Leçon 123 - Corps finis. Applications.

Extrait du rapport de jury

La construction des corps finis doit être connue et une bonne maîtrise des calculs dans les corps finis est indispensable. Le calcul des degrés des extensions, le théorème de la base télescopique, les injections des divers $\mathbb{F}_q$ sont incontournables. La structure du groupe multiplicatif doit aussi être connue.
Des applications des corps finis (y compris pour $\mathbb{F}_q$ avec q non premier !) ne doivent pas être oubliées. Par exemple, l'étude de polynômes à coefficients entiers et de leur irréductibilité peut figurer dans cette leçon. L'étude des carrés dans un corps fini et la résolution d'équations de degré 2 sont des pistes intéressantes.
Les candidates et candidats peuvent aller plus loin en détaillant des codes correcteurs ou en étudiant l'irréductibilité des polynômes à coefficients dans un corps fini.

Présentation de la leçon

Je vais vous présenter la leçon 123 intitulée : "Corps finis.". La théorie des corps finis émerge avec les travaux arithmétiques de Gauss ainsi que les travaux sur les groupes de racines de Galois. Si le travail sur les corps s'est alors essentiellement concentré sur l'utilisation d'une structure si riche et de bon comportement, l'avènement de l'informatique et l'importance croissante de la cryptographie comme de la correction d'erreurs est un souffle nouveau pour l'étude, la compréhension et la manipulation des corps finis pour eux-mêmes.
Dans une première partie, on essaie de comprendre ce qu'est un corps fini et d'en construire. On commence d'abord avec des résultats théoriques utiles pour la suite sur la caractéristique d'un corps avec la notion de sous-corps premier, de caractéristique d'un corps et d'une description du sous-corps premier. On enchaîne ensuite avec les définitions et résultats généraux sur les extensions de corps avec la définition d'une extension de corps et de degré d'une extension ainsi que le théorème de la base télescopique qui est très utile en pratique. On introduit ensuite la notion d'élément algébrique et transcendant ainsi qu'une caractérisation très utilisée en pratique avant de finir cette partie avec l'existence et l'unicité du corps de rupture et de décomposition à l'isomorphisme près ainsi qu'en parlant brièvement de la clôture algébrique. Dans un deuxième point on s'intéresse à l'existence et l'unicité des corps finis. On montre d'abord qu'ils sont tous commutatifs (ce qui montre que l'hypothèse faite au départ n'est en rien restrictive) et que leur cardinal n'est pas quelconque avant de prouver que ces corps existent et sont uniques à l'isomorphisme près dès que leur cardinal est une puissance d'un nombre premier ainsi que deux méthodes de constructions du corps à 4 éléments. Enfin dans un dernier point on s'intéresse à la structure du groupe multiplicatif en montrant qu'il est cyclique et isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$ et qu'on peut appliquer le théorème de l'élément primitif grâce à ce résultat.
Dans une deuxième partie on s'intéresse cette fois-i aux propriétés sur les corps finis. Tout d'abord on s'intéresse à l'inclusion des corps finis avec le corollaire 30 qui permet de construire des trellis comme dans l'exemple 31 avant de passer sur le groupe des automorphismes de $\mathbb{F}_q$ en montrant qu'il est cyclique et engendré par le morphisme de Frobenius. Enfin dans un dernier point on s'intéresse aux carrés dans un corps fini ainsi qu'au symbole de Legendre. on commence par dénombrer les carrés dans un corps fini ainsi que quelques propriétés sur les carrés avant de donner la définition du symbole de Legendre ainsi que les théorèmes de Frobenius-Zolotarev et de réciprocité quadratique.
Dans une troisième partie on s'intéresse aux liens entre les polynômes et les corps finis. Tout d'abord on donne deux outils d'irréductibilité avec le critère d'Eisenstein et de réduction qui permettent de montrer en pratique que des polynômes sont irréductibles dans $\mathbb{Q}[X]$. Puis ensuite on regarde les polynômes irréductibles dans $\mathbb{F}_q[X]$ avec deux nouveaux critères qui concernent les degrés des extensions de corps qui permettent de montrer que des polynômes sont irréductibles dans des corps finis.
Enfin dans une dernière partie on s'intéresse au dénombrement sur les corps finis avec tout d'abord les polynômes irréductibles unitaires de degré n. On introduit pour cela

la fonction de Möbius qui nous permet de dénombrer ces polynômes et d'obtenir un équivalent de ce nombre en $+\infty$, ce qui au passage nous permet de retrouver le fait que les corps à p^n éléments existent toujours. On consacre un dernier point à l'étude des matrices dans un corps fini avec tous d'abord les cardinaux de $\mathrm{GL}_n(\mathbb{F}_q)$ et $\mathrm{SL}_n(\mathbb{F}_q)$ ainsi que de leurs centres avant de donner leurs groupes dérivés ainsi que quelques isomorphismes exceptionnels et enfin le dénombrement des endomorphismes nilpotents sur un corps fini.

