# 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, $\mathfrak{S}_3$.

**Solution**. C'est le théorème 20.27 du cours. Pour la dernière question, le calcul du discriminant de $X^3+pX+q$ est donné dans la proposition 20.26 (cf. aussi la proposition 20.30).

**Exercice 2.** 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 $\alpha - \beta \notin Q$.

**Solution**. Il existe un automorphisme $\sigma$ du corps de décomposition de $P$ qui envoie $\alpha$ sur $\beta$ par irréductibilité de $P$. Supposons par l'absurde que $k := \alpha - \beta \in K$. On montre alors par récurrence sur $n \in \mathbb{N}$ que $\sigma^n(\alpha) = \alpha - nk$. Comme $K$ est de caractéristique nulle et $k \neq 0$, on en déduit $\sigma^n(\alpha) \neq \alpha$ pour tout $n \geq 1$, ce qui est impossible puisque $\sigma$ doit être d'ordre fini.

**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 $\alpha$ 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 $C_4$.

**Solution**.

a) $\alpha$ est racine du polynôme $P_{a,b} = (X^2-a)^2 - b = X^4 - 2aX^2 + (a^2-b)$. Les autres racines sont $-\alpha$ et $\pm\beta$, avec $\beta = \sqrt{a-\sqrt{b}}$. Si $a^2 - b = c^2$, avec $c \in \mathbb{Z}$, alors ces deux dernières racines peuvent s'écrire $\pm c/\alpha$ et sont dans $\mathbb{Q}(\alpha)$. Comme on ne sait pas si $P_{a,b}$ est irréductible, $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ n'est pas connu.

b) Ici $\sqrt{b} = \pm 4$, donc $\alpha$ est une racine carrée de 11 ou de 3 et $\mathbb{Q}(\alpha)/\mathbb{Q}$ est quadratique donc galoisienne.

c) Si $\mathbb{Q}(\alpha)/\mathbb{Q}$ était galoisienne, elle contiendrait $\alpha^2 - 4 = \sqrt{3}$ et $\alpha\beta = \sqrt{13}$ et on aurait $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{3}, \sqrt{13})$. On peut alors résoudre l'équation $\alpha^2 = 4 + \sqrt{3}$ dans le corps $\mathbb{Q}(\sqrt{3}, \sqrt{13})$ et voir qu'elle n'a pas de solution.

d) On a $F' = 4X(X^2 - a)$, donc le discriminant de $F$ est

$$4^4(a^2-b)N(\alpha^2 - a) = 2^8(a^2-b)F(\sqrt{a})F(-\sqrt{a}) = 2^8 b^2(a^2-b).$$

e) Ici le degré est 4, et on a vu que les racines de $F$ sont $\pm\alpha$ et $\pm c/\alpha$ si $\sigma \in \mathrm{Gal}(F)$, pour toute racine $\gamma$ de $f$ et tout $\sigma$, on a $\sigma^2(\gamma) = \gamma$. Donc $\mathrm{Gal}(f)$ ne contient pas d'élément d'ordre 4 ; c'est donc $C_2 \times C_2$.

f) Ici $\alpha^2\beta^2 = a^2 - b = bt^2$, donc $\beta = t\sqrt{b}/\alpha \in \mathbb{Q}(\alpha)$ qui est donc galoisien. Soit $\sigma \in \mathrm{Gal}(F)$ tel que $\sigma(\alpha) = \beta$. Comme $\sigma(\alpha) \neq \pm\alpha$, on a $\sigma(\alpha^2) \neq \alpha^2$ et $\sigma(\sqrt{b}) = -\sqrt{b}$. On a donc $\sigma(\beta) = t\sigma(\sqrt{b})/\sigma(\alpha) = -\alpha$. On en déduit que $\sigma$ est un 4-cycle et $\mathrm{Gal}(F) = C_4$.

**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 $\tau_i$ 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 $\mathrm{Aut}(L/\mathbb{Q}(\sqrt{-7}))$.

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 $\mathrm{Aut}(L/\mathbb{Q}(\theta))$ ? Est-il distingué dans $G$ ?

