Agrégation Externe
Corps finis

On pourra consulter les ouvrages suivants.

P. Boyer, J. J. Risler : *Algèbre pour la licence 3. Groupes, anneaux, corps.* Dunod (2006).

F. Combes — *Algèbre et géométrie.* Bréal (2003).

J. P. Escoffier. *Toute l'algèbre de la licence.* Dunod (2006).

S. Francinou, H. Gianella, S. Nicolas : *Exercices de mathématiques. Oraux X-ENS. Algèbre 1.* Cassini (2001).

S. Francinou, H. Gianella. *Exercices de mathématiques pour l'agrégation. Algèbre 1.* Masson (1994).

F. Liret. *Arithmétique.* Dunod (2011).

D. Perrin. *Cours d'algèbre.* Ellipses (1996).

E. Ramis, C. Deschamps, J. Odoux. *Cours de Mathématiques Spéciales. Volumes 1 et 2.* Masson (1974 et 1995).

A. Szpirglas. *Mathématiques L3. Algèbre.* Pearson (2009).

P. Tauvel. *Corps comutatifs et théorie de Galois.* Calvage et Mounet (2008).

1 Énoncé

Définition 1 *Un corps est un anneau commutatif unitaire dans lequel tout élément non nul est inversible.*

Un corps est donc, a priori, commutatif.

Plutôt de parler de « corps non commutatif », on préfère parler d'anneau à division ou de corps gauche.

Définition 2 *Un anneau à division (ou corps gauche) est un anneau unitaire dans lequel tout élément non nul est inversible.*

Le théorème de Wedderburn nous dit qu'un anneau à division fini est commutatif ce qui justifie l'appellation « corps fini ».

Un anneau à division est intègre.

L'ensemble :

$$\mathbb{H} = \left\{ \begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix} \mid (a, b) \in \mathbb{C}^2 \right\}$$

(où $\overline{a}$ est le nombre complexe conjugué de a) est un anneau à division non commutatif (corps gauche des quaternions de Hamilton).

Pour tout nombre premier $p \geq 2$, $\mathbb{F}_p = \dfrac{\mathbb{Z}}{p\mathbb{Z}}$ désigne le corps commutatif des classes résiduelles modulo p.

Si $\mathbb{K}$ est un corps, le plus petit sous-corps $\mathbb{K}_0$ de $\mathbb{K}$ est son sous-corps premier.

Si $\mathbb{K}, \mathbb{L}$ sont deux corps commutatifs tels que $\mathbb{K} \subset \mathbb{L}$, on dit alors que $\mathbb{L}$ est une extension de $\mathbb{K}$.

Une telle extension est une algèbre sur $\mathbb{K}$. Sa dimension $\dim_{\mathbb{K}} (\mathbb{L})$ en tant que $\mathbb{K}$-espace vectoriel est notée $[\mathbb{L} : \mathbb{K}]$ et appelée degré de l'extension $\mathbb{L}$ sur $\mathbb{K}$.

Dans le cas où ce degré est fini, on dit que $\mathbb{L}$ est une extension finie de $\mathbb{K}$.

Pour tout ω dans $\mathbb{L}$, on note :

$$\mathbb{K}[\omega] = \{P(\omega) \mid P \in \mathbb{K}[X]\}$$

et on désigne par $\mathbb{K}(\omega)$ le plus petit sous-corps de $\mathbb{L}$ qui contient $\mathbb{K}$ et ω.

On dit qu'une extension $\mathbb{L}$ de $\mathbb{K}$ est un corps de rupture d'un polynôme non constant $P \in \mathbb{K}[X]$, si le polynôme P a une racine ω dans $\mathbb{L}$ telle que $\mathbb{L} = \mathbb{K}[\omega]$.

On dit qu'un élément ω de $\mathbb{L}$ est algébrique sur $\mathbb{K}$ s'il existe un polynôme non nul P dans $\mathbb{K}[X]$ tel que $P(\omega) = 0$.

L'anneau $\mathbb{K}[X]$ étant principal, pour tout élément ω de $\mathbb{L}$ qui est algébrique sur $\mathbb{K}$, il existe un unique polynôme unitaire P_ω dans $\mathbb{K}[X]$ tel que :

$$\{P \in \mathbb{K}[X] \mid P(\omega) = 0\} = (P_\omega)$$

P_ω est le polynôme minimal de ω et son degré est le degré de ω sur $\mathbb{K}$.

