Corps finis.

Exercice 1. Décrire les éléments des anneaux suivants et en dresser les tables d'addition et de multiplication :

$$\mathbf{F}_2[X]/(X^2+1)\ ;\ \mathbf{F}_2[X]/(X^2+X+1)\ ;\ \mathbf{F}_2[X]/(X^3+X+1).$$

Lesquels de ces anneaux sont-ils des corps ?

Exercice 2. Pour quels entiers $1 \leq n \leq 100$ existe-t-il un corps de cardinal n ?

Exercice 3. Soit $P = X^4 + X + 1 \in \mathbf{F}_2[X]$. On note $\mathbf{K} = \mathbf{F}_2[X]/(P)$ et $\alpha = \mathrm{cl}(X) \in \mathbf{K}$.
1. Montrer que $\mathbf{K}$ est un corps. Quelle est sa caractéristique ?
Donner une base du $\mathbf{F}_2$-espace vectoriel $\mathbf{K}$. Quel est le cardinal de $\mathbf{K}$?
2. Quel est l'inverse de l'élément $1 + \alpha + \alpha^2$ dans le groupe multiplicatif $\mathbf{K}^*$?
3. Montrer que α est une racine primitive de l'unité de $\mathbf{K}$.

Exercice 4. Soit $P = X^3 - X + 1 \in \mathbf{F}_3[X]$. On note $\mathbf{K} = \mathbf{F}_3[X]/(P)$ et $\alpha = \mathrm{cl}(X) \in \mathbf{K}$.
1. Montrer que $\mathbf{K}$ est un corps. Quelle est sa carctéristique ?
Donner une base du $\mathbf{F}_3$-espace vectoriel $\mathbf{K}$. Quel est le cardinal de $\mathbf{K}$?
2. Quels sont les ordres (multiplicatifs) possibles des éléments de $\mathbf{K}^*$? De $\mathbf{K}^* \backslash \mathbf{F}_3$?
3. Le but de cette question est de montrer que α est une racine primitive de l'unité de $\mathbf{K}$.
  a) Montrer que $\alpha^{13} = -1$ si et seulement si P divise le polynôme $X(X-1)^4 + 1$ dans $\mathbf{F}_3[X]$.
  b) Conclure.
4. Le polynôme $Q = X^4 + X^3 + X^2 + X + 1$ a-t-il des racines dans $\mathbf{K}[X]$?

Exercice 5. Soit $P = X^2 + X + 2 \in \mathbf{F}_5[X]$. On note $\mathbf{K} = \mathbf{F}_5[X]/(P)$ et $\alpha = \mathrm{cl}(X) \in \mathbf{K}$.
1. Montrer que $\mathbf{K}$ est un corps. Quelle est sa caractéristique ?
Donner une base du $\mathbf{F}_5$-espace vectoriel $\mathbf{K}$. Quel est le cardinal de $\mathbf{K}$?
2. Exprimer toutes les puissances distinctes de α dans la base décrite ci-dessus. Quel est l'ordre de α dans le groupe $\mathbf{K}^*$?
3. Quels sont les éléments $a \in \mathbf{K}$ tels que $a^5 = a$? En déduire que si un polynôme $Q \in \mathbf{F}_5[X]$ admet une racine $a \in \mathbf{K}$, alors a^5 est aussi racine de Q.
4. Montrer que pour tout $a \in \mathbf{K}$, on a : $a + a^5 \in \mathbf{F}_5$ et $a \times a^5 \in \mathbf{F}_5$. En déduire le polynôme minimal de a dans $\mathbf{F}_5[X]$.
5. Factoriser le polynôme $X^{25} - X$ dans $\mathbf{F}_5[X]$ et donner les racines dans $\mathbf{K}$ de chaque facteur.

Exercice 6. Soit $\mathbf{K}$ un corps fini de caractéristique $p > 3$, et soit $P = X^2 - X + 1 \in \mathbf{K}[X]$.
1. Soit $a \in \mathbf{K}$. Montrer que a est une racine de P si et seulement si a est d'ordre 6 dans $\mathbf{K}^*$.
2. En déduire une condition nécessaire et suffisante sur $b \in \mathbf{K}$ pour que b soit racine du polynôme $Q = X^4 - X^2 + 1$.
3. Montrer que Q a 0 ou 4 racines distinctes dans $\mathbf{K}$.

4. Qu'en est-il pour $\mathbf{K} = \mathbf{F}_{73}$? $\mathbf{K} = \mathbf{F}_{89}$?
5. Donner l'exemple d'un corps $\mathbf{K}$ dans lequel P possède deux racines distinctes mais Q n'a pas de racine.

