X

Exercice 1

a) Montrer que $\mathbb{Z}[\sqrt{2}]/(3)$ est un corps fini de cardinal 9.

b) Montrer que $\left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z}/5\mathbb{Z} \right\}$ est un corps fini de cardinal 25.

Exercice 2 a) Factoriser $X^8 - X$ sur $\mathbb{F}_2$ puis $X^{16} - X$ sur $\mathbb{F}_2$. En déduire les polynômes irréductibles unitaires sur $\mathbb{F}_2$ de degré $\leqslant 4$.

b) Déterminer les polynnômes irréductibles de degré 2 sur $\mathbb{F}_3$. En déduire la factorisation de $X^9 - X$ sur $\mathbb{F}_3$.

c) Montrer que $\mathbb{F}_2[X]/(X^3 + X^2 + 1)$ est un corps. On pose $x := X \bmod (X^3 + X^2 + 1)$. Exprimer les racines de $X^3 + X^2 + 1$ dans la base $1, x, x^2$.

d) Montrer que $X^3 - 2$ est irréductible sur $\mathbb{F}_7$. Déterminer les trois racines de $X^3 - 2$ dans le corps $\mathbb{F}_7[X]/(X^3 - 2)$ en fonction de $x := X \bmod (X^3 - 2)$. Montrer que $x^2 + x + 2$ est une racine de $P := X^3 + X^2 - X - 2$. Déterminer les autres racines de ce polynôme dans la base $1, x, x^2$.

Exercice 3 *a) Montrer qu'il existe un unique corps de cardinal q^d entre $\mathbb{F}_q$ et $\mathbb{F}_{q^n}$ si $d|n$. Existe-t-il un corps de cardinal 4 dans $\mathbb{F}_8$?*

b) Soit $P \in \mathbb{F}_q[X]$ un polynôme irréductible de degré d. Montrer que $P|X^{q^n} - X$ dans $\mathbb{F}_q[X] \Leftrightarrow d|n$.

Exercice 4 Soit k un corps.

a) Soient $p(x), q(x) \in k[x]$ deux polynômes premiers entre eux. Montrer que $[k(x) : k(p/q)] = \max\{\deg p, \deg q\}$.

b) En déduire qu'un sous-corps $k \leqslant K \leqslant k(x)$ tel que $k \neq K$ est de la forme $K = k(p/q)$ pour un certain $p/q \in k(x)$ *(indication : soit $f = T^d + a_1 T^{d-1} + ... + a_d$ le polynôme minimal de x sur K ; un des $a_i \notin k$, poser alors $p/q := a_i$; montrer que si p, q sont premiers entre eux, si $c(X)$ est le ppcm des dénominateurs des coefficients de f, les polynômes $F(X,T) := c(X)f(X,T)$ et $p(X)q(T) - p(T)q(X)$ sont associés dans $k[X,T]$)*

Exercice 5 *a) Soit $f := Y^2 - X^3$. Montrer que $\mathrm{Frac}\mathbb{C}[X,Y]/(f) = \mathbb{C}(t)$ où $t := Y/X$.*

b) Soit $f := Y^2 + X^2 - 1$. Montrer que $\mathrm{Frac}\mathbb{R}[X,Y]/(f) = \mathbb{R}(t)$ où $t := Y/(X+1)$.

c) Soit $f := Y^2 - X^3 + X$. Montrer que $\mathrm{Frac}\mathbb{C}[X,Y]/(f)$ n'est pas isomorphe à un corps de la forme $\mathbb{C}(t)$.

Exercice 6 *a) Montrer que $\mathbb{C}(y + y^{-1})$ est le sous-corps de $\mathbb{C}(y)$ invariant par l'automorphisme $y \mapsto y^{-1}$.*

b) Soit G le sous-groupe des automorphismes de $\mathbb{F}_q[x]$ de la formme $x \mapsto ax + b/cx + d$ où $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$. Montrer que $\mathbb{F}_q(x)^G = \mathbb{F}_q\left(\frac{(x^{q^2}-x)^{q+1}}{(x^q-x)^{q^2+1}}\right)$.

c) Soit $H \leqslant G$ le sous-groupe des automorphismes de la forme $x \mapsto ax + b$, $a \in \mathbb{F}_q^\times$, $b \in \mathbb{F}_q$. Montrer que $\mathbb{F}_q(x)^H = \mathbb{F}_q((x^q - x)^{q-1})$.

d) Soit $H' \leqslant h$ le sous-groupe des automorphismes de la forme $x \mapsto x + b$, $b \in \mathbb{F}_q$. Montrer que $\mathbb{F}_q(x)^{H'} = \mathbb{F}_q((x^q - x))$.