DS (année 2023/2024) - corrigé

Exercice 1. (1) Comme $\overline{K}$ est algébriquement clos, le polynôme $X^p - a$ a une racine $b \in \overline{K}$: on a $a = b^p$ d'où $X^p - a = (X-b)^p$ (car $\overline{K}$ est caractéristique p), et $X^p - a$ admet b comme unique racine dans $\overline{K}$.
(2) On applique le critère d'Eisenstein avec l'élément premier T de $\mathbf{F}_{p^2}[T]$.
(3) Si $x \in \overline{K}$, alors x est racine de P si et seulement si x^p est racine de $Q = X^{p^2} - T^2X + T$, ce qui montre que P a au plus p^2 racines (parce que $x \mapsto x^p$ est un automorphisme de $\overline{K}$). Si $c \in \mathbf{F}_{p^2}$, on a

$$\begin{aligned} P(\theta + c\beta) &= \theta^{p^3} + c^{p^3}\beta^{p^3} - T^2(\theta^p + c^p\beta^p) + T \\ &= P(\theta) + c^p\beta^p(\beta^{p(p^2-1)} - T^2) \\ &= c^p\beta^p(\alpha^p - T^2) = 0 \end{aligned}$$

parce que $c^{p^2} = c$ vu que $c \in \mathbf{F}_{p^2}$. Cela montre que pour tout $c \in \mathbf{F}_{p^2}$, l'élément $\theta + c\beta \in \overline{K}$ est une racine de P. Cela fournit p^2 racines de P qui a donc exactement p^2 racines, qui sont les éléments $\theta + c\beta$ avec $c \in \mathbf{F}_{p^2}$.
(4) Le corps de décomposition de P dans $\overline{K}$ est $K[\theta + c\beta]_{c\in\mathbf{F}_{p^2}} = K[\theta, \beta]$ (*cf* question précédente), parce que $\mathbf{F}_{p^2} \subset K$.
(5) D'après le théorème de prolongement des isomorphismes, il y a une bijection

$$\begin{aligned} \mathrm{Hom}_K(K[\theta], \overline{K}) &\to \{\theta + c\beta\}_{c\in\mathbf{F}_{p^2}} \\ \sigma &\mapsto \sigma(\theta) \end{aligned}$$

ce qui montre que $\#\,\mathrm{Hom}_K(K[\theta], \overline{K}) = p^2 < p^3 = \deg(P) = [K(\theta) : K]$, *i.e.* que $K[\theta]/K$ n'est pas séparable.
(6) Le polynôme minimal de θ^p sur K est $Q = X^{p^2} - T^2X + T$, et $Q' = -T^2$: cela montre que θ^p est séparable sur K, de degré $\deg(Q) = p^2$. L'extension $K[\theta^p]/K$ est donc séparable. Si $K[\theta]/K[\theta^p]$ était séparable, il en serait donc de même de l'extension $K[\theta]/K$, contredisant la question (5) : l'extension $K[\theta]/K$ n'est pas séparable.
(7) On a $K[\theta^p] \subset \{x \in K[\theta]\,;\, x \text{ est séparable sur } K\}$ d'après la question précédente. Réciproquement, soit $x \in K[\theta]$ séparable sur K : l'élément x est *a fortiori* séparable sur $K[\theta^p]$. Comme $K[\theta^p]/K$ est séparable, cela implique que $K[\theta^p, x]/K$ est séparable. Comme $K[\theta^p] \subset K[\theta^p, x] \subset K[\theta]$ et $[K[\theta] : K[\theta^p]] = p$ est premier, on a $K[\theta^p, x] = K[\theta^p]$ ou $K[\theta^p, x] = K[\theta]$. Le deuxième cas est exclu d'après la question (5). On a donc $K[\theta^p, x] = K[\theta^p]$, *i.e.* $x \in K[\theta^p]$, ce qui conclut.

Exercice 2. (1) On a $P \in K[X] \subset F[X]$ et $P(\theta) = 0$ donc $P \in QF[X]$ (par définition du polynôme minimal Q), *i.e.* $Q \mid P$ dans $F[X]$.
(2) Comme L/K est normale, toutes les racines de P sont dans L : c'est *a fortiori* le cas des racines de Q en vertu de la question précédente.
(3) Les coefficients de Q sont, au signe près, les polynômes symétriques élémentaires en les racines de Q. Comme ces dernières appartiennent à L d'après la question précédente, on a $Q \in L[X]$. Par ailleurs, $Q \in F[X]$ et $F \cap L = K$: on a en fait $Q \in K[X]$, et Q divise P dans $K[X]$. Comme P est irréductible sur K, on a donc $Q = P$ (les deux sont unitaires). Finalement, on a $[F[\theta] : F] = \deg(Q) = \deg(P) = [K[\theta] : K] = [L : K]$ vu que $L = K[\theta]$.