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

**Solution**.

a) La fonction $t \mapsto P_1(t)$ atteint son minimum sur $\mathbb{R}^+$ au point $\sqrt{7/3}$, où elle vaut

$$\frac{7}{3\sqrt{3}}(3\sqrt{3} - 2\sqrt{7}) < 0.$$

Comme $P_1(0)$ et $P_1(1)$ sont positifs et $P_1(-4) = -29$ est négatif, $P_1$ a trois racines réelles distinctes, dont une seule est négative. Si une des racines de $P_1$ était rationnelle, ce serait un entier divisant 7, ce qui ne laisse que 4 possibilités, dont aucune n'est racine de $P_1$. On en déduit que $P_1$ est irréductible sur $\mathbb{Q}$, et le degré de $M$ sur $\mathbb{Q}$ est 3. On aurait aussi pu invoquer le critère d'Eisenstein pour le nombre premier 7.

b) Le discriminant $\Delta = -(4(-7)^3 + 27.7^2) = 49$ est un carré sur $\mathbb{Q}$. L'extension $M/Q$ est galoisienne. Le groupe de Galois agit sur les trois racines de $P_1$ comme le groupe alterné : les deux automorphismes non triviaux de $M$ permutent circulairement $x_1$, $x_2$ et $x_3$.

c) a) Le corps $\mathbb{Q}(y_1, y_2)$ est inclus dans $\mathbb{R}$ et ne peut donc contenir $y_3$ qui est imaginaire pur.

b) L'automorphisme de $M$ qui envoie $x_1$ sur $x_2$ se prolonge en un automorphisme $\psi$ de $L$ qui envoie $y_1$ sur $\pm y_2$ et $y_2$ sur $\pm y_3$. Si $y_2 \in \mathbb{Q}(y_1)$, il existe une fraction rationnelle $R$ coefficients dans $\mathbb{Q}$ telle que $R(y_1) = y_2$. En appliquant $\psi$, on trouve $R(\pm y_2) = \pm y_3$, donc $y_3 \in \mathbb{Q}(y_1, y_2)$, en contradiction avec la question précédente.

c) Le même raisonnement qu'au b) montre que $y_1 \notin M$ et $\mathbb{Q}(y_1)$ est quadratique sur $M$, donc de degré 6 sur $\mathbb{Q}$ (on peut aussi voir par le critère d'Eisenstein que $P_2$ est irréductible sur $\mathbb{Q}$). Les questions 2 b) et 2 a) montrent que $\mathbb{Q}(y_1, y_2)$ est une extension quadratique de $\mathbb{Q}(y_1)$ et $L$ est une extension quadratique de $\mathbb{Q}(y_1, y_2)$. En conclusion, $L/M$ est de degré 8 et $L/\mathbb{Q}$ de degré 24.

d) $L$ est le corps de décomposition de $P_2$, c'est donc une extension galoisienne de $\mathbb{Q}$. Si elle était abélienne, tous ses sous-corps seraient galoisiens. Ce n'est pas le cas, puisque $\mathbb{Q}(y_1)$ ne contient pas le conjugué $y_3$ de $y_1$.

d) Le groupe $\mathrm{Gal}(L/M)$ est d'ordre 8. Pour tout élément $\tau$ de ce groupe, on a $\tau(x_i) = x_i$, donc $\tau(y_i) = \epsilon_i y_i$, avec $\epsilon_i = \pm 1$ pour $i \in \{1, 2, 3\}$. L'application qui $\tau$ associe le triplet $(\epsilon_1(\tau), \epsilon_2(\tau), \epsilon_3(\tau))$ induit donc un isomorphisme de $\mathrm{Gal}(L/M)$ sur $\{\pm 1\}^3$. Par exemple, le $\tau_1$ de l'énoncé est l'image réciproque de $(-1, 1, 1)$ et le $\tau$ de l'énoncé est l'image réciproque de $(-1, -1, -1)$. Les 7 éléments non triviaux de $\mathrm{Gal}(L/M)$ sont les $\tau_i$, les $\tau_i'$ et $\tau$. Leurs corps fixes sont les 7 sous-corps de $L$ contenant $M$ et de degr 4 sur $M$. Le corps fixe de $\tau_1$ est $\mathbb{Q}(y_2, y_3)$, celui de $\tau_1'$ est $\mathbb{Q}(y_1, y_2y_3)$. Enfin, le corps fixe de $\tau$ est $M(y_1y_2, y_2y_3)$.

