TD n°7.

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

Solution. Comme $A = \mathbb{F}_p[X]$ est factoriel (même principal),$K = \mathrm{Frac}(A)$ et X est irréductible, le polynôme $T^p - X$ est irréductible dans $K[T]$, donc n'a pas de racine. Donc X n'est pas dans l'image du frobenius.

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 $P' = 0$.

Solution. Si $P' \neq 0$, alors $\deg \mathrm{pgcd}(P, P') \leq \deg P' < \deg P$, et $\mathrm{pgcd}(P, P')|P$, donc si P est irréductible $\mathrm{pgcd}(P, P') = 1$. Il suffit donc de montrer que $P' \neq 0$ (ce qui est évident si $p := \mathrm{car}\, K = 0$, on suppose dorénavant $p \neq 0$). Supposons $P' = 0$ et écrivons $P = \sum_k a_k X^k$. Alors $P' = \sum_k k a_k X^{k-1} = 0$ donc $a_k = 0$ si k n'est pas divisible par p. Donc $P = \sum_j a_{pj} X^{pj}$. Comme K est supposé parfait, il existe b_j tel que $b_j^p = a_p j$. Alors $P = \sum_j (b_j X^j)^p = (\sum_j b_j X^j)^p$, ce qui contredit l'irréductibilité de P.

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.

Solution. a) Soit $y = \sum_i a_i x_i \in \ker f$ avec $a_i \in K$. Comme K est parfait, soit $b_i \in K$ tel que $b_i^p = a_i$. Alors $0 = f(y) = (\sum_i b_i x_i)^p$, donc comme (x_i) est une famille libre, pour tout i, $b_i = 0$, donc $a_i = 0$, donc $y = 0$.

b) Soit $y \in K'$. Comme K' est de dimension finie sur K, l'injectvité de f implique sa surjectivité. Il existe donc $z = \sum_i a_i x_i$ avec $a_i \in K$ tel que $f(z) = y$. Comme K est parfait, il existe $b_i \in K$ tel que $b_i^p = a_i$. On a alors $y = (\sum_i b_i x_i)^p$, ce qui prouve que K' est parfait.

c) Soit $y \in K'$. Alors $K(y)$ est une extension finie de K, donc $K(y)$ est parfait d'après 2. Il existe donc $z \in K(y) \subset K'$ tel que $z^p = y$, ce qui montre 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 $K^{\mathrm{pf}} \to L$.

Solution. a) Soit K' une clôture algébrique de K. Soit $x \in K'$. Comme K' est algébriquement clos, le polynôme $X^p - x$ admet une racine, et donc x est dans l'image du frobenius. Donc K' est parfait.

b) Si $x, y \in K^{\mathrm{pf}}$, il existe n, m tels que $x^{p^n}, y^{p^m} \in K$. On peut supposer $n = m$ quitte à les remplacer par le maximum des deux. Alors $(x-y)^{p^n} = x^{p^n} - y^{p^n} \in K$ et si $y \neq 0$, $(x/y)^{p^n} = x^{p^n}/y^{p^n} \in K$, donc K^{pf} est un sous-corps de K'. De plus si $x \in K$, $x^{p^0} = x \in K$ donc K^{pf} contient K.
Enfin, si $x \in K^{\mathrm{pf}}$, soit n tel que $x^{p^n} \in K$. Comme K' est parfait il existe $y \in K'$ tel que $y^p = x$. Alors $y^{p^{n+1}} = x^{p^n} \in K$ donc $y \in K^{\mathrm{pf}}$, ce qui montre que K^{pf} est parfait.

c) Soit L comme dans l'énoncé. Soit $x \in K^{\mathrm{pf}}$. Il existe n tel que $x^{p^n} \in K \subset L$. Comme L est parfait le polynôme $X^{p^n} - x^{p^n}$ admet une racine y, unique par injectivité du frobenius.
Soit f un morphisme de K-algèbres $K^{\mathrm{pf}} \to L$. Alors $f(x)^{p^n} = f(x^{p^n}) = y^{p^n}$, donc par injectivité du frobenius, $f(x) = y$, ce qui montre l'unicité de f.
Réciproquement, posons $f(x) = y$ (ceci ne dépend pas du choix de n). Si $x_1, x_2 \in K^{\mathrm{pf}}$, il existe n tels que $x_1^{p^n}, x_2^{p^n} \in K$. Alors $(f(x_1) + f(x_2))^{p^n} = f(x_1)^{p^n} + f(x^2)^{p^n} = x_1^{p^n} + x_2^{p^n} = (x_1 + x_2)^{p^n} = f(x_1 + x_2)^{p^n}$, et donc par injectivité du frobenius f est additive. La multiplicativité de f se prouve de la même façon.

