

## TD n°9.

**Exercice 1.** Soit  $K$  un corps et  $\Omega$  une extension de  $k$ . Soit  $L_1$  et  $L_2$  deux sous-corps de  $\Omega$  contenant  $K$  de dimensions finies sur  $K$ . On note  $L_1L_2$  le sous-corps de  $\Omega$  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  $\text{Gal}(L_1L_2/L_2) \rightarrow \text{Gal}(L_1/L_1 \cap L_2)$ .
- 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  $\phi : \text{Gal}(L_1L_2/K) \rightarrow \text{Gal}(L_1/K) \times \text{Gal}(L_2/K)$
- f) Montrer que l'image de  $\phi$  est  $\{(g_1, g_2) \in \text{Gal}(L_1/K) \times \text{Gal}(L_2/K), \pi_1(g_1) = \pi_2(g_2)\}$ , où  $\pi_i : \text{Gal}(L_i/K) \rightarrow \text{Gal}(L_1 \cap L_2/K)$  est la surjection canonique.
- g) Soit  $\mathbb{Q}^{\text{ab}}$  l'ensemble des nombres algébriques  $x$  contenus dans une extension galoisienne  $L$  de  $\mathbb{Q}$  telle que  $\text{Gal}(L/\mathbb{Q})$  soit commutatif. Montrer que  $\mathbb{Q}^{\text{ab}}$  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  $E/\mathbb{Q}$ . Écrivons  $P = \prod_{i=1}^n (X - \alpha_i)$ . Soit  $A := \mathbb{Z}[\alpha_1, \dots, \alpha_n] \subset E$  la sous- $\mathbb{Z}$ -algèbre de  $E$  engendrée par  $(\alpha_i)_i$ . Soient  $p$  un nombre premier et  $\bar{P}$  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  $\pi/A \rightarrow L$  la projection canonique.
- d) Montrer que  $L$  est un corps de décomposition de  $\bar{P}$  sur  $\mathbb{F}_p$ .
- e) On suppose dorénavant que  $\text{pgcd}(\bar{P}, \bar{P}') = 1$ . Montrer que  $\text{pgcd}(P, P') = 1$ . On note  $\Omega := \{\alpha_i\}$  et  $\bar{\Omega} := \{\pi(\alpha_i)\}$ .  
On a deux injections naturelles  $i : G \rightarrow \mathfrak{S}_\Omega$  et  $j : \text{Gal}(L/\mathbb{F}_p) \rightarrow \mathfrak{S}_{\bar{\Omega}}$  et  $\pi_\Omega : \Omega \rightarrow \bar{\Omega}$  induit un isomorphisme  $\pi^* : \mathfrak{S}_{\bar{\Omega}} \rightarrow \mathfrak{S}_\Omega$  qui envoie  $\sigma$  sur  $\pi_\Omega^{-1} \circ \sigma \circ \pi_\Omega$ . L'objectif de l'exercice est de montrer que  $\pi^*j(\text{Gal}(L/\mathbb{F}_p)) \subset i(G)$ .
- 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  $\text{Hom}_{\mathbb{Z}\text{-Mod}}(A, L)$ . 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  $A \rightarrow L$  est de la forme  $\pi \circ \sigma$  pour un unique  $\sigma \in G$ .
- h) Montrer que si  $s \in \text{Gal}(L/\mathbb{F}_p)$ , alors  $s \circ \pi$  est un morphisme d'anneaux  $A \rightarrow L$ .
- i) En déduire un morphisme injectif  $\text{Gal}(L/\mathbb{F}_p) \rightarrow \text{Gal}(E/\mathbb{Q})$ .
- 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  $L/K$  une extension de corps de degré 2. Montrer que c'est une extension normale.

**Exercice 5.** Soient  $P = X^4 + aX^2 + b \in \mathbb{Q}[X]$  un polynôme irréductible,  $L$  le corps de décomposition de  $P$  et  $G = \text{Gal}(L/\mathbb{Q})$ . 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 6.** Soit  $P = (X^2 + 3)(X^3 - 3X + 1) \in \mathbb{Q}[X]$  et  $G$  le groupe de Galois de  $P$ .

- Montrer que  $G$  est isomorphe à un sous-groupe de  $\mathbb{Z}/2\mathbb{Z} \times \mathfrak{S}_3$
- Calculer le cardinal de  $G$ .
- Le groupe est-il commutatif? cyclique?

