TD n°10.

Exercice 1. Soit $P \in K[X]$ un polynôme unitaire à racine simples dans toute extension de K et L son corps de décomposition. Soit $\Omega = \{\alpha_1, \cdots, \alpha_n\}$ l'ensemble des racines de P dans L. On note $d = \mathrm{disc}(P) = \prod_{i<j}(\alpha_i - \alpha_j)^2 \in K$ et $\sqrt{d} = \prod_{i<j}(\alpha_i - \alpha_j)$. On identifie $G = \mathrm{Gal}(L/K)$ avec un sous-groupe de $\mathfrak{S}_n$. On note $H = G \cap \mathfrak{A}_n$.

a) Soit $g \in G$. Montrer que $g(\sqrt{d}) = \epsilon(g)\sqrt{d}$, où $\epsilon : G \to \{\pm 1\}$ est le morphisme signature.

b) Montrer que $G \subset \mathfrak{A}_n$ si et seulement si d est un carré dans K.

c) 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 2. Soit $P \in K[X]$ un polynôme irréductible et α, β deux racines distinctes dans un corps de décomposition de P.
On suppose K de caractéristique nulle, montrer que $\alpha - \beta \notin Q$.

Exercice 3. 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 4. 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 5. 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 6. Soient $a, b \in \mathbb{Z}$. Soit $\sqrt{b}$ une racine carrée de b dans $\mathbb{C}$ et α 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 7. 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 $\mathrm{Aut}(L)$. Montrer que, pour $i \in \{1,2,3\}$, il existe deux éléments τ_i et τ_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 τ 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 σ 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 $\mathrm{Aut}(L/\mathbb{Q}(\sqrt{-7}))$.

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

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

Exercice 8. 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_{pi} l'ensemble des $x \in L$ tels qu'il existe $k \in \mathbb{N}$ tel que $x^{p^k} \in K$.

a) Montrer que K_s et K_{pi} sont des corps et $K_s \cap K_{pi} = K$.

b) Soit $x \in L$. Montrer que $x \in K_s$ si et seulement si $K(x^p) = K(x)$.

c) Montrer que pour tout $x \in L$, il existe $k \in \mathbb{N}$ tel que $x^{p^k} \in K_s$.

d) Soit $x \in K_s$ et $P \in K[X]$ le polynôme minimal de x. Montrer que P est irréductible dans $K_{pi}[X]$.

e) Montrer que $[L : K_{pi}] \geq [K_s : K]$.

f) On suppose l'extension L/K normale et soit $G = \mathrm{Aut(L/K)}$.

i) Montrer que K_s/K est une extension galoisienne.

ii) Montrer que L/K_{pi} est galoisienne de groupe de Galois G.

iii) Construire un isomorphisme $G \to \mathrm{Gal}(K_s/K)$.

Exercice 9. Soit k un corps et $A := k[[X]]$ l'anneau des séries formelles à coefficients dans K un élément de $k[[X]]$ est un élément $(a_n)_{n\in\mathbb{N}} \in k^{\mathbb{N}}$, noté ici $\sum a_n X^n$, et la multiplication est définie par $(\sum a_n X^n)(\sum b_n X^n) = \sum c_n X^n$ avec $c_n = \sum_{i+j=n} a_i b_j$. Si $a = \sum a_n X^n \in A$ est non nul, on note $v(a) = \min\{n \in \mathbb{N}, a_n \neq 0\}$ et $v(0) = +\infty$. On note $\pi : A \to k$ le morphisme d'anneaux qui à $\sum_n a_n X^n$ associe a_0. Si P est un polynôme de $A[T]$, on note encore $\pi(P)$ l'image dans $k[T]$ obtenue en appliquant π à chaque coefficient.

a) i) Montrer que $v(ab) = v(a) + v(b)$ et que A est intègre.

ii) Montrer que $a \in A$ est inversible si et seulement si $v(a) = 0$

iii) Montrer que deux éléments non nuls a, b sont associés si et seulement si $v(a) = v(b)$.

iv) Montrer que A est un anneau principal.

v) On note $K = \mathrm{Frac}(A)$. Si $a = p/q$ est un élément non nul de K avec p et q premiers entre eux, on note $v(a) = v(p) - v(q)$. Montrer que $a \in A$ si et seulement si $v(a) \geq 0$.

b) i) Soit $P \in A[T]$, et on suppose que $\pi(P) = fg$ avec $f, g \in k[T]$ premiers entre eux et f unitaire. Montrer qu'il existe $\tilde{f}, \tilde{g} \in A[T]$ avec $\tilde{f}$ unitaire, $deg(f) = deg(\tilde{f})$, $P = \tilde{f}\tilde{g}$, $f = \pi(\tilde{f})$ et $g = \pi(\tilde{g})$.
Indice : On écrira $\tilde{f} = \sum f_n X^n$ et $\tilde{g} = \sum g_n X^n$ avec $f_n, g_n \in k[T]$ et on construira f_n et g_n par récurrence sur n.

