Corps finis - exercices

1 Définition et construction

Exercice 1. Soit $q = p^m$. Montrer que le produit des éléments de $\mathbb{F}_q^*$ vaut -1.

Exercice 2. Calculer les cardinaux de $\mathrm{GL}_n(\mathbb{F}_q)$ et de $\mathrm{SL}_n(\mathbb{F}_q)$.

Exercice 3. [Retour d'oraux] Construire le corps à 4 éléments ainsi que sa table de multiplication.

Exercice 4. [Ortiz, III.10]

1. Donner l'ordre des éléments non nuls de $\mathbb{F}_4$ et leur polynôme minimal sur $\mathbb{F}_2$.
2. (a) Construire un corps fini $\mathbb{F}_8$ de cardinal 8. Donner l'ordre des éléments non nuls et leur polynôme minimal sur le corps premier. Déterminer tous les sous-corps de $\mathbb{F}_8$.
   (b) Vérifier que le polynôme cyclotomique Φ_7 est réductible sur $\mathbb{F}_2$.
3. (a) Construire un corps fini $\mathbb{F}_{16}$ de cardinal 16 en utilisant un polynôme irréductible sur $\mathbb{F}_2$. Donner l'ordre des éléments non nuls et leur polynôme minimal sur le corps premier. Déterminer tous les sous-corps de $\mathbb{F}_{16}$.
   (b) Construire un corps fini $\mathbb{F}'_{16}$ de cardinal 16 en utilisant un polynôme irréductible sur le corps $\mathbb{F}_4$ de la question 1. Donner une base de $\mathbb{F}'_{16}$ sur $\mathbb{F}_2$. Construire à l'aide du théorème de factorisation par un anneau quotient un isomorphisme de $\mathbb{F}_{16}$ sur $\mathbb{F}'_{16}$.
4. (a) Construire un corps fini $\mathbb{F}_9$ de cardinal 9 en utilisant le polynôme irréductible $X^2+1 \in \mathbb{F}_3[X]$. Donner l'ordre des éléments non nuls et leur polynôme minimal sur le corps premier.
   (b) Montrer que le quotient de l'anneau des entiers de Gauss $\mathbb{Z}[i]$ par l'idéal principal (3) est un corps de cardinal 9. Expliciter un isomorphisme du corps $\mathbb{F}_9$ construit à la question précédente sur $\mathbb{Z}[i]/(3)$

Exercice 5. Définition : On dit qu'une extension de corps $k \subset \bar{k}$ est une clôture algébrique si :

1. Tout élément $x \in \bar{k}$ est algébrique sur k, i.e. il existe une polynôme $P \in k[X]$ tel que $P(x) = 0$;
2. Tout polynôme $P \in \bar{k}[X]$ est totalement décomposé dans $\bar{k}$.

Soit p un nombre premier. Montrez alors que

$$\overline{\mathbb{F}}_p := \bigcup_{n \geqslant 1} \mathbb{F}_{p^{n!}}$$

est une clôture algébrique de $\mathbb{F}_p$.

Exercice 6. Montrez que $\mathrm{PGL}_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ et $\mathrm{PGL}_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$.

2 Structure algébrique interne

Exercice 7. Soit $K = \mathbb{F}_4$ et $L = \mathbb{F}_{16}$ les corps respectivement à 4 et 16 éléments. Montrer que L est une extension de degré 2 de K qui peut s'écrire $L = K(\alpha)$ où α est un élément d'ordre 5 de L^* (ici α n'est donc pas un générateur de L^*).

Exercice 8. Montrer les isomorphismes suivant et donner un générateur du groupe des inversibles des corps en question :

1. $\mathbb{F}_4 \simeq \mathbb{F}_2[X]/(X^2 + X + 1)$;
2. $\mathbb{F}_8 \simeq \mathbb{F}_2[X]/(X^3 + X + 1)$;
3. $\mathbb{F}_9 \simeq \mathbb{F}_3[X]/(X^2 + X - 1)$

Exercice 9. Soit n un entier tel que, pour tout p premier sauf éventuellement un nombre fini, n est un carré modulo p. Montrer que n est un carré dans $\mathbb{N}$.