**Exercice 7.** 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  $\zeta$  une racine primitive  $q^e$  de 1 dans une clôture algébrique  $\overline{\mathbb{F}_p}$  de  $\mathbb{F}_p$  et

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

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

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

- En déduire que  $\tau^2 = (-1)^{\frac{q-1}{2}} q$ .
- Montrer que  $\tau^p = \left(\frac{p}{q}\right) \tau$
- En déduire deux expressions pour  $\tau^{p-1}$  et montrer que  $\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$ .

**Exercice 8.** Soit  $p$  un nombre premier impair et  $\zeta \in \mathbb{C}$  une racine primitive  $p^e$  de 1. Soit

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

- Montrer que  $\tau^2 = (-1)^{\frac{p-1}{2}} p$ .
- En déduire que toute extension de degré 2 de  $\mathbb{Q}$  est contenue dans une extension cyclotomique  $\mathbb{Q}(\zeta_0)$  où  $\zeta_0$  est une racine de 1.

**Exercice 9.** Soit  $f$  le polynôme  $X^4 + 8X + 12 \in \mathbb{Q}[X]$ .

- Montrer que  $f$  est irréductible sur  $\mathbb{Q}$ .
- Montrer que  $\text{Gal}(f)$  est isomorphe à  $\mathfrak{A}_4$ .
- 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 10.** Soit  $f$  le polynôme  $X^4 + X + 1 \in \mathbb{Q}[X]$ .

- Montrer que  $f$  est irréductible sur  $\mathbb{Q}$ .
- Montrer que  $\text{Gal}(f)$  est isomorphe à  $\mathfrak{S}_4$ .
- Soit  $\alpha$  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 11.** 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  $\mathfrak{S}_5$ .

**Exercice 12.** Soit  $P \in K[X]$  un polynôme unitaire à racines simples dans toute extension de  $K$  et  $L$  son corps de décomposition. Soit  $\Omega = \{\alpha_1, \dots, \alpha_n\}$  l'ensemble des racines de  $P$  dans  $L$ . On note  $d = \text{disc}(P) = \prod_{i < j} (\alpha_i - \alpha_j)^2 \in K$  et  $\sqrt{d} = \prod_{i < j} (\alpha_i - \alpha_j)$ . On identifie  $G = \text{Gal}(L/K)$  avec un sous-groupe de  $\mathfrak{S}_n$ . On note  $H = G \cap \mathfrak{A}_n$ .

- Soit  $g \in G$ . Montrer que  $g(\sqrt{d}) = \epsilon(g)\sqrt{d}$ , où  $\epsilon : G \rightarrow \{\pm 1\}$  est le morphisme signature.
- Montrer que  $G \subset \mathfrak{A}_n$  si et seulement si  $d$  est un carré dans  $K$ .
- Montrer que  $K[\sqrt{d}] = L^H$ .

- d) Soit  $P = X^3 + pX + q \in \mathbb{Q}[X]$  sans racines dans  $\mathbb{Z}$ . Montrer que, si  $-(4p^3 + 27q^2)$  est un carré dans  $\mathbb{Q}$ , le groupe de Galois de  $P$  est  $\mathbb{Z}/3\mathbb{Z}$  et, sinon,  $\mathfrak{S}_3$ .

**Exercice 13.** Soit  $P \in K[X]$  un polynôme irréductible et  $\alpha, \beta$  deux racines distinctes dans un corps de décomposition de  $P$ .

On suppose  $K$  de caractéristique nulle, montrer que  $\alpha - \beta \notin Q$ .

**Exercice 14.** Pour chacun des polynômes suivants, calculer l'action du groupe de Galois sur les racines, faire la liste des sous-corps d'un corps de décomposition et pour chacun d'eux donner un élément primitif du corps et dire s'il est normal.

- a)  $P = X^4 - 7$ ,    b)  $\Phi_{20} = X^8 - X^6 + X^4 - X^2 + 1$ ,    c)  $X^6 + 3$ ,  
d)  $(X^2 - 2)(X^2 - 3)$ ,    e)  $X^3 - 1$ ,    f)  $(X^2 - 2X - 1)(X^2 - 2X - 7)(X^2 - 2X + 2)$ ,  
g)  $\Phi_9 = X^6 + X^3 + 1$ ,    h)  $X^3 + X + 1$ .

**Exercice 15.** Calculer les groupes de Galois de sur  $\mathbb{Q}$  de :

- a)  $X^4 + 2X^2 + X + 3$ ;  
b)  $X^4 + 3X^3 - 3X - 2$ ;  
c)  $X^6 + 22X^5 - 9X^4 + 12X^3 - 37X^2 - 29X - 15$ .

*Indice* : on réduira modulo 2, 3 et 5.

