

## IX

- Exercice 1** a) Soit  $(x, y) \in \mathbb{Q}^2$  tel que  $y^2 = x^3 - 2$ . Déterminer l'intersection de la courbe d'équation  $y^2 = x^3 - 2$  avec sa tangente en  $(x, y)$ .
- b) On pose  $(x_0, y_0) := (3, 5)$  et par récurrence  $x_{n+1} = \frac{x_n^4 + 16x_n}{4y_n^2}$ ,  $y_{n+1} = \frac{-x_n^6 + 40x_n^3 + 32}{8y_n^2}$ . Montrer que l'on obtient des points deux à deux distincts.
- c) En déduire que l'équation  $y^2 = x^3 - 2$  a une infinité de solutions rationnelles.

**Exercice 2**

- 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 3** 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  $\leq 4$ .
- b) Déterminer les polynômes 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 4** 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 5** 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  $k \leq K \leq k(x)$  tel que  $k \neq K$  est de la forme  $K = k(p/q)$  pour un certain  $p/q \in k(x)$  (indication : soit  $f = T^d + a_1T^{d-1} + \dots + a_d$  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 6** Soit  $f := Y^2 - X^3 + X$ . Montrer que  $\text{Frac}\mathbb{C}[X, Y]/(f)$  n'est pas isomorphe à un corps de la forme  $\mathbb{C}(t)$  (indication : supposons que  $\mathbb{C}(x, y) = \mathbb{C}(t)$  avec  $y^2 = x^3 - x$ ,  $x, y$  non constants ; montrer que quitte à remplacer  $t$  par  $\frac{\alpha t + \beta}{\gamma t + \delta}$ , avec  $\alpha\delta - \beta\gamma \neq 0$ , on peut supposer  $x(t) = \frac{at^2 + b}{ct^2 + d}$  pour certains  $a, b, c, d \in \mathbb{C}$ . Obtenir alors une contradiction).

**Exercice 7** 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 forme  $x \mapsto ax + b/cx + d$  où  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_q)$ . Montrer que  $\mathbb{F}_q(x)^G = \mathbb{F}_q\left(\frac{(x^q - x)^{q+1}}{(x^q - x)^{q^2 + 1}}\right)$ .

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

**Exercice 8**

a) Montrer qu'il existe  $i \in \mathbb{F}_9$  tel que  $i^2 + 1 = 0$ . Montrer que  $\mathrm{PSL}_2(\mathbb{F}_9)$  contient un sous-groupe  $H$  isomorphe à  $\mathfrak{A}_5$  (indication : utiliser la présentation  $\mathfrak{A}_5 = \langle x, y : x^2 = y^3 = (xy)^5 = 1 \rangle$  et considérer les matrices :

$$\left( \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right), \left( \begin{array}{cc} 1 & i-1 \\ 0 & 1 \end{array} \right).$$

b) En déduire, en considérant l'action de  $\mathrm{PSL}_2(\mathbb{F}_9)$  sur  $\mathrm{PSL}_2(\mathbb{F}_9)/H$  que :

$$\mathrm{PSL}_2(\mathbb{F}_9) \simeq \mathfrak{A}_6 .$$

**Exercice 9** Montrer que les groupes simples  $\mathfrak{A}_8$  et  $\mathrm{PSL}_3(\mathbb{F}_4)$  ont même cardinal mais ne sont pas isomorphes (indication : en utilisant la forme réduite de Jordan des matrices, montrer que dans  $\mathrm{PSL}_3(\mathbb{F}_4)$  les éléments d'ordre 2 sont conjugués).