TD n°9.

Exercice 1. Soit K un corps et Ω une extension de k. Soit L_1 et L_2 deux sous-corps de Ω contenant K de dimensions finies sur K. On note L_1L_2 le sous-corps de Ω engendré par L_1 et L_2.

a) Montrer que $[L_1L_2 : K] \leq [L_1 : K][L_2 : K]$, et qu'en cas d'égalité, $K = L_1 \cap L_2$.

b) On suppose dorénavant L_1/K galoisienne. Montrer que L_1L_2/L_2 est galoisienne et construire un isomorphisme $\mathrm{Gal}(L_1L_2/L_2) \to \mathrm{Gal}(L_1/L_1 \cap L_2)$.

c) Montrer que $[L_1L_2 : K] = [L_1 : K][L_2 : K]/[L_1 \cap L_2 : K]$.

d) On suppose dorénavant que L_2/K est également galoisienne. Montrer que L_1L_2 et $L_1 \cap L_2$ sont des extensions galoisiennes de K.

e) Construire un morphisme injectif $\phi : \mathrm{Gal}(L_1L_2/K) \to \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K)$

f) Montrer que l'image de ϕ est $\{(g_1, g_2) \in \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_2/K), \pi_1(g_1) = \pi_2(g_2)\}$, où $\pi_i : \mathrm{Gal}(L_i/K) \to \mathrm{Gal}(L_1 \cap L_2/K)$ est la surjection canonique.

g) Soit $\mathbb{Q}^{\mathrm{ab}}$ l'ensemble des nombres algébriques x contenus dans une extension galoisienne L de $\mathbb{Q}$ telle $\mathrm{Gal}(L/\mathbb{Q})$ soit commutatif. Montrer que $\mathbb{Q}^{\mathrm{ab}}$ est un corps. Est-ce une extension finie de $\mathbb{Q}$?

Exercice 2. Soit $P \in \mathbb{Z}[X]$ un polynôme unitaire de degré n. Soit E un corps de décomposition de P sur $\mathbb{Q}$, G le groupe de Galois de $E/\mathbb{Q}$. Ecrivons $P = \prod_{i=1}^{n}(X - \alpha_i)$. Soit $A := \mathbb{Z}[\alpha_1, \cdots, \alpha_n] \subset E$ la sous-$\mathbb{Z}$-algèbre de E engendrée par $(\alpha_i)_i$. Soient p un nombre premier et $\overline{P}$ la réduction de P modulo p. Soit N le cardinal de G.

a) Montrer que A est un $\mathbb{Z}$-module libre de rang N.

b) Montrer que si $g \in G$, $g(A) = A$ et en déduire une action de G sur A.

c) Soit $\mathfrak{m}$ un idéal maximal de A contenant pA (justifier l'existence d'un tel $\mathfrak{m}$). Montrer que $L := A/\mathfrak{m}$ est une extension finie de $\mathbb{F}_p$. On note $\pi/A \to L$ la projection canonique.

d) Montrer que L est un corps de décomposition de $\overline{P}$ sur $\mathbb{F}_p$.

e) On suppose dorénavant que $\mathrm{pgcd}(\overline{P}, \overline{P}') = 1$. Montrer que $\mathrm{pgcd}(P, P') = 1$. On note $\Omega := \{\alpha_i\}$ et $\overline{\Omega} := \{\pi(\alpha_i)\}$.
On a deux injections naturelles $i : G \to \mathfrak{S}_\Omega$ et $j : \mathrm{Gal}(L/\mathbb{F}_p) \to \mathfrak{S}_{\overline{\Omega}}$ et $\pi_\Omega : \Omega \to \overline{\Omega}$ induit un isomorphisme $\pi^* : \mathfrak{S}_{\overline{\Omega}} \to \mathfrak{S}_\Omega$ qui envoie σ sur $\pi_\Omega^{-1} \circ \sigma \circ \pi_\Omega$. L'objectif de l'exercice est de montrer que $\pi^* j(\mathrm{Gal}(L/\mathbb{F}_p)) \subset i(G)$.

f) Montrer que si $(\phi_i)_i$ est une famille de morphismes d'anneaux de A vers L deux à deux distincts, alors $(\phi_i)_i$ est une famille libre du L-espace vectoriel $\mathrm{Hom}_{\mathbb{Z}\text{-Mod}}(A, L)$. En déduire qu'il y a au plus N morphismes d'anneaux de A vers L. *Indice* : si $y \in A$ et $\sum_i a_i\phi_i = 0$, alors $\sum_i a_i(\phi_i(y) - \phi_1(y))\phi_i = 0$.

g) Montrer que tout morphisme d'anneaux $A \to L$ est de la forme $\pi \circ \sigma$ pour un unique $\sigma \in G$.

h) Montrer que si $s \in \mathrm{Gal}(L/\mathbb{F}_p)$, alors $s \circ \pi$ est un morphisme d'anneaux $A \to L$.

i) En déduire un morphisme injectif $\mathrm{Gal}(L/\mathbb{F}_p) \to \mathrm{Gal}(E/\mathbb{Q})$.

j) Conclure.

Exercice 3. Soit $P = X^4 - 2 \in \mathbb{Q}[X]$ et L le corps de décomposition de P. Décrire le groupe de Galois G de P et toutes les extensions intermédiaires K telles que $\mathbb{Q} \subset K \subset L$.