e) L'élément $\psi$ de $G$ construit la question 3 b) envoie $y_1$ sur $\epsilon_2 y_2$, $y_2$ sur $\epsilon_3 y_3$ et $y_3$ sur $\epsilon_1 y_1$. En le composant gauche par l'élément de $\mathrm{Gal}(L/M)$ qui envoie $y_i$ sur $\epsilon_i y_i$, on trouve l'élément $\sigma$ de $G$ cherché. Un élément de $G$ est uniquement caractérisé par son action sur les $y_i$. On en déduit

$$\tau_1\sigma\tau_3 = \tau_3\sigma\tau_2 = \tau_2\sigma\tau_1 = \tau_3'\sigma\tau_2' = \tau_2'\sigma\tau_1' = \tau_1'\sigma\tau_3' = \sigma.$$

Quant $\tau_1\sigma^2\tau_1 = \tau_2'\sigma^2$, il n'a rien de remarquable... (Il y a une faute de frappe dans l'énoncé).

f) On a $x_1x_2x_3 = -7$, et $y_1y_2y_3 = \pm\sqrt{-7} \in L$. L'image de $\sqrt{-7}$ par $\sigma$ est donc $\sqrt{-7}$. Le groupe de Galois de $L/\mathbb{Q}(\sqrt{-7})$ a 12 éléments, soit

$$H = \{Id, \sigma, \sigma^2, \tau_i', \tau_i'\sigma, \tau_i'\sigma^2\}.$$

Il est isomorphe au groupe alterné $\mathfrak{A}_4$.

g) Les 8 images $\pm y_1 \pm y_2 \pm y_3$ sont distinctes, puisque une égalité entre elles donnerait une relation linéaire entre $y_1$, $y_2$ et $y_3$ sur $\mathbb{Q}$. On en déduit que $\theta$ est de degré 8 sur $\mathbb{Q}$, et le groupe de Galois $\mathrm{Gal}(L/\mathbb{Q}(\theta)$ a 3 éléments : c'est $\{Id, \sigma, \sigma^2\}$, qui est cyclique d'ordre 3. On a vu plus haut que $\tau_1\sigma^2\tau_1^{-1} = \tau_1\sigma^2\tau_1 = \tau_2'\sigma^2$ n'est pas dans ce sous-groupe, qui n'est donc pas distingué.

h) Un sous-corps de $\mathbb{Q}(\theta)$ qui contient $\sqrt{-7}$ correspond un sous-groupe de $H$ qui contient $\{Id, \sigma, \sigma^2\}$. Un tel sous-groupe, s'il n'est pas réduit $\{Id, \sigma, \sigma^2\}$, contient l'un des $\tau_i'$, par exemple $\tau_1'$, donc il contient aussi $\tau_2' = \sigma\tau_1'\sigma^2$ et $\tau_3' = \tau_1'\tau_2'$. Finalement, le groupe contient $H$ tout entier, et il n'y a aucun corps intermédiaire entre $K(\theta)$ et $\mathbb{Q}(\sqrt{-7})$.

**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 $G \to \mathrm{Gal}(K_s/K)$.

**Solution**. a) Si $x, y \in K_s$ alors $K(x,y)$ est une extension séparable de $K$ d'après le cours, donc $xy^{-1}$ et $x-y$ sont dans $K_s$. Donc $K_s$ est bien un corps. Si $x, y \in K_{pi}$, on peu prendre le même $k$ quitte à prendre le max dans la définition de $K_{pi}$. Alors $(x-y)^{p^k} = x^{p^k} - y^{p^k} \in K$ puisque le frobenius est un morphisme d'anneau, et la même preuve fonctionne pour $xy^{-1}$. Donc $K_{pi}$ est un corps.