Exercice 7. Soit $P = X^3 + X^2 + X - 1 \in \mathbf{F}_5[X]$. On note $\mathbf{K} = \mathbf{F}_5[X]/(P)$ et $\alpha = \mathrm{cl}(X) \in \mathbf{K}$.
1. Montrer que $\mathbf{K}$ est un corps. Quelle est sa caractéristique ?
Donner une base du $\mathbf{F}_5$-espace vectoriel $\mathbf{K}$. Quel est le cardinal de $\mathbf{K}$?
2. Quels sont les ordres possibles des éléments de $\mathbf{K}^*$? De $\mathbf{K}^* \backslash \mathbf{F}_5$?
3. Combien existe-t-il de racines primitives de l'unité dans $\mathbf{K}$?
4. Montrer, sans effectuer de calculs, que α^4 est d'ordre 31. En déduire une racine primitive de l'unité de $\mathbf{K}$. Quel est son polynôme minimal ?

Exercice 8. **1.** Donner la liste des polynômes unitaires irréductibles de degré 2 de $\mathbf{F}_3[X]$.
2. Soit $P = X^4 + X - 1 \ \in \mathbf{F}_3[X]$. On pose $\mathbf{K} = \mathbf{F}_3[X]/(P)$, et $\alpha = \mathrm{cl}(X) \in \mathbf{K}$.
  a) Montrer que $\mathbf{K}$ est un corps. Quelle est sa caractéristique ?
  b) Donner une base du $\mathbf{F}_3$-espace vectoriel $\mathbf{K}$. Quel est le cardinal de $\mathbf{K}$?
3. On s'intéresse ici au groupe multiplicatif $\mathbf{K}^*$.
  a) Quels sont les ordres possibles des éléments de $\mathbf{K}^*$? De $\mathbf{K}^* \backslash \mathbf{F}_3$?
  b) Combien le corps $\mathbf{K}$ admet-il de racines primitives de l'unité ?
4. On cherche ici à montrer que α est une racine primitive de l'unité dans $\mathbf{K}$.
  a) Donner une condition nécessaire et suffisante sur α^{40} pour que α soit une racine primitive de l'unité dans $\mathbf{K}$.
  b) Calculer α^{13} (on pourra calculer α^4 puis α^{12}).
  c) Calculer α^{40} et conclure.
5. On cherche ici à factoriser le polynôme P dans le corps $\mathbf{K}$.
  a) Montrer que $\alpha,\ \alpha^3,\ \alpha^9,\ \alpha^{27}$ sont des éléments de $\mathbf{K}$ deux à deux distincts.
  b) Montrer que pour tout entier naturel i on a : $P(X^{3^i}) = (P(X))^{3^i}$
  (On pourra raisonner par récurrence sur i.)
  c) Donner la décomposition de P en facteurs irréductibles dans $\mathbf{K}[X]$.
  d) En déduire les racines dans $\mathbf{K}$ du polynôme $P_1 = -X^4 + X^3 + 1$.
6. **a)** Quelles sont les racines dans $\mathbf{K}$ du polynôme $Q = X^4 + X^3 + X^2 + X + 1$?
  b) Même question avec $R = X^6 + X^5 + X^4 + X^3 + X^2 + X + 1$.

Exercice 9. Alice et Bob décident d'utiliser le protocole de **Diffie-Helman**. Ils rendent public le couple $(\mathbf{K}, \alpha)$ de l'exercice **4.** Alice choisit $a = 9$ et transmet α^9 à Bob. Ce dernier choisit un entier b et renvoie à Alice $\alpha^b = 2 + \alpha + 2\alpha^2$.
1. Quelle est la clef secrète d'Alice et Bob ?
2. Alice souhaite faire passer à Bob le message $M = 2 + \alpha^2$. Que transmet-elle ?
3. En réponse, elle reçoit 2α. Quel était le message de Bob ?

Exercice 10. Utilisant l'exercice **3.**, Alice rend publics le corps $\mathbf{K}$, la racine primitive de l'unité $\alpha \in \mathbf{K}$ et l'élément $1 + \alpha^2 \in \mathbf{K}$ (correspondant ainsi au triplet $(\mathbf{K}, g, g^e)$ du cours). Bob envoie des messages à Alice en utilisant l'algorithme de **El Gamal**.
1. Bob veut coder le messge $M = 1 + \alpha$ en utilisant $x = 3$. Que transmet-il à Alice ?
2. Même question avec $M = \alpha + \alpha^3$ et $x = 4$.
3. Vous décidez de casser le code d'Alice. Ceci fait, vous interceptez le message $(\alpha^3, \alpha^3 + \alpha^2 + \alpha)$, c'est-à-dire le couple (g^x, Mg^{xe}). Quel était le message M de Bob ?