Le polynôme minimal de ω est aussi l'unique polynôme unitaire irréductible de $\mathbb{K}[X]$ qui annule ω.

– I – Résultats préliminaires sur les corps

Pour cette partie, $(\mathbb{K}, +, \cdot)$ est un corps.

1. Soient $\mathbb{K}, \mathbb{L}$ deux corps. Montrer que tout morphisme de corps σ de $\mathbb{K}$ dans $\mathbb{L}$ est injectif.
2. Montrer qu'un anneau commutatif et unitaire qui est fini est intègre si, et seulement si, c'est un corps.

3. Montrer que tout sous-groupe fini du groupe multiplicatif $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ d'un corps (commutatif) $\mathbb{K}$ est cyclique.
   En particulier, si $\mathbb{K}$ est un corps fini (donc commutatif), $\mathbb{K}^*$ est alors cyclique.
4. Soit $\mathbb{K}$ un corps fini à q éléments. Que dire des sous groupes de $\mathbb{K}^*$?
5. Soit $P \in \mathbb{K}[X]$ un polynôme unitaire de degré $n \geq 1$.
   (a) Montrer que l'algèbre $\dfrac{\mathbb{K}[X]}{(P)}$ est de dimension n et que $\left(\overline{X^k}\right)_{0 \leq k \leq n-1}$ en est une base.
   (b) Montrer que les assertions suivantes sont équivalentes :
      i. $\dfrac{\mathbb{K}[X]}{(P)}$ est un corps ;
      ii. l'anneau $\dfrac{\mathbb{K}[X]}{(P)}$ est intègre ;
      iii. le polynôme P est irréductible.
6.
   (a) Soit $P \in \mathbb{K}[X]$ un polynôme unitaire irréductible de degré $n \geq 1$.
   Montrer que $\dfrac{\mathbb{K}[X]}{(P)}$ est un corps de rupture de P et que P est le polynôme minimal de $\omega = \overline{X}$ sur $\mathbb{K}$.
   (b) Montrer que, pour tout polynôme $Q \in \mathbb{K}[X]$ de degré $n \geq 1$, il existe un corps de rupture $\mathbb{L}$ de Q tel que $[\mathbb{L} : \mathbb{K}] \leq n$.
7. Soit $Q \in \mathbb{K}[X]$ un polynôme de degré $n \geq 1$.
   Montrer si Q et Q' sont premiers sont entre eux, le polynôme Q est alors sans facteur carré dans sa décomposition en produit de polynômes irréductibles.
   La réciproque est-elle vraie ?
8. Soient $m \in \mathbb{N}^*$ et p un nombre premier qui ne divise pas m.
   Montrer que dans $\mathbb{F}_p[X]$, le polynôme $Q_m(X) = X^m - 1$ est sans facteur carré dans sa décomposition en produit de polynômes irréductibles.

– II – Caractéristique d'un corps

Pour cette partie, $(\mathbb{K}, +, \cdot)$ est un corps (commutatif).
L'application :

$$\begin{array}{rccc} \varphi : & \mathbb{Z} & \to & \mathbb{K} \\ & n & \mapsto & n \cdot 1 \end{array}$$

est l'unique morphisme d'anneaux de $\mathbb{Z}$ dans $\mathbb{K}$.
Son noyau étant un idéal de l'anneau principal $\mathbb{Z}$, il existe un unique entier naturel p tel que :

$$\ker(\varphi) = \{n \in \mathbb{Z} \mid n \cdot 1 = 0\} = p\mathbb{Z}$$

Définition 3 *L'entier p ainsi défini est la caractéristique de* $\mathbb{K}$.

On note $\mathrm{caract}(\mathbb{K})$ cette caractéristique.

1. Montrer que si $\mathrm{caract}(\mathbb{K}) = 0$, le sous-corps premier $\mathbb{K}_0$ de $\mathbb{K}$ est alors infini isomorphe à $\mathbb{Q}$ (donc $\mathbb{K}$ est infini) et dans le cas contraire, cette caractéristique est un nombre premier $p \geq 2$ et $\mathbb{K}_0$ est fini isomorphe à $\mathbb{F}_p$.
2. Soient $\mathbb{K} \subset \mathbb{L}$ deux corps. Montrer qu'ils sont de même caractéristique.