**Exercice 16.** Montrer que pour tout  $n \geq 1$ , il existe un polynôme unitaire  $P \in \mathbb{Z}[X]$  dont le groupe de Galois sur  $\mathbb{Q}$  soit  $\mathfrak{S}_n$ .

**Exercice 17.** Soient  $a, b \in \mathbb{Z}$ . Soit  $\sqrt{b}$  une racine carrée de  $b$  dans  $\mathbb{C}$  et  $\alpha$  une racine carrée de  $a + \sqrt{b}$  dans  $\mathbb{C}$ .

- a) Montrer que si  $a^2 - b$  est un carré dans  $\mathbb{Z}$ , l'extension  $\mathbb{Q}(\alpha)/\mathbb{Q}$  est galoisienne de degré au plus 4.  
b) Supposons  $(a, b) = (7, 16)$ . Montrer que l'extension  $\mathbb{Q}(\alpha)/\mathbb{Q}$  est galoisienne.  
c) Si  $(a, b) = (4, 3)$  montrer que l'extension  $\mathbb{Q}(\alpha)/\mathbb{Q}$  n'est pas galoisienne.  
On pose  $F = X^4 - 2aX^2 + a^2 - b \in \mathbb{Z}[X]$ .  
d) Calculer le discriminant de  $F$ .  
On suppose que  $F$  est irréductible sur  $\mathbb{Q}$ .  
e) Montrer que si  $a^2 - b$  est un carré dans  $\mathbb{Z}$ , l'extension  $\mathbb{Q}(\alpha)/\mathbb{Q}$  est galoisienne de groupe de Galois isomorphe à  $C_2 \times C_2$ .  
f) Montrer que si  $a^2 - b$  appartient à  $b\mathbb{Z}^2$ , l'extension  $\mathbb{Q}(\alpha)/\mathbb{Q}$  est galoisienne de groupe de Galois isomorphe à  $C_4$ .

**Exercice 18.** Soit  $P_1(T) = T^3 - 7T + 7 \in \mathbb{Q}[X]$

- a) Montrer que le polynôme  $P_1$  a trois racines réelles  $x_1, x_2$  et  $x_3$  vérifiant  $x_1 > x_2 > 0 > x_3$ . Calculer le degré de l'extension  $M = \mathbb{Q}(x_1)$  de  $\mathbb{Q}$ .  
b) Montrer que l'extension  $M/\mathbb{Q}$  est galoisienne, et décrire son groupe de Galois.  
c) On note  $\pm y_1, \pm y_2$  et  $\pm y_3$  les racines de  $P_2(T) = T^6 - 7T^2 + 7$ , numérotées de façon que  $x_i = y_i^2$ , et  $L$  le corps  $\mathbb{Q}(y_1, y_2, y_3)$ .  
a) Montrer que  $y_3$  n'appartient pas à  $\mathbb{Q}(y_1, y_2)$ .  
b) Montrer que  $y_2$  n'appartient pas à  $\mathbb{Q}(y_1)$ .  
c) Calculer le degré de  $M$  sur  $L$ .  
d) L'extension  $L/\mathbb{Q}$  est-elle galoisienne? Abélienne?  
d) On note  $G$  le groupe  $\text{Aut}(L)$ . Montrer que, pour  $i \in \{1, 2, 3\}$ , il existe deux éléments  $\tau_i$  et  $\tau'_i$  de  $G$  tels que, pour  $j \neq i$ , on ait

$$\tau_i(y_i) = -y_i, \quad \tau'_i(y_i) = y_i, \quad \tau_i(y_j) = y_j, \quad \tau'_i(y_j) = -y_j.$$

Montrer qu'il existe un élément  $\tau$  de  $G$  tel que

$$\forall i \in \{1, 2, 3\}, \quad \tau(y_i) = -y_i.$$

Donner la liste des sous-corps  $N$  de  $L$  contenant  $M$  et tels que  $[L : N] = 2$ .

e) Montrer qu'il existe un élément  $\sigma$  de  $G$  tel que

$$\sigma(y_1) = y_2, \quad \sigma(y_2) = y_3, \quad \sigma(y_3) = y_1,$$

et calculer

$$\tau_1\sigma\tau_3, \quad \tau_1\sigma^2\tau_1, \quad \tau_3'\sigma\tau_2'.$$

f) Montrer que  $\sqrt{-7}$  appartient à  $L$  et déterminer le groupe  $\text{Aut}(L/\mathbb{Q}(\sqrt{-7}))$ .

g) On pose  $\theta = y_1 + y_2 + y_3$ . Calculer le degré de  $\theta$  sur  $\mathbb{Q}$  (on pourra étudier les images de  $\theta$  sous l'action de  $G$ ). Quelle est la structure du groupe  $\text{Aut}(L/\mathbb{Q}(\theta))$ ? Est-il distingué dans  $G$ ?

h) Indiquer combien de sous-corps de  $\mathbb{Q}(\theta)$  contiennent  $\sqrt{-7}$ .