Exercice 10. Montrer l'existence d'une infinité de nombres premiers $p \equiv -1 \bmod 12$.

Exercice 11.

1. Le nombre 2 est-il un carré dans $\mathbb{F}_5$? Montrer que $X^2 + X + 1$ est irréductible sur $\mathbb{F}_5$.
2. Soit $P(X) \in \mathbb{F}_5[X]$ un polynôme unitaire irréductible de degré deux. Montrer que le quotient
$$\frac{\mathbb{F}_5[X]}{(P(X))}$$
est isomorphe au corps $\mathbb{F}_{25}$ et que P a deux racines dans $\mathbb{F}_{25}$.
3. On note α une racine de $X^2 + X + 1$ dans $\mathbb{F}_{25}$. Montrer que tout $\beta \in \mathbb{F}_{25}$ peut s'écrire $a\alpha + b$ avec a et b dans $\mathbb{F}_5$.
4. Soit $P = X^5 - X + 1$. Montrer que pour tout $\beta \in \mathbb{F}_{25}$, on a $P(\beta) \neq 0$. En déduire que P est irréductible sur $\mathbb{F}_5$.P est-il irréductible sur $\mathbb{Q}$?

Exercice 12. Soit p un nombre premier impair.

1. Soit ξ une racine 8e primitive de l'unité dans une extension de $\mathbb{F}_p$, montrer que $\xi + \xi^{-1}$ est une racine carrée de 2.
2. En utilisant la question précédente, montrer que 2 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \bmod 8$.

3 Polynômes irréductibles

Exercice 13.

1. Donner tous les polynômes irréductibles de degré inférieur à 4 sur $\mathbb{F}_2$.
2. Quelle est la factorisation sur $\mathbb{F}_4$ d'un polynôme de $\mathbb{F}_2[X]$ irréductible de degré 4 ?
3. Déduire des questions précédentes, le nombre de polynômes irréductibles de degré 2 sur $\mathbb{F}_4$.
4. Expliciter les polynômes irréductibles de degré 2 sur $\mathbb{F}_4$.

Exercice 14. Montrer que $X^4 + 1$ est irréductible sur $\mathbb{Q}$ mais réductible sur chacun des $\mathbb{F}_p$.

Exercice 15. On considère le polynôme $Q(X) = X^9 - X + 1$ sur $\mathbb{F}_3$.

1. Montrer que le polynôme Q n'a pas de racines dans $\mathbb{F}_3, \mathbb{F}_9$.
2. Montrer que $\mathbb{F}_{27} \simeq \frac{\mathbb{F}_3[X]}{(X^3-X-1)}$.
3. Montrer que toute racine $\alpha \in \mathbb{F}_{27}$ du polynôme $X^3 - X - 1$ est une racine du polynôme Q.
4. Déterminer toutes le racines de Q dans $\mathbb{F}_{27}$.
5. Factoriser le polynôme Q sur le corps $\mathbb{F}_3$.

Exercice 16. Soit k un corps fini de caractéristique p et a un élément de k. Montrer que le polynôme $X^p - X - a$ est irréductible dans $k[X]$ si et seulement s'il n'a pas de racine.

Exercice 17. Soit $n \in \mathbb{N}$ et p un nombre premier tel que $\mathrm{pgcd}(p, n) = 1$. Montrer que le polynôme cyclotomique ϕ_n est irréductible sur $\mathbb{F}_p$ si et seulement si p est un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$.

Exercice 18.

1. Factoriser le polynôme $P = X^5 + X^4 + 1$ sur $\mathbb{F}_2$.
2. Factoriser le polynôme $X^6 + 7$ sur $\mathbb{F}_{11}$.