3. Donner un exemple de corps infini de caractéristique finie.
4. Montrer que si $\mathbb{K}$ est fini, il est alors de cardinal p^n, où $p \geq 2$ est un nombre premier.
5. Soient $\mathbb{K}$ un corps de caractéristique $p \geq 2$, n, r deux entiers naturels non nuls et $\lambda_1, \cdots, \lambda_r$ des éléments de $\mathbb{K}$. Montrer que :

$$\left(\sum_{i=1}^{r} \lambda_i \right)^{p^n} = \sum_{i=1}^{r} \lambda_i^{p^n}$$

6. Soit $\mathbb{F}_{p^n}$ un corps fini à p^n éléments ($p \geq 2$ premier et $n \geq 1$).
   (a) Montrer que tout sous-corps $\mathbb{K}$ de $\mathbb{F}_{p^n}$ est de cardinal p^d où d est un diviseur de n.
   (b) Réciproquement, montrer que pour tout diviseur d de n, il existe un unique sous-corps de $\mathbb{F}_{p^n}$ de cardinal p^d, à savoir le corps :

$$\mathbb{K} = \left\{ x \in \mathbb{F}_{p^n} \mid x^{p^d} = x \right\}$$

– III – Polynômes irréductibles dans $\mathbb{F}_p[X]$ et construction de corps finis

Pour cette partie, $p \geq 2$ est un nombre premier.

Pour tout entier $n \in \mathbb{N}^*$, on note $\mathcal{U}_n(p)$ l'ensemble de tous les polynômes unitaires irréductibles de degré n dans $\mathbb{F}_p[X]$ et $I_n(p)$ le cardinal de $\mathcal{U}_n(p)$.

L'ensemble $\mathcal{U}_n(p)$ peut, a priori, être vide.

Pour tout entier $n \in \mathbb{N}^*$, on note $\mathcal{D}_n$ l'ensemble de tous les diviseurs de n dans $\mathbb{N}^*$.

En notant $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ la décomposition en facteurs premiers d'un entier $n \geq 2$ où $r \geq 1$, les p_i sont premiers deux à deux distincts et les α_i entiers naturels non nuls, on définit la fonction μ de Möbius par :

$$\forall n \in \mathbb{N}^*,\ \mu(n) = \begin{cases} 1 \text{ si } n = 1 \\ (-1)^r \ \text{ si } n = \prod_{i=1}^{r} p_i \text{ (i. e. } n \text{ est sans facteurs carrés)} \\ 0 \text{ sinon} \end{cases}$$

1. Le produit de convolution (de Dirichlet) de deux suites réelles u, v de $\mathbb{R}^{\mathbb{N}^*}$ est la suite $u * v$ définie par :

$$\forall n \in \mathbb{N}^*,\ (u * v)(n) = \sum_{d \in \mathcal{D}_n} u(d)\, v\left(\frac{n}{d}\right)$$

   On vérifie facilement que l'ensemble $\mathbb{R}^{\mathbb{N}^*}$ muni des lois $+$ et $*$, est un anneau commutatif unitaire.

   (a) En notant e le neutre de $\mathbb{R}^{\mathbb{N}^*}$ pour la loi $*$ et ω la suite constante égale à 1 (i. e. $\omega(n) = 1$ pour tout $n \in \mathbb{N}^*$), montrer que $\mu * \omega = e$, c'est-à-dire que :

$$\forall n \geq 1,\ \sum_{d \in \mathcal{D}_n} \mu(d) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ si } n \geq 2 \end{cases}$$

(b) Soient u, v dans $\mathbb{R}^{\mathbb{N}^*}$. Montrer que les assertions suivantes sont équivalentes :

$$\forall n \in \mathbb{N}^*,\ u(n) = \sum_{d \in \mathcal{D}_n} v(d) \tag{1}$$

et :

$$\forall n \in \mathbb{N}^*,\ v(n) = \sum_{d \in \mathcal{D}_n} \mu(d)\, u\left(\frac{n}{d}\right) \tag{2}$$

(formule d'inversion de Möbius).