**Exercice 19.** Soit  $K$  un corps de caractéristique  $p > 0$  et  $L$  une extension finie de  $K$ . On note  $K_s$  l'ensemble des éléments de  $L$  séparables sur  $K$  et  $K_r$  l'ensemble des  $x \in L$  tels qu'il existe  $k \in \mathbb{N}$  tel que  $x^{p^k} \in K$ .

- Montrer que  $K_s$  et  $K_r$  sont des corps et  $K_s \cap K_r = K$ .
- Soit  $x \in L$ . Montrer que  $x \in K_s$  si et seulement si  $K(x^p) = K(x)$ .
- Montrer que pour tout  $x \in L$ , il existe  $k \in \mathbb{N}$  tel que  $x^{p^k} \in K_s$ .
- Soit  $x \in K_s$  et  $P \in K[X]$  le polynôme minimal de  $x$ . Montrer que  $P$  est irréductible dans  $K_r[X]$ .
- Montrer que  $[L : K_r] \geq [K_s : K]$ .
- On suppose l'extension  $L/K$  normale et soit  $G = \text{Aut}(L/K)$ .
  - Montrer que  $K_s/K$  est une extension galoisienne.
  - Montrer que  $L/K_r$  est galoisienne de groupe de Galois  $G$ .
  - Construire un isomorphisme  $G \rightarrow \text{Gal}(K_s/K)$ .

**Exercice 20.** Soient  $K$  un corps et  $P, Q \in K[X]$  deux polynômes non constants. On note  $n$  le degré de  $P$  et  $m$  le degré de  $Q$ . Soit  $L$  un corps de décomposition de  $P \circ Q = P(Q(X))$ . On suppose de plus que  $L/K$  est une extension séparable.

- Montrer que  $L/K$  est une extension galoisienne.
- On note  $K_0$  le sous-corps de  $L$  engendré par  $K$  et les racines de  $P$  contenues dans  $L$ . Montrer que  $K_0/K$  est une extension galoisienne.
- Montrer que  $P \circ Q = \prod_{i=1}^n R_i$  où  $R_1, \dots, R_n \in K_0[X]$  sont des polynômes de degré  $m$ .
- En déduire que  $[L : K]$  divise  $n!(m!)^n$ .

**Exercice 21.** Soit  $K \subset L$  une extension galoisienne de corps tel que  $G := \text{Gal}(L/K)$  soit cyclique de cardinal  $n$ . On suppose de plus que  $K$  contient une racine  $\zeta$  exactement  $n$ ième de 1. On veut montrer qu'il existe  $a \in K$  tel que  $L \simeq K[X]/(X^n - a)$ .

Soit  $\sigma$  un générateur de  $G$  et  $N : L \rightarrow K$  l'application qui à  $x$  associe  $\prod_g g(x)$ .

- Soit  $x \in L$  tel que  $N(x) = 1$ . Montrer que  $\phi_x = id + x\sigma + \dots + [x\sigma(x) \dots \sigma^{n-2}(x)]\sigma^{n-1} : L \rightarrow L$  n'est pas nulle.
- Soit  $y \in \text{Im } \phi_x - \{0\}$ . Montrer que  $x = y/\sigma(y)$ .
- Soit  $b \in L$  tel que  $b/\sigma(b) = \zeta$ . Montrer que  $L = K[b]$  et que  $b^n \in K$ .
- Conclure.

**Exercice 22.** a) Soit  $K \subset L$  une extension de corps et  $P \in K[X]$ . Construire un isomorphisme  $L \otimes_K K[X]/(P) \simeq L[X]/(P)$ .

- Soit  $\Omega$  une extension de  $K$  avec  $\Omega$  algébriquement clos. Soit  $P \in K[X]$  un polynôme irréductible.
  - Montrer que  $P$  est séparable sur  $K$  si et seulement si  $\Omega[X]/(P)$  est réduit.
  - Montrer que  $P$  est radiciel (i.e. de la forme  $X^{p^k} - a$  où  $p = \text{Car}K$ ) si et seulement si  $\Omega[X]/(P)$  est local.
- Soit  $L$  une extension finie de  $K$ .
  - Montrer que  $L/K$  est séparable si et seulement si  $\Omega \otimes_K L$  est réduit.
  - Montrer que  $L/K$  est radicielle si et seulement si  $\Omega \otimes_K L$  est local.