Exercice bonus.

1. Soit $K \subseteq L$ une extension finie de corps, et supposons que K est parfait alors que L ne l'est pas. Il existe alors un polynôme irréductible $f(t) \in L[t]$ tel que f a des racines multiples dans son corps de décomposition E. Soit $\alpha \in E$ une racine multiple de $f(t)$, et soit $g(t)$ le polynôme minimal de α dans K.

   omme $g(\alpha) = 0$, on a par définition que $f(t)$ divise $g(t)$ dans $L[t]$. Ainsi, α est une racine double de $g(t)$. Or, comme K est parfait, g n'a que des racines simples, ce qui donne donc une contradiction.

20 pts

2. Notons K le corps de l'énoncé, et pour tout $n > 0$, soit

$$K_n := \mathbb{F}_p(t)[X_1, X_2, \dots, X_n]/(X_1^p - t, X_2^p - X_1, \dots, X_n^p - X_{n-1}).$$

Montrons tout d'abord que chaque K_n est un corps. Montrons tout d'abord que

$$\mathbb{F}_p(t)[X_1, X_2, \dots, X_n]/(X_1^p - t, X_2^p - X_1, \dots, X_n^p - X_{n-1}) \cong \mathbb{F}_p(t)[X_n]/(X_n^{p^n} - t).$$

On a un morphisme naturel

$$f\colon \mathbb{F}_p(t)[X_n] \to \mathbb{F}_p(t)[X_1, X_2, \dots, X_n]/(X_1^p - t, X_2^p - X_1, \dots, X_n^p - X_{n-1})$$

envoyant X_n sur X_n. Ce morphisme est surjective, vu que dans le quotient de droite, chaque X_i vaut une puissance de X_n. De plus, on vérifie que $X_n^{p^n} - t \in \ker(f)$, donc on obtient par passage un quotient un morphisme surjectif

$$\mathbb{F}_p(t)[X_n]/(X_n^{p^n} - t) \to \mathbb{F}_p(t)[X_1, X_2, \dots, X_n]/(X_1^p - t, X_2^p - X_1, \dots, X_n^p - X_{n-1}).$$

De plus, le polynôme $X_n^{p^n} - t \in \mathbb{F}_p(t)[X_n]$ est irréductible. EN effet, par le lemme de Gauss, il suffit montrer que $X_n^{p^n} - t \in \mathbb{F}_p[t, X_n]$ est irréductible. C'est bien le cas, par exemple par le critère d'Eisenstein appliqué a $t \in \mathbb{F}_p[t, X_n]$.

Comme $\mathbb{F}_p(t)[X_n]$ est principal, l'idéal $(X_n^{p^n} - t)$ est alors automatiquement maximal, et donc le quotient $\mathbb{F}_p(t)[X_n]/(X_n^{p^n} - t)$ est un corps. Le morphisme f est alors automatiquement injectif, car un corps n'a pas d'idéal non-trivial.

Ainsi, la preuve ci-dessus montre que K_n est un corps. Notez que l'on a un morphisme

$$\mathbb{F}_p(t)[X_1, \dots, X_n] \to \mathbb{F}_p(t)[X_j]_{j \geq 1} \to K,$$

qui en passant au quotient donne un morphisme $\phi_n\colon K_n \to K$. Par le même argument que ci-dessus, ϕ_n est injectif, et donc $\phi_n(K_n)$ est un sous-corps de K.

Finalement, comme seulement un nombre fini de variable n'apparaît dans un élément de $\mathbb{F}_p(t)[X_n]_{n \geq 1}$, on en déduit automatiquement de

$$K = \bigcup_{n \geq 1} \phi_n(K_n).$$

On peut maintenant déduire que K est un corps. Soit $0 \neq \alpha \in K$. Alors $\alpha \in \phi_n(K_n)$ pour un certain n, et donc vu que $\phi_n(K_n)$ est un corps, α admet bel et bien un inverse.

Montrons finalement que K est parfait, en montrant que $K^p = K$. Pour chaque n, notons par t^{1/p^n} l'image de X_n dans K (cette notation a du sens, car $(t^{1/p^n})^{p^n} = t$). Alors un élément K s'écrit comme quotient d'éléments de la forme

$$f = \sum_{i=1}^{n} a_i t^{1/p^i}$$

avec $a_i \in \mathbb{F}_p$. Alors

$$\left(\sum_{i=2}^{n+1} a_{i-1} t^{1/p^i}\right)^p = \sum_{i=2}^{n+1} a_{i-1}^p \left(t^{1/p^i}\right)^p = \sum_{i=2}^{n+1} a_{i-1} t^{1/p^{i-1}} = f,$$

et donc $f \in K^p$. Ainsi, tout élément de K s'écrit comme quotient d'éléments ayant une racine p'ème, et donc $K^p = K$ (i.e. K est parfait).

40 pts (30 pour montrer que c'est un corps, 10 pour montrer qu'il est parfait)

3. Comme $K^p = K$, le morphisme de Frobenius $(\cdot)^p \colon K \to K$ est surjectif. Il est aussi injectif car K est un corps, et donc c'est un isomorphisme. Soit alors ϕ' le morphisme $K[X] \to K[X]$ fixant X et valant l'inverse du Frobenius sur K. Par construction, $\phi' = \phi^{-1}$ et donc ϕ est un isomorphisme.

   15 pts

4. Fixons $i \in \mathbb{Z}$. Soient α_j les racines de f dans L (L est alors généré par les α_j par définition). Soit aussi L_i le corps de décomposition de $\phi_i(f)$ sur L.

   Montrons que les racines de $\phi_i(f)$ sont les $\alpha_j^{p^i}$. Ecrivons $f = \sum_s a_s X^s$, et $\beta \in L_i$. Alors

$$\phi_i(f)(\beta) = \sum_s a_s^{p^i} \beta = \sum_s a_s^{p^i} (\beta^{p^{-i}})^{p^i} = \left(\sum_s a_s \beta\right)^{p^i},$$

   et donc

$$\phi_i(f)(\beta) = 0 \iff \beta = \alpha_j^{p^i}$$

   pour un certain i. Cela montre que L contient toutes les racines de $\phi_i(f)$, et donc que $L = L_i$. De plus, L est bel est bien généré par les éléments $\alpha_j^{p^i}$. En effet, soit M_i le sous-corps de L généré par ces éléments. Vu que M_i est parfait par le point (1), on a alors que pour tout j,

$$\alpha_j = (\alpha_j^{p^i})^{p^{-i}} \in M_i,$$

   et donc on a bel et bien $M_i = L$. On a donc montré que L était le corps de décomposition de $\phi_i(f)$.

25 pts.