2. Montrer que pour tout polynôme $P \in \mathcal{U}_n(p)$, l'anneau quotient $\dfrac{\mathbb{F}_p[X]}{(P)}$ est un corps fini de cardinal p^n, ce corps pouvant être muni d'une structure de $\mathbb{F}_p$-espace vectoriel de base $\left(\overline{X}^k\right)_{0 \leq k \leq n-1}$.
3. Calculer $I_1(p)$ et $I_2(p)$.
4. Donner tous les polynômes unitaires de degré 2 irréductibles dans $\mathbb{F}_2[X]$ et dans $\mathbb{F}_3[X]$.
5. Pour $p \geq 3$, montrer que le polynôme $X^2 + 1$ est irréductibles dans $\mathbb{F}_p[X]$ si, et seulement si, p est congru à 3 modulo 4.
6. Construire deux corps à 8 et 16 éléments respectivement. Donner un générateur du groupe $\mathbb{K}^*$ correspondant.
7. Soient n un entier naturel non nul et :

$$P_n(X) = X^{p^n} - X \in \mathbb{F}_p[X]$$

(a) Montrer que, pour tout $d \in \mathcal{D}_n$, tout polynôme $P \in \mathcal{U}_d(p)$ divise P_n.

(b) Réciproquement, montrer que s'il existe un polynôme $P \in \mathcal{U}_d(p)$ qui divise P_n, l'entier d est alors un diviseur de n.

(c) Montrer que le polynôme $P_n(X) = X^{p^n} - X$ est sans facteurs carrés dans $\mathbb{F}_p[X]$, puis que :

$$X^{p^n} - X = \prod_{d \in \mathcal{D}_n} \prod_{P \in \mathcal{U}_d(p)} P$$

et :

$$p^n = \sum_{d \in \mathcal{D}_n} d \cdot I_d(p)$$

(d) En déduire un algorithme de calcul des $I_n(p) = \mathrm{card}(\mathcal{U}_n(p))$.
Par exemple, calculer $I_q(p)$ et $I_{q^2}(p)$ pour $q \geq 2$ premier.

(e) Montrer que :

$$nI_n(p) = \sum_{d \in \mathcal{D}_n} \mu\left(\frac{n}{d}\right) p^d$$

(f) Montrer qu'il existe dans $\mathbb{F}_p[X]$ des polynômes irréductibles de degré n et que :

$$I_n(p) \underset{n \to +\infty}{\backsim} \frac{p^n}{n}$$

8. Donner tous les polynômes unitaires de degré 4 irréductibles dans $\mathbb{F}_2[X]$.
9. Soient n un entier naturel non nul, P un polynôme unitaire et irréductible de degré n dans $\mathbb{F}_p[X]$ et $\mathbb{F}_{p^n}$ le corps $\dfrac{\mathbb{F}_p[X]}{(P)}$.
On désigne par $\mathbb{K}$ un autre corps à p^n éléments.
Comme $\mathbb{K}$ est de caractéristique p, le corps $\mathbb{F}_p$ peut être identifié au sous-corps premier de $\mathbb{K}$ et un polynôme dans $\mathbb{F}_p[X]$ à un polynôme dans $\mathbb{K}[X]$.

(a) Montrer que le polynôme P est scindé à racines simples dans $\mathbb{K}[X]$.

(b) En déduire l'existence d'un isomorphisme de corps de $\mathbb{F}_{p^n}$ sur $\mathbb{K}$.

Donc, a un isomorphisme près, il n'existe qu'un seul corps à p^n éléments, c'est $\mathbb{F}_{p^n} = \dfrac{\mathbb{F}_p[X]}{(P)}$ où $P \in \mathcal{U}_n(p)$.

10. Montrer qu'un corps fini ne peut être algébriquement clos.
11. Montrer que si $\mathbb{K}$ est un corps fini alors toute application de $\mathbb{K}$ dans $\mathbb{K}$ est polynomiale.
12. On se donne un entier $n \geq 1$ et on note G le groupe des automorphismes de corps de $\mathbb{F}_{p^n}$.

(a) Montrer que l'application $\alpha : \lambda \mapsto \lambda^p$ est un automorphisme de corps de $\mathbb{F}_{p^n}$.

(b) Montrer que α est d'ordre n dans G.

(c) Montrer que G est un groupe cyclique engendré par α.

– IV – Carrés dans un corps fini

Pour tout nombre premier impair $p \geq 3$ et tout entier $n \geq 1$, en notant $q = p^n$, on désigne par $\mathbb{F}_q$ un corps fini de cardinal q et on s'intéresse à l'ensemble $P_2 = \left\{x^2 \mid x \in \mathbb{F}_q^*\right\}$ des carrés dans $\mathbb{F}_q^*$.