Plan général

Cours détaillé

I Construction de corps finis

I.1 Caractéristique et extension de corps

Dans toute cette sous-partie, on considère $\mathbb{K}$ un corps commutatif quelconque.

Définition 1 : Sous-corps premier [Perrin, p.72] :
On appelle **sous-corps premier de** $\mathbb{K}$ le plus petit sous-corps de $\mathbb{K}$ (contenant l'élément $1_{\mathbb{K}}$).

On considère le morphisme d'anneaux :

$$\varphi : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{K} \\ n & \longmapsto & n \cdot 1_{\mathbb{K}} \end{array} \right.$$

Le noyau de φ est un idéal de $\mathbb{Z}$ et par le premier théorème d'isomorphisme, on a $\mathbb{Z}/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi) \subseteq \mathbb{K}$, donc $\operatorname{Ker}(\varphi)$ est un idéal premier de $\mathbb{Z}$ de la forme $p\mathbb{Z}$ avec $p \in \mathcal{P} \cup \{0\}$.

Définition 2 : Caractéristique d'un corps [Perrin, p.72] :
On appelle **caractéristique de** $\mathbb{K}$ le nombre $p \in \mathcal{P} \cup \{0\}$ qui est le générateur de $\operatorname{Ker}(\varphi)$ et on le note $\operatorname{car}(\mathbb{K})$.

Proposition 3 : [Perrin, p.72]
* $\operatorname{car}(\mathbb{K}) = 0$ si, et seulement si, le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Q}$.
* $\operatorname{car}(\mathbb{K}) > 0$ si, et seulement si, le sous-corps premier de $\mathbb{K}$ est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

Définition 4 : Extension de corps [Perrin, p.65] :
On considère $\mathbb{K}$ et $\mathbb{L}$ deux corps commutatifs quelconques.
On dit que $\mathbb{L}$ est une **extension de corps de** $\mathbb{K}$ lorsque $\mathbb{K} \subseteq \mathbb{L}$ et on la note $\mathbb{L}/\mathbb{K}$.

Définition 5 : Degré d'un extension de corps [Perrin, p.65] :
On considère une extension de corps $\mathbb{L}/\mathbb{K}$.
On appelle **degré de l'extension** $\mathbb{L}/\mathbb{K}$ la dimension de $\mathbb{L}$ vu comme $\mathbb{K}$-espace vectoriel et on la note $\dim_{\mathbb{K}} \mathbb{L}$ (ou encore $[\mathbb{L} : \mathbb{K}]$).

Exemple 6 :
* $\mathbb{C}$ est une extension de corps de $\mathbb{R}$ de degré 2.
* $\mathbb{Q}(i)$ est une extension de corps de $\mathbb{Q}$ de degré 2.
* $\mathbb{R}$ est une extension de corps de $\mathbb{Q}$ de degré infini (car $\mathbb{Q}$ est dénombrable).

Théorème 7 : Théorème de la base télescopique [Perrin, p.65] :
Soient $\mathbb{K}$, $\mathbb{L}$ et $\mathbb{M}$ trois corps commutatifs quelconques tels que $\mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{M}$.
Si $(e_i)_{i\in I}$ est une $\mathbb{K}$-base de $\mathbb{L}$ et $(f_j)_{j\in J}$ une $\mathbb{L}$-base de $\mathbb{M}$, alors $(e_i f_j)_{(i,j)\in I\times J}$ est une base de $\mathbb{M}$ en temps de $\mathbb{K}$-espace vectoriel.
On a alors en particulier : $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Définition 8 : Élément algébrique/transcendant [Perrin, p.66] :
On considère une extension de corps $\mathbb{L}/\mathbb{K}$, $\alpha \in \mathbb{L}$ ainsi que le morphisme de corps $\varphi : \mathbb{K}[T] \longrightarrow \mathbb{L}$ tel que $\varphi|_{\mathbb{K}} = \mathrm{Id}_{\mathbb{K}}$ et $\varphi(T) = \alpha$.
∗ Lorsque φ est injectif, il n'y a que le polynôme nul qui s'annule en α. On dit alors que α est **transcendant sur** $\mathbb{K}$.
∗ Lorsque φ n'est pas injectif, il existe $\mu_\alpha \in \mathbb{K}[T]$ non nul unitaire tel que $\mathrm{Ker}(\varphi) = (\mu_\alpha)$. On dit alors que α est **algébrique sur** $\mathbb{K}$ et que μ_α est le **polynôme minimal de** α **sur** $\mathbb{K}$.

Exemple 9 : [Perrin, p.66]
∗ Les nombres $\sqrt{2}$, i et $\sqrt[3]{2}$ sont algébriques sur $\mathbb{Q}$ de polynômes minimaux respectifs $X^2 - 2$, $X^2 + 1$ et $X^3 - 2$.
∗ Les nombres π et e sont transcendants sur $\mathbb{Q}$ (mais pas sur $\mathbb{R}$) [ADMIS].

Proposition 10 : Caractérisation des éléments algébriques [Perrin, p.66] :
Soient $\mathbb{L}/\mathbb{K}$ une extension de corps et $\alpha \in \mathbb{L}$.
Les assertions suivantes sont équivalentes :
∗ α est algébrique sur $\mathbb{K}$. ∗ On a $\mathbb{K}[\alpha] = \mathbb{K}(\alpha)$.
∗ On a $\dim_{\mathbb{K}} \mathbb{K}[\alpha] < +\infty$ (plus précisément, $\dim_{\mathbb{K}} \mathbb{K}[\alpha] = \deg(\mu_\alpha)$).
∗ Il existe un unique polynôme $\mu_\alpha \in \mathbb{K}[X]$ unitaire et irréductible dans $\mathbb{K}[X]$ tel que $\mu_\alpha(\alpha) = 0_{\mathbb{K}}$.
∗ $\mathbb{K}(\alpha) = \mathrm{Vect}_{\mathbb{K}}(1_{\mathbb{K}}, \alpha, \alpha^2, ..., \alpha^{\deg(\mu_\alpha)-1})$.

Définition 11 : Extension finie/algébrique [Perrin, p.67] :
On considère une extension de corps $\mathbb{L}/\mathbb{K}$.
On dit que $\mathbb{L}/\mathbb{K}$ est une extension :
∗ **finie** lorsque $[\mathbb{L} : \mathbb{K}] < +\infty$.
∗ **algébrique** lorsque tout élément de $\mathbb{L}$ est algébrique sur $\mathbb{K}$.

Définition 12 : Corps de rupture [Perrin, p.70] :
On considère $P \in \mathbb{K}[X]$ un polynôme irréductible dans $\mathbb{K}[X]$.
Une extension de corps $\mathbb{L}/\mathbb{K}$ est appelée **corps de rupture de** P **sur** $\mathbb{K}$ lorsque $\mathbb{L}$ est monogène $\mathbb{L} = \mathbb{K}(\alpha)$, avec $P(\alpha) = 0$.

Théorème 13 : [Perrin, p.70]
Soit $P \in \mathbb{K}[X]$ irréductible.
Il existe un corps de rupture de P sur $\mathbb{K}$, unique à isomorphisme près.
De plus, $\mathbb{K}[X]/(P)$ est un corps de rupture de P (si on note α la classe de X dans $\mathbb{K}[X]/(P)$, on a $P(X)$ congru à 0 modulo $P(X)$, c'est-à-dire $P(\alpha) = 0$. Ainsi, α est une racine de P dans $\mathbb{K}[X]/(P)$).

Définition 14 : Corps de décomposition [Perrin, p.71] :
On considère $P \in \mathbb{K}[X]$.
Une extension de corps $\mathbb{L}/\mathbb{K}$ est appelée **corps de décomposition de** P **sur** $\mathbb{K}$ lorsque dans $\mathbb{L}[X]$, P est produit de facteurs de degrés 1 et que le corps $\mathbb{L}$ est minimal pour cette propriété.

Théorème 15 : [Perrin, p.71]
Pour tout $P \in \mathbb{K}[X]$, il existe un corps de décomposition de P sur $\mathbb{K}$ et il est unique à isomorphisme près.

Définition 16 : Corps algébriquement clos [Perrin, p.67] :
On considère un corps $\mathbb{K}$ commutatif quelconque.
On dit que $\mathbb{K}$ est un **corps algébriquement clos** lorsqu'il vérifie l'une des propriétés équivalentes suivantes :
∗ Tout polynôme $P \in \mathbb{K}[X]$ de degré strictement positif admet une racine dans $\mathbb{K}$.
∗ Tout polynôme $P \in \mathbb{K}[X]$ est produit de polynômes de degré 1.
∗ Les éléments irréductibles de $\mathbb{K}[X]$ sont exactement les $X - a$ avec $a \in \mathbb{K}$.
∗ Si une extension $\mathbb{L}/\mathbb{K}$ est algébrique, alors $\mathbb{L} = \mathbb{K}$.

Définition 17 : Clôture algébrique [Perrin, p.72] :
On considère $\mathbb{K}$ un corps commutatif quelconque.
Une extension $\overline{\mathbb{K}}$ de $\mathbb{K}$ est appelée **clôture algébrique de** $\mathbb{K}$ lorsque $\overline{\mathbb{K}}$ est algébriquement clos et que $\overline{\mathbb{K}}$ est algébrique sur $\mathbb{K}$.

Proposition 18 : [Gourdon, p.67]
Tout corps commutatif algébriquement clos est infini.

I.2 Existence, unicité et structure des corps finis

Théorème 19 : Théorème de Wedderburn [Perrin, p.82] :
Tout corps fini est commutatif.

Proposition 20 : [Perrin, p.72]
Soient p un nombre premier et $\mathbb{K}$ un corps fini.
Si $\mathbb{K}$ est de caractéristique p, alors $\mathbb{K}$ a pour cardinal une puissance de p.

Exemple 21 :
Il n'existe pas de corps de cardinal 6 mais de cardinal 7 oui (par exemple $\mathbb{Z}/7\mathbb{Z}$).

Théorème 22 : [Perrin, p.73]
Soient p un nombre premier et $n \in \mathbb{N}^*$.
Si l'on pose $q = p^n$, alors il existe un corps commutatif $\mathbb{K}$ à q éléments (c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$).
En particulier, $\mathbb{K}$ est unique à isomorphisme près et on le note $\mathbb{F}_q$.

Exemple 23 :
On peut construire un corps à 4 éléments de deux manières :
* En tant que corps de décomposition de $X^4 - X$ sur $\mathbb{F}_2$.
* Grâce à l'isomorphisme $\mathbb{F}_4 \cong \mathbb{F}_2[X]/(X^2 + X + 1)$.

I.3 Structure du groupe multiplicatif d'un corps fini

Définition 24 : Indicatrice d'Euler [Berhuy, p.156] :
Pour tout $n \geq 1$, on note $\varphi(n)$ le nombre d'entiers de l'ensemble $[\![1; n]\!]$ qui sont premiers avec n et on appelle **indicatrice d'Euler** la fonction $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}^*$.

Lemme 25 : [Perrin, p.74]
Pour tout $n \in \mathbb{N}^*$, on a $n = \sum_{d|n} \varphi(d)$.

Théorème 26 :
Le groupe multiplicatif $\mathbb{F}_q^*$ est un groupe cyclique.

Corollaire 27 : [Perrin, p.74]
On a $\mathbb{F}_q^*$ isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.

Remarque 28 : [Perrin, p.74]
* On en sait pas, en général, trouver explicitement un générateur de $\mathbb{F}_q^*$...
* La même démonstration montre que tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.

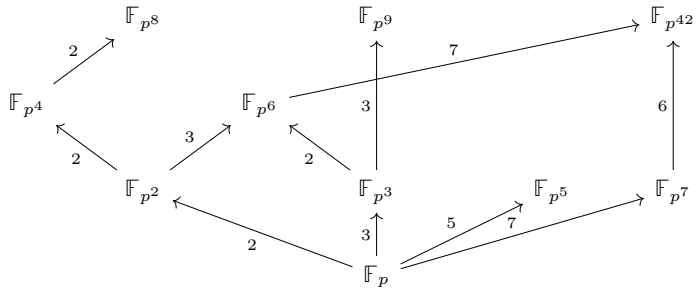
Théorème 29 : Théorème de l'élément primitif [Gourdon, p.97] :
Soit $\mathbb{K}$ un corps fini.
$\mathbb{L}/\mathbb{K}$ une extension de corps finie, alors il existe $\alpha \in \mathbb{L}$ tel que $\mathbb{L} = \mathbb{K}(\alpha)$.

II Propriétés sur les corps finis

II.1 Inclusion des corps finis

Corollaire 30 :
Soient p un nombre premier et $n, d \in \mathbb{N}^*$.
Si $\mathbb{K}$ est un corps à p^n éléments, alors il existe un unique sous-corps de $\mathbb{K}$ de cardinal p^d si, et seulement si, d divise n.
De plus, un tel sous-corps est alors isomorphe à $\mathbb{F}_{p^d}$.

Exemple 31 :
Pour un nombre premier p quelconque, on a par exemple le trellis suivant :



II.2 Automorphismes de $\mathbb{F}_q$

Proposition 32 : [Perrin, p.73]
Soit $\mathbb{K}$ un corps fini de caractéristique $p > 0$.
L'application $F : \mathbb{K} \longrightarrow \mathbb{K}$ définie par $F(x) = x^p$ est un morphisme de corps appelé **morphisme de Frobenius**.
De plus, si $\mathbb{K}$ est fini alors c'est un automorphisme et si $\mathbb{K} = \mathbb{F}_p$, alors c'est l'identité.

Proposition 33 : [Rombaldi, p.425]
Soit $\mathbb{K}$ un corps fini de cardinal $q = p^n$.
Le groupe $\mathrm{Aut}(\mathbb{K})$ des automorphismes de corps $\mathbb{K}$ est cyclique d'ordre n engendré par l'automorphisme de Frobenius.