# TD n°6.

Un corps est dit parfait si $Car(k) = 0$ ou si $p := Car(k) > 0$ et $\mathrm{Frob}_p : K \to K$ est surjectif ($\mathrm{Frob}_p(x) = x^p$).

## 1 Extensions transcendantes

**Exercice 1.** Soit $k$ un corps et $K = k(X)$.

a) Soit $F \in K \backslash k$. On écrit $F = \frac{P(X)}{Q(X)}$, avec $P, Q \in k[X]$ premiers entre eux.

i) Montrer que $X$ est algébrique sur $k(F)$ (on pourra considérer $R(T) := P(T) - FQ(T) \in k(F)[T]$).

ii) En déduire que $F$ est transcendant sur $k$.

iii) Montrer que $[K : k(F)] = \max(\deg(P), \deg(Q))$ (on pourra montrer que $R(T)$ est irréductible dans $k[F][T]$).

b) Soit $\phi : \mathrm{GL}_2(k) \to \mathrm{Aut}_k(K)$ le morphisme de groupe défini par

$$\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} (F) = F\left(\frac{aX+b}{cX+d}\right).$$

Montrer que $\phi$ est surjectif, et que $\ker(\phi) = k^\times$.

## 2 Caractéristique non nulle

**Exercice 2. Algorithme de Berlekamp**

a) Soit $A$ une $\mathbb{F}_p$-algèbre. Montrer que $\mathrm{Frob}_p : A \to A$ définie par $f(x) = x^p$ est $\mathbb{F}_p$-linéaire.

b) Montrer que si $A$ est un corps, alors $E := \ker(\mathrm{Frob}_p - \mathrm{Id}_A)$ 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 $E := \ker(\mathrm{Frob}_p - \mathrm{Id}_A)$ 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 $E := \ker(\mathrm{Frob}_p - \mathrm{Id}_A)$ est un sous-espace vectoriel de $A$ de dimension le nombre de facteurs irréductibles de $P$.

**Exercice 3.** 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 $\mathbb{Q}[X]$.

**Exercice 4.** Soient $X$ et $Y$ deux indéterminées et $p$ un nombre premier. On pose

$$K = \mathbb{F}_p(X^p, Y^p) \quad \text{et} \quad L = \mathbb{F}_p(X, Y).$$

(i) Montrer que $L$ est une extension finie de $K$ de degré $p^2$.
(ii) Montrer qu'il n'existe pas d'élément $\theta \in L$ tel que $L = K(\theta)$.

**Exercice 5.** Soient $K$ un corps , $F = X^3 - 3X - 1 \in K[X]$ et $\alpha$ une racine de $F$ dans une clôture algébrique de $K$. Montrer que $K(\alpha)$ est une extension séparable de $K$.

**Exercice 6.** Soient $K$ un corps de caractéristique un nombre premier $p$ et $f$ un polynôme irréductible sur $K$. Montrer que $f$ n'est pas séparable si et seulement si il existe $g$ dans $K[X]$ tel que $f(X) = g(X^p)$.

**Exercice 7.** Soient $K$ un corps de caractéristique un nombre premier $p$ et $L$ une extension finie de $K$ de degré non divisible par $p$. Montrer que $L$ est séparable sur $K$.

**Exercice 8.** Soient $K = \mathbb{F}_p(X)$ et $P = T^p - X \in K[T]$. Montrer que $P$ n'est pas séparable.

**Exercice 9.** Soit $k$ un corps, $P \in k[X]$ un polynôme irréductible et $L$ une extension finie de $k$. Soit $\Omega$ une extension algébriquement close de $k$.

a) Montrer que $P$ est séparable si et seulement si $\Omega \otimes_k k[X]/(P)$ est un anneau réduit.

b) Montrer que $L$ est une extension séparable de $k$ si et seulement si $\Omega \otimes_k L$ est un anneau réduit.

**Exercice 10.** Montrer que $K = \mathbb{F}_p(X)$ n'est pas un corps parfait.

**Exercice 11.** 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 12.** 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 13.** 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 $K^{\mathrm{pf}}$ est un sous-corps parfait de $K'$ contenant $K$.

c) Montrer que $K^{\mathrm{pf}}$ 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 $K^{\mathrm{pf}} \to L$.

# 3 Extensions galoisiennes

**Exercice 14.** Soit $n \in \mathbb{N}^*$. Soit $\Phi_n = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} (X - e^{2i\pi k/n}) \in \mathbb{C}[X]$.

a) Montrer que $X^n - 1 = \prod_{d|n} \Phi_d$. En déduire que $\Phi_n \in \mathbb{Z}[X]$.

b) Soit $\zeta$ une racine primitive $n^{\mathrm{e}}$de 1 et $p$ un nombre premier premier à $n$. Soit $f$ et $g$ les polynômes minimaux unitaire sur $\mathbb{Q}$ de $\zeta$ et $\zeta' = \zeta^p$. On suppose $f \neq g$.

   i) Montrer que $fg | \Phi_n$ et $f | g(X^p)$.

   ii) Montrer que l'image de $\Phi_n$ dans $\mathbb{F}_p[X]$ a un facteur irréductible ayant multiplicité au moins deux, et en déduire une contradiction.

c) En déduire que $\Phi_n$ est un polynôme irréductible.

d) Montrer que $\mathbb{Q}(e^{2i\pi/n})$ est une extension galoisienne de $\mathbb{Q}$ et décrire son groupe de Galois.

e) Soit $K$ une extension finie de $\mathbb{Q}$. Montrer que $K$ ne contient qu'un nombre fini de racines de 1.

**Exercice 15.** Soit $a$ un entier sans facteur carré, différent de $0, 1$ et $-1$. Soit $p$ un nombre premier. Soit $K$ un corps de décomposition de $X^p - a$ sur $\mathbb{Q}$. Calculer $[K : \mathbb{Q}]$.
Soit $G = \mathrm{Gal}(K/\mathbb{Q})$. Montrer que $G$ a un sous-groupe distingué $H$ isomorphe à $\mathbb{Z}/p\mathbb{Z}$ tel que $G/H$ soit isomorphe à $(\mathbb{Z}/p\mathbb{Z})^*$.

**Exercice 16.** Soit $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Montrer que $K$ est une extension galoisienne de $\mathbb{Q}$ et décrire son groupe de Galois.

**Exercice 17.** Soient $p_1, \cdots, p_n$ des nombres premiers distincts deux à deux. Montrer que $\mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$ est une extension galoisienne de $\mathbb{Q}$ et décrire son groupe de Galois.

**Exercice 18.** Soient $f$ un polynôme irréductible de $\mathbb{Q}[X]$ et $K$ le corps de décomposition de $f$ dans $\mathbb{C}$. On suppose que le groupe de Galois de $K$ sur $\mathbb{Q}$ est abélien. Montrer que pour toute racine $\alpha$ de $f$, on a $K = \mathbb{Q}(\alpha)$.