1. Montrer que :

(a) Il y a $\dfrac{q-1}{2}$ carrés et $\dfrac{q-1}{2}$ non carrés dans $\mathbb{F}_q^*$.

(b) $P_2 = \left\{x \in \mathbb{F}_q^* \mid x^{\frac{q-1}{2}} = 1\right\}$ et $\mathbb{F}_q^* \setminus P_2 = \left\{x \in \mathbb{F}_q^* \mid x^{\frac{q-1}{2}} = -1\right\}$ (les carrés de $\mathbb{F}_q^*$ sont les racines de $X^{\frac{q-1}{2}} - 1$ et les non carrés sont les racines de $X^{\frac{q-1}{2}} + 1$).

(c) Le produit de deux non carrés de $\mathbb{F}_{p^n}^*$ est un carré, le produit d'un carré et d'un non carré est un non carré.

(d) -1 est un carré dans $\mathbb{F}_q^*$ si, et seulement si, q est congru à 1 modulo 4 ;

(e) En déduire qu'il existe une infinité de nombres premiers de la forme $4m + 1$.

(f) Pour $q = p$, -1 est un carré dans $\mathbb{F}_p^*$ si, et seulement si, il existe deux entiers a, b non divisibles par p et premiers entre eux tels que p divise $a^2 + b^2$.

(g) En déduire qu'il existe une infinité de nombres premiers de la forme $8m + 5$.

2. Soient a, b dans $\mathbb{F}_q^*$. Montrer que pour tout $c \in \mathbb{F}_q$, il existe x, y dans $\mathbb{F}_q$ tels que $c = ax^2 + by^2$ (prenant $a = b = 1$, on en déduit que tout élément de $\mathbb{F}_q$ est somme de deux carrés).

3. Pour tout $a \in \mathbb{F}_p^*$, on définit le symbole de Legendre $\left(\dfrac{a}{p}\right)$ par :

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \text{ si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 \text{ sinon} \end{cases}$$

(a) Montrer que $a^{\frac{p-1}{2}} = \overline{\left(\dfrac{a}{p}\right)}$ dans $\mathbb{F}_p^*$.

(b) Montrer que le nombre de solutions dans $\mathbb{F}_p^*$ de l'équation $ax^2 = 1$ est $\left(\dfrac{a}{p}\right) + 1$.

(c) Montrer que le symbole de Legendre est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^*$ sur $\{-1, 1\}$.

4. n est entier naturel non nul.

(a) Montrer que l'application :

$$\begin{array}{rccc} \gamma : & GL_n(\mathbb{F}_p) & \to & \{-1,1\} \\ & A & \mapsto & \left(\dfrac{\det(A)}{p}\right) \end{array}$$

est l'unique morphisme de groupes non trivial de $GL_n(\mathbb{F}_p)$ sur $\{-1,1\}$.

(b) Soient $\mathbb{F}_{p^n}$ un corps fini à p^n éléments et ω un générateur du groupe cyclique $\mathbb{F}_{p^n}^*$. Calculer la signature de la permutation $\sigma : x \in \mathbb{F}_{p^n} \mapsto \omega x$.

(c) En notant, pour toute matrice $A \in GL_n(\mathbb{F}_p)$, par $\varepsilon(A)$ la signature de la permutation de $\mathbb{F}_p^n$ définie par A, montrer que :

$$\varepsilon(A) = \left(\frac{\det(A)}{p}\right)$$

(théorème de Frobénius-Zolotarev).

(d) En utilisant le théorème de Frobénius-Zolotarev, calculer $\left(\dfrac{2}{p}\right)$.

5. E est un $\mathbb{F}_q$-espace vectoriel de dimension $m \geq 1$ (avec $q = p^n$, où $p \geq 3$ est premier) et φ est une forme quadratique sur E de rang r compris entre 1 et m.

(a) Montrer qu'il existe une base de E dans laquelle la matrice de φ est de la forme :

$$D = \begin{pmatrix} I_{r-1} & 0 & 0 \\ 0 & \delta & 0 \\ 0 & 0 & 0_{n-r} \end{pmatrix}$$

avec $\delta = 1$ ou δ non carré dans $\mathbb{F}_q^*$.