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 $E := \ker(\mathrm{Fr}_p - \mathrm{Id}_A)$ 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 $E := \ker(\mathrm{Fr}_p - \mathrm{Id}_A)$ 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 $E := \ker(\mathrm{Fr}_p - \mathrm{Id}_A)$ est un sous-espace vectoriel de A de dimension le nombre de facteurs irréductibles de P.

Solution. a) Si $a, b \in \mathbb{F}_p$, alors $\mathrm{Fr}_p(ax + by) = \sum_{k=0}^{p} \binom{p}{k} a^k x^k b^{p-k} y^{p-k} = a^p x^p + b^p y^p$ car les coefficients binomiaux pour $k \neq 0, p$ sont divisibles par p. Or $a^p = a$ et $b^p = b$ d'après le petit théorème de Fermat, donc Fr_p est bien $\mathbb{F}_p$ linéaire.

b) E est l'ensemble des racines de $X^p - X$. Comme A est un corps, il y a au plus p telles racines. Les éléments de $\mathbb{F}_p \subset A$ sont de telles racines, et donc $E = \mathbb{F}_p$ est bien un $\mathbb{F}_p$-espace vectoriel de dimension 1.

c) $(x_1, \cdots, x_n) \in E$ si et seulement si $x_i^p = x_i$ pour tout i, si et seulement si $x_i \in \mathbb{F}_p$ d'après la question précédente. Donc $E = \mathbb{F}_p \times \cdots \times \mathbb{F}_p$ est de dimension n.

d) Comme $\mathrm{pgcd}(P, P') = 1$, les facteurs irréductibles de P apparaissent avec multiplicité 1 dans la factorisation de P. Donc $P = Q_1 \cdots Q_n$ où les Q_i sont tous distincts. Le théorème des restes chinois affirme que $A = \prod_i \mathbb{F}_p[X]/Q_i$ et $K_i = \mathbb{F}_p[X]/Q_i$ est un corps puisque Q_i est irréductible. La question précédente nous dit donc que E est de dimension n sur $\mathbb{F}_p$.

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 $\mathbb{Q}[X]$.

Solution. a) Si $x \in \mathbb{F}_p$, $P(x) = 0$ donc $\prod_{x \in \mathbb{F}_p}(X - x)$ divise P, et comme les deux polynômes sont de même degré et de même coefficient dominant, ils sont égaux.

b) $P(X + 1) = (X + 1)^p - (X + 1) - a = X^p + 1 - X - 1 - a = X^p - X - a$.

c) L'application $\mathbb{F}_p[X] \to \mathbb{F}_p[X]$ qui à R associe $R(X + 1)$ est un isomorphisme d'anneaux, donc préserve l'irréductibilité et la relation de divisibilité. Donc $Q(X+1)$ est irréductible et $Q(X+1)$ divise $P(X+1) = P$, comme voulu.

d) On considère l'action $k.Q \mapsto Q(X + k)$. Le stabilisateur de Q est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$, c'est donc soit $\mathbb{Z}/p\mathbb{Z}$ (auquel cas $Q(X + 1) = Q$ comme voulu), soit $\{0\}$. Si le stabilisateur est $\{0\}$, alors l'orbite de Q est de cardinal p. Or comme P est de degré p, s'il a au moins p facteurs irréductibles, ils doivent être de degré 1, et donc P devrait avoir une racine. Or si $x \in \mathbb{F}_p$, $P(x) = -a \neq 0$. Contradiction.

e) Soit z une racine de R dans une extensions K de $\mathbb{F}_p$. Alors $(z+a)_{a \in \mathbb{F}_p}$ est une famille de p racines distinctes de R, ce qui contredit $\deg R < p - 1$.

f) Si Q est un facteur irréductible de P, alors $Q(X + 1) = Q(X)$ d'après d), donc $\deg Q \geq p$ d'après e, ce qui prouve que P est irréductible.

g) Si $P = X^p - X - b$ était réductible, son image $\bar{P}$ dans $\mathbb{F}_p[X]$ par réduction modulo p serait aussi réductible puisque P est unitaire, ce qui est en contradiction avec f). Donc P est irréductible dans $\mathbb{Z}[X]$ donc dans $\mathbb{Q}[X]$