Si $x \in K_s \cap K_{pi}$, alors $x$ est racine de $P = X^{p^k} - x^{p^k} \in K[X]$. Donc le polynôme minimal de $x$ divise $P$ et, par séparabilité, est à racine simple dans une clôture algébrique. Or $P = (X-x)^{p^k}$ donc le polynôme minimal de $x$ est $X-x$, et donc $x \in K$. La réciproque est évidente.

b) $x$ est racine de $(X-x)^p = X^p - x^p \in K(x^p)[X]$. Si $x$ est séparable sur $K$, il l'est aussi sur $K(x^p)$ et donc $Irr_{K(x^p)}x$ est séparable divisant $(X-x)^p$, c'est donc $X-x$, et donc $x \in K(x^p)$. Réciproquement, si $x$ n'est pas séparable, le polynôme minimal de $x$ sur $K$ est de la forme $P = \sum_i a_i X^{pi}$ et donc $x^p$ est racine de $\sum_i a_i X^i$ qui est de degré strictement inférieur à celui de $P$. Donc $[K(x^p) : K] < [K(x) : K]$, et donc $K(x^p) \neq K(x)$.

c) La suite décroissante d'extensions $K(x) \supset K(x^p) \supset K(x^{p^2}) \supset K(x^{p^3}) \supset \cdots$ doit être stationnaire (c'est une suite décroissante de sous-$K$-espaces vectoriels d'un espace vectoriel de dimension finie), et donc il existe $k$ tel que $K(x^{p^k}) = K(x^{p^{k+1}})$, et donc $x^{p^k} \in K_s$ d'après la question précédente.

d) Si $Q = \sum b_i X^i$ est le polynôme minimal de $x$ dans $K_{pi}[X]$, il existe $k$ tel que pour tout $i$, $b_i^{p^k} \in K$. Soit $Q_0 = \sum b_i^{p^k} x^i \in K[X]$. Alors $Q_0(x^{p^k}) = Q(x)^{p^k} = 0$. Donc $[K(x^{p^k}) : K] \leq \deg(\mathrm{Q}_0) = \deg(\mathrm{Q})$. Or comme $x$ est séparable sur $K$, d'après b), $[K(x^{p^k}) : K] = [K(x) : K] = \deg(\mathrm{P})$. On obtient donc $\deg(\mathrm{Q}) \geq \deg(\mathrm{P})$, ce qui prouve que $P$ est irréductible dans $K_{pi}[X]$.

e) Comme $K_s/K$ est séparable, elle admet un élément primitif $x \in K_s$. D'après la question précédente $[K_{pi}(x) : K_{pi}] = [K(x) : K] = [K_s : K]$. Comme $K_{pi}(x) \subset L$ on en déduit l'inégalité voulu (en fait, on a même la divisibilité).

f) i) $K_s/K$ est une extension séparable par définition. Si $g \in G$ et $x \in K_s$ alors $g(x)$ a le même polynôme minimal sur $K$ que $x$, donc est aussi dans $K_s$. Donc $K_s$ est stable par $G$, donc c'est une extension normale.

ii) Si $g \in G$ et $x^{p^k} \in K$, alors $g(x)^{pk} = g(x^{p^k}) = x^{p^k}$, donc $g(x) = x$ par injectivité du frobenius. Donc $K_{pi} \subset L^G$. Réciproquement, soit $x \in L^G$. Il existe $k$ tel que $x^{p^k} \in K_s$. Si $g \in \mathrm{Gal}(K_s/K)$, alors $g$ se prolonge en un élément $\tilde{g}$ de $G$. On a alors $g(x^{p^k}) = \tilde{g}(x)^{p^k} = x^{p^k}$. Donc $x^{p^k} \in K_s^{\mathrm{Gal}(K_s/K)} = K$, et donc $x \in K_[pi$.

iii) La restriction à $K_s$ définit un morphisme surjectif $\pi : G \to \mathrm{Gal}(K_s/K)$. Soit $g \in G$ tel que $\pi(g) = id$ et soit $x \in L$. Il existe $k$ tel que $x^{p^k} \in K_s$. Donc $g(x^{p^k}) = x^{p^k}$. Or $g(x^{p^k}) = g(x)^{p^k}$, donc par injectivité du frobénius, $g(x) = x$. Donc $g$ est l'identité, ce qui montre l'injectivité de $\pi$.

On en déduit en particulier $[L : K_{pi}] = [K_s : K]$.

**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 $\pi$ à chaque coefficient.

i) 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 $v(a) \geq 0$.

ii) 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 $A[T]$.

iii) 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 $d = n/[l:k]$.

iv) 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 $\psi$ 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 $\mu_n$.

**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 $\mathrm{Gal}(L/K)$.