(b) Pour φ non dégénérée, vérifier que $\delta = 1$ si, et seulement si, le discriminant de φ dans une base de E est un carré.

6. On se donne un entier impair $n = 2m+1 \geq 3$, on note $J = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ dans $\mathcal{M}_2(\mathbb{F}_q)$, $\alpha = (-1)^m$ dans $\mathbb{F}_q$ et est la forme quadratique de matrice :

$$A = \begin{pmatrix} J & 0 & \cdots & \cdots & 0 \\ 0 & J & \ddots & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & J & 0 \\ 0 & 0 & \cdots & 0 & \alpha \end{pmatrix} \in \mathcal{M}_n(\mathbb{F}_q)$$

dans la base canonique $\mathcal{B}_0$ de $E = \mathbb{F}_q^n$.

(a) Donner une expression de φ dans la base $\mathcal{B}_0$.

(b) Justifier l'existence d'une base $\mathcal{B}$ de E dans laquelle la matrice de φ est I_n.

(c) En désignant par Q l'ensemble des $x \in E$ tels que $Q(x) = 1$, montrer que :

$$\begin{aligned} \operatorname{card}(Q) &= \operatorname{card}\left\{ (x_k)_{1\leq k\leq n} \in \mathbb{F}_q^n \mid 2\sum_{k=1}^{m} x_{2k-1}x_{2k} + \alpha x_n^2 = 1 \right\} \\ &= \operatorname{card}\left\{ (y_k)_{1\leq k\leq n} \in \mathbb{F}_q^n \mid \sum_{k=1}^{n} y_k^2 = 1 \right\} \end{aligned}$$

7. Soient p, q deux nombres premiers impairs distincts et φ la forme quadratique sur $E = \mathbb{F}_q^p$ définie à la question précédente.

   (a) En utilisant la première expression de $\operatorname{card}(Q)$, montrer que :

   $$\operatorname{card}(Q) = q^{\frac{p-1}{2}} \left(\frac{(-1)^{\frac{p-1}{2}}}{q} \right) + q^{p-1}$$

   où $\left(\frac{(-1)^{\frac{p-1}{2}}}{q} \right)$ est le symbole de Legendre.

   (b) À tout entier k compris entre 0 et $p-1$, on associe l'application τ_k qui associe à tout entier relatif j le reste dans la division euclidienne de $k+j$ par p et on fait agir le groupe additif $(\mathbb{F}_p, +)$ sur l'ensemble :

   $$Q_2 = \left\{ (y_k)_{1 \leq k \leq p} \in \mathbb{F}_q^p \mid \sum_{k=1}^{p} y_k^2 = 1 \right\}$$

   par :

   $$\forall \left(\overline{k}, y\right) \in \mathbb{F}_p \times Q_2,\ \overline{k} \cdot y = \left(y_{\tau_k(1)}, \cdots, y_{\tau_k(p)}\right)$$

   Montrer que :

   $$\operatorname{card}(Q) = \left(1 + \left(\frac{p}{q}\right)\right) + Np$$

   où N est le nombre d'orbites non réduites à un point.

   (c) Déduire de tout cela que :

   $$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right)$$

   (formule de réciprocité quadratique).

8.

   (a) Soient α un entier supérieur ou égal à 2, m un entier impair compris entre 1 et $2^\alpha - 1$ et $q = 2^\alpha m + 1$.
   On suppose qu'il existe un nombre premier impair $p \geq 3$ ne divisant pas q tel que q ne soit pas un carré modulo p.
   Montrer que q est premier si, et seulement si, $p^{\frac{q-1}{2}} \equiv -1$ modulo q.

   (b) En utilisant le test de primalité de la question précédente, montrer qu'un entier de Fermat, $F_n = 2^{2^n} + 1$ où n est un entier naturel non nul, est premier si, et seulement si, $3^{\frac{F_n - 1}{2}}$ est congru à -1 modulo F_n.

– V – Algèbre linéaire sur un corps fini

E est un $\mathbb{F}_q$-espace vectoriel de dimension $n \geq 1$ (avec $q = p^r$, où $p \geq 2$ est premier).