Exercice 4. Soit p un nombre premier.

a) Montrer qu'un groupe de cardinal p^2 est commutatif.

b) Montrer qu'un groupe de cardinal p^n est résoluble.

Indice : Commencer par montrer que le centre du groupe n'est pas réduit à l'élément neutre.

Exercice 5. Soit L/K une extension de corps de degré 2. Montrer que c'est une extension normale.

Exercice 6. Soient $P = X^4 + aX^2 + b \in \mathbb{Q}[X]$ un polynôme irréductible, L le corps de décomposition de P et $G = \mathrm{Gal}(L/\mathbb{Q})$. On note $\pm\alpha, \pm\beta$ les racines de P.

a) Montrer que G est isomorphe à un sous-groupe du groupe diédral D_4 d'ordre 8.

b) Montrer que $G \simeq \mathbb{Z}/4\mathbb{Z}$ si et seulement si $(\alpha/\beta - \beta/\alpha) \in \mathbb{Q}$.

c) Montrer que $G \simeq (\mathbb{Z}/2\mathbb{Z})^2$ si et seulement si $\alpha\beta \in \mathbb{Q}$ ou $\alpha^2 - \beta^2 \in \mathbb{Q}$.

d) Montrer que sinon G est isomorphe à D_4.

e) Déterminer le groupe de Galois de $X^4 - 4X^2 - 1$.

Exercice 7. Soit $P = (X^2+3)(X^3-3X+1) \in \mathbb{Q}[X]$ et G le groupe de Galois de P.

a) Montrer que G est isomorphe à un sous-groupe de $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_3$

b) Calculer le cardinal de G.

c) Le groupe est-il commutatif ? cyclique ?

Exercice 8. Si p est un nombre premier et n est un entier premier à p, on note $\left(\frac{n}{p}\right) = 1$ si n est un carré dans $\mathbb{F}_p^\times$ et $\left(\frac{n}{p}\right) = -1$ sinon. Si n est un multiple de p, on note $\left(\frac{n}{p}\right) = 0$
Soient q, p deux nombres premiers impairs distincts. Soient ζ une racine primitive q^{e}de 1 dans une clotûre algébrique $\overline{\mathbb{F}}_p$ de $\mathbb{F}_p$ et

$$\tau = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \zeta^x \in \overline{\mathbb{F}_p}$$

a) Montrer que $\sum_{x\in\mathbb{F}_q} \left(\frac{x}{q}\right) = 0$.

b) Soit $x \in \mathbb{F}_p$. Montrer que

$$\sum_{(y,z)\in\mathbb{F}_p^2/\, y+z=x} \left(\frac{yz}{q}\right) = \left(\frac{-1}{q}\right) \sum_{y\in\mathbb{F}_p^\times} \left(\frac{1-xy^{-1}}{q}\right) = \begin{cases} (-1)^{\frac{q-1}{2}}(q-1) & \text{if} \quad x = 0 \\ (-1)^{\frac{q-1}{2}}(-1) & \text{if} \quad x \neq 0 \end{cases}$$

c) En déduire que $\tau^2 = (-1)^{\frac{q-1}{2}} q$.

d) Montrer que $\tau^p = \left(\frac{p}{q}\right) \tau$

e) En déduire deux expressions pour τ^{p-1} et montrer que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.

Exercice 9. Soit p un nombre premier impair et $\zeta \in \mathbb{C}$ une racine primitive p^{e}de 1. Soit

$$\tau = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right) \zeta^x.$$

a) Montrer que $\tau^2 = (-1)^{\frac{p-1}{2}} p$.

b) En déduire que toute extension de degré 2 de $\mathbb{Q}$ est contenue dans une extension cyclotomique $\mathbb{Q}(\zeta_0)$ où ζ_0 est une racine de 1.

Exercice 10. Soit f le polynôme $X^4 + 8X + 12 \in \mathbb{Q}[X]$.
(i) Montrer que f est irréductible sur $\mathbb{Q}$.
(ii) Montrer que $\mathrm{Gal}(f)$ est isomorphe à $\mathfrak{A}_4$.
(iii) Soit L le corps de décomposition de f dans $\mathbb{C}$. Montrer qu'il n'existe pas d'extension quadratique de $\mathbb{Q}$ contenue dans L.

Exercice 11. Soit f le polynôme $X^4 + X + 1 \in \mathbb{Q}[X]$.
(i) Montrer que f est irréductible sur $\mathbb{Q}$.
(ii) Montrer que $\mathrm{Gal}(f)$ est isomorphe à $\mathfrak{S}_4$.
(iii) Soit α une racine de f dans $\mathbb{C}$. Montrer qu'il n'existe pas d'extension quadratique de $\mathbb{Q}$ contenue dans $\mathbb{Q}(\alpha)$.

Exercice 12. Soient p un nombre premier et f un polynôme irréductible de $\mathbb{Q}[X]$ de degré p. Soit K le corps de décomposition de f dans $\mathbb{C}$. On suppose que f possède exactement deux zéros non réels. Montrer que le groupe de Galois de K sur $\mathbb{Q}$ est isomorphe à $\mathfrak{S}_p$.
Application. Montrer que le groupe de Galois du polynôme $f = X^5 - 4X^3 - 2 \in \mathbb{Q}[X]$ est isomorphe à $\mathfrak{S}_5$.