ii) Soit $P \in K[T]$ un polynôme unitaire irréductible tel que $P(0) \in A$. Montrer que $P \in A[T]$.
Indice : Raisonner par l'absurde et appliquer $i)$ à cP où $c \in K^*$ est tel que cP soit un polynôme primitif de $A[T]$.

c) Soit L une extension finie de K de degré n. Si $x \in L$, on note $v_L(x) = v(\det_K(\mu_x))$, où $\det_K(\mu_x)$ est le déterminant de l'application K-linéaire $L \to L$ qui à y associe xy.

i) Montrer que $v_L(xy) = v_L(x) + v_L(y)$.

ii) Montrer que si $x \in K$, $v_L(x) = nv(x)$.

iii) Soit P le polynôme minimal unitaire de x sur K et d le degré de P. Montrer que $v_L(x) = nv(P(0))/d$.

iv) Montrer que si $v_L(x) \geq 0$ alors $v_L(1+x) \geq 0$ (on appliquera $b)ii)$ au polynôme minimal de x). En déduire que pour tout $x, y \in L$, $v_L(x+y) \geq \min(v_L(x), v_L(y))$.

v) Montrer que $B = \{x \in L, v_L(x) \geq 0\}$ est une sous-A-algèbre de L.

vi) Montrer que les idéaux non nuls de B sont les $I_j = \{x \in L, v_L(x) \geq j\}$ pour $j \in \mathbb{N}$ et montrer que B est principal.

vii) Montrer que $\mathfrak{m} := I_1$ est l'unique idéal maximal de B. On note l le corps $B/\mathfrak{m}$.

viii) Montrer que B est un A-module libre de rang n et en déduire que B/XB est un k-espace vectoriel de dimension n.

ix) Montrer que l est une extension finie de k.

x) Montrer que I_j/I_{j+1} est un l-espace vectoriel de dimension 1 si $j \in v_L(L^*)$ et 0 si $j \notin v_L(L^*)$.

xi) Montrer que $v_L(L^*) = d\mathbb{Z}$ où $d = n/[l : k]$.

d) On garde les notations de $c)$ et on suppose dorénavant que k est un corps algébriquement clos de caractéristique nulle.

i) Montrer qu'il existe $x_0 \in L$ tel que $v_L(x_0) = 1$. Montrer que $(1, x_0, \cdots, x_0^{n-1})$ est une base du A-module B.

ii) Montrer qu'il existe un unique morphisme de k-algèbres $\psi : k[[X]] \to B$ envoyant X sur x_0 et tel que $v_L(\psi(f)) = v(f)$ pour tout $f \in k[[X]]$. Montrer que ψ est un isomorphisme.

iii) Montrer que si $a \in B$ et $v(a) = 0$, $T^n - a$ est scindé dans L (on pourra appliquer $b)ii)$).

iv) Montrer qu'il existe $x \in L$ tel que $x^n = X$.

v) En déduire que L est le corps de rupture de $T^n - X$.

vi) Montrer que L/K est une extension galoisienne de groupe de Galois μ_n.

Exercice 10. Soit K un corps. Une extension algébrique L/K est dite ind-galoisienne si pour tout $x \in L$ il existe une extension L_x finie galoisienne de K contenue dans L et contenant x. Si L/K est une extension ind-galoisienne on note $\mathrm{Gal}(L/K)$ le groupe des automorphismes de L fixant K, que l'on munit de la topologie suivante : $U \subset \mathrm{Gal}(L/K)$ est ouvert si et seulement si pour tout $g \in U$ il existe $x \in L$ tel que $g\mathrm{Stab\ x} \subset \mathrm{U}$.

Soit L/K une extension ind-galoisienne.

i) Montrer que l'on obtient effectivement une topologie sur $\mathrm{Gal}(L/K)$ pour laquelle la multiplication $(x, y) \to xy$ et l'inversion $x \mapsto x^{-1}$ sont continues.

ii) Montrer que si K' est une extension intermédiaire $K \subset K' \subset L$, tout morphisme $K' \to L$ de K-algèbres se prolonge en un élément de $\mathrm{Gal}(L/K)$.

iii) Montrer que si H est un sous-groupe fermé de $\mathrm{Gal}(L/K)$, L^H est un sous-corps de L et $\mathrm{Gal}(L/L^H) = H$.

iv) Montrer que si K' est une extension intermédiaire de L/K, L/K' est ind-galoisienne, $\mathrm{Gal}(L/K')$ est un sous-groupe fermé de $\mathrm{Gal}(L/K)$ muni de la topologie induite et $K' = L^{\mathrm{Gal}(L/K')}$.

v) Montrer que K'/K est ind-galoisienne si et seulement si $\mathrm{Gal}(L/K')$ est un sous-groupe distingué de $\mathrm{Gal}(L/K)$.

vi) Montrer que K'/K est une extension finie si et seulement si $\mathrm{Gal}(L/K')$ est un sous-groupe ouvert de $\mathrm{Gal}(L/K)$.