q}(\zeta_9)$.

**Exercice 9 :**

Soit $p$ un nombre premier impair, on pose $S = \left\{a^2, a \in \mathbb{F}_p^*\right\}$ et $N = \mathbb{F}_p^* \setminus S$.

1. Montrer que $\phi : x \mapsto x^{\frac{p-1}{2}} \bmod p$ permet d'écrire une suite exacte

$$1 \to S \to \mathbb{F}_p^* \to \{\pm 1\} \to 1.$$

On prolonge $\phi$ en une application multiplicative $\mathbb{F}_p \to \{-1, 0, 1\}$ en posant $\phi(0) = 0$.

2. Soit $\zeta_p = e^{\frac{2i\pi}{p}}$. Montrer que l'application $a \mapsto \zeta^a$ est bien définie de $\mathbb{F}_p \to \mathbb{C}$. Que vaut $\sum_{a\in\mathbb{F}_p} \zeta^a$ ?
3. On pose $\beta = \sum_{a\in S} \zeta^a - \sum_{b\in N} \zeta^b$. Vérifier que

$$\beta = \sum_{a\in\mathbb{F}_p} \phi(a)\zeta^a.$$

4. Montrer que

$$\beta^2 = \sum_{a=0}^{p-1}\sum_{c=0}^{p-1} \phi(ac - a^2)\zeta^c$$

5. Montrer que si $a \neq 0$, $c \mapsto ac - a^2$ est une bijection de $\mathbb{F}_p$.
6. En déduire que $\beta^2 = p\phi(-1)$.
7. En déduire que $\beta = \pm\sqrt{p}$ si $p \equiv 1 \bmod 4$, et $\beta = \pm i\sqrt{p}$ si $p \equiv 3 \bmod 4$.
8. Montrer que toute extension quadratique de $\mathbb{Q}$ est incluse dans une extension cyclotomique.

## 2 Corps finis

**Exercice 10 :**

Déterminer le diagramme des sous-extensions de $\mathbb{F}_{2^{30}}$.

**Exercice 11 :**

Soit $p$ premier et $n$ un entier premier à $p$.

1. Montrer que $\Phi_n$ est scindé dans $\mathbb{F}_{p^k}$ si et seulement si $n \mid p^k - 1$.
2. Montrer que sur $\mathbb{F}_p$, $\Phi_n$ est produit de $\varphi(n)/r$ facteurs irréductibles de degré $r$, où $r$ est l'ordre de $p$ modulo $n$.
3. Montrer que $\Phi_{11}$ est irréductible sur $\mathbb{F}_2$.
4. Comment se factorise-t-il sur $\mathbb{F}_3$ ?