1. Montrer que :

   $$\operatorname{card}(GL(E)) = \prod_{k=1}^{n} \left(q^n - q^{k-1}\right) = q^{\frac{n(n-1)}{2}} \prod_{j=1}^{n} \left(q^j - 1\right)$$

2. Soit F un $\mathbb{F}_q$-espace vectoriel de dimension $m \geq 1$.
   Montrer que les espaces vectoriels E et F sont isomorphes si, et seulement si, les groupes $GL(E)$ et $GL(F)$ sont isomorphes.

3. Montrer que si $\mathbb{L}$ est un corps tel que les groupes $GL_n(\mathbb{F}_q)$ et $GL_n(\mathbb{L})$ sont isomorphes, $\mathbb{L}$ est alors isomorphe à $\mathbb{F}_q$.
4. Montrer qu'un automorphisme $u \in GL(E)$ [resp. $u \in \mathcal{L}(E)$] est diagonalisable si, et seulement si, $u^{q-1} = Id$ [resp. $u^q = u$].
5.
   (a) Donner un exemple de p-Sylow de $GL_n(\mathbb{F}_q)$ pour $n \geq 2$.

   (b) Montrer que, tout groupe fini d'ordre $n \geq 1$ est isomorphe à un sous-groupe de $GL_n(\mathbb{F}_p)$.
   Indication : utiliser un théorème de Cayley et les matrices de permutations.

   (c) Rappeler comme le résultat précédent permet de montrer le premier théorème de Sylow : si G est un groupe d'ordre $p^\alpha m$ avec $\alpha \geq 1$ et p premier ne divisant pas m, il existe alors un p-Sylow de G.
6. On désigne par $\mathcal{J}_n(\mathbb{F}_q)$ l'ensemble de toutes les matrices de $\mathcal{M}_n(\mathbb{F}_q)$ nilpotentes d'ordre n. On fait agir par conjugaison le groupe $GL_n(\mathbb{F}_q)$ sur l'ensemble $\mathcal{M}_n(\mathbb{F}_q)$.

   (a) Montrer que $\mathcal{J}_n(\mathbb{F}_q)$ est l'orbite de la matrice $J_n = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$.

   (b) Montrer que le stabilisateur de J_n est $\mathbb{F}_q[J_n]_{n-1} \cap GL_n(\mathbb{F}_q)$, où $\mathbb{F}_q[J_n]_{n-1}$ est l'ensemble des matrices de la forme $P(J_n)$ où P est un polynôme dans $\mathbb{F}_q[X]$ de degré au plus égal à $n-1$.

   (c) En déduire que :
   $$\operatorname{card}(\mathcal{J}_n(\mathbb{F}_q)) = \prod_{k=1}^{n-1} \left(q^n - q^{k-1}\right)$$
7. En désignant par $DL(E)$ l'ensemble des $\mathbb{F}_q$-automorphismes de E qui sont diagonalisables, montrer que :
   $$\operatorname{card}(DL(E)) = \sum_{\substack{(n_1,\cdots,n_{q-1}) \in \mathbb{N}^{q-1} \\ n_1+\cdots+n_{q-1}=n}} \frac{\operatorname{card}(GL_n(\mathbb{F}_q))}{\operatorname{card}(GL_{n_1}(\mathbb{F}_q)) \cdots \operatorname{card}\left(GL_{n_{q-1}}(\mathbb{F}_q)\right)}$$
   avec la convention $\operatorname{card}(GL_0(\mathbb{F}_q)) = 1$.
   Indication : vérifier que $DL(E)$ est en bijection avec l'ensemble $\mathcal{F}$ des familles $(E_1, \cdots, E_{q-1})$ de sous-espaces vectoriels de E tels que $E = \bigoplus_{k=1}^{q-1} E_k$, puis utiliser une action du groupe $GL(E)$ sur l'ensemble des éléments de $\mathcal{F}$ tels que $\dim(E_k) = n_k$, où $(n_1, \cdots, n_{q-1})$ est fixé.
8.
   (a) Montrer que deux formes quadratiques non dégénérées φ et φ' sur E sont équivalentes si, et seulement si, pour toute base $\mathcal{B}$ de E, le rapport $\dfrac{\operatorname{Discr}_{\mathcal{B}}(\varphi')}{\operatorname{Discr}_{\mathcal{B}}(\varphi)}$ est un carré dans $\mathbb{F}_q^*$.

   (b) Montrer qu'il y a, dans l'espace vectoriel $Q(E)$ des formes quadratiques sur E, $2n+1$ classes d'équivalence, dont deux de formes quadratiques non dégénérées.