TD n°7.

Exercice 1. Montrer que $\mathbb{F}_p(X)$ n'est pas un corps parfait.

Exercice 2. Soit K un corps parfait et $P \in K[X]$. Montrer que si P est irréductible, alors $\mathrm{pgcd}(P, P') = 1$. Soit K un corps qui n'est pas parfait. Montrer qu'il existe un polynôme irréductible $P \in K[X]$ irréductible tel que $P' = 0$.

Exercice 3. Soit K un corps parfait de caractéristique $p > 0$ et K' une extension finie de K.

a) Soient $(x_i)_i$ une base du K-espace vectoriel K' et $f : K' \to K'$ l'unique application K-linéaire telle que $f(x_i) = x_i^p$ pour tout i. Montrer que f est injective.
b) En déduire que K' est parfait.
c) on ne suppose plus K'/K finie, mais seulement algébrique. Montrer que K' est parfait.

Exercice 4. Soit K un corps de caractéristique $p > 0$.

a) Montrer qu'il existe une extension K' de K tel que K soit un corps parfait (on pourra prendre pour K' une clôture algébrique de K) .
b) On note $K^{\mathrm{pf}} = \{x \in K' : \exists n \in \mathbb{N}, x^{p^n} \in K\}$. Montrer que K^{pf} est un sous-corps parfait de K' contenant K.
c) Montrer que K^{pf} vérifie la propriété universelle suivante : pour toute extension L de K telle que L soit un corps parfait, il existe un unique morphisme de K-algèbres $K^{\mathrm{pf}} \to L$.

Exercice 5. Algorithme de Berlekamp

a) Soit A une $\mathbb{F}_p$-algèbre. Montrer que $\mathrm{Fr}_p : A \to A$ définie par $f(x) = x^p$ est $\mathbb{F}_p$-linéaire.
b) Montrer que si A est un corps, alors $\ker(\mathrm{Fr}_p - \mathrm{Id}_A)$ est un sous-$\mathbb{F}_p$-espace vectoriel de A de dimension 1.
c) Montrer que si $A = K_1 \times \cdots K_n$ est un produit de n corps, alors $\ker(\mathrm{Fr}_p - \mathrm{Id}_A)$ est un sous-$\mathbb{F}_p$-espace vectoriel de A de dimension n.
d) Soit $P \in \mathbb{F}_p[X]$ tel que $\mathrm{pgcd}(P, P') = 1$. On pose $A = \mathbb{F}_p[X]/(P)$. Montrer que $\ker(\mathrm{Fr}_p - \mathrm{Id}_A)$ est un sous-espace vectoriel de A de dimension le nombre de facteurs irréductibles de P.

Exercice 6. Soit p un nombre premier et $a \in \mathbb{F}_p$. Soit $P = X^p - X - a \in \mathbb{F}_p[X]$.

a) Si $a = 0$, donner la décomposition en facteur irréductible de P. On suppose dorénavant $a \neq 0$.
b) Montrer que $P(X + 1) = P(X)$.
c) Soit Q un facteur irréductible de P. Montrer que $Q(X + 1)$ est aussi un facteur irréductible de P.
d) Montrer que $Q(X + 1) = Q(X)$ (on pourra considérer une action de $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble des facteurs irréductibles de P).
e) Montrer que si $R \in \mathbb{F}_p[X]$ est de degré $\leq p - 1$ et $R(X + 1) = R(X)$, alors R est un polynôme constant.
f) En déduire que P est irréductible.
g) Soit $b \in \mathbb{Z}$ premier à p. Montrer que $X^p - X - b$ est un polynôme irréductible de $\mathbb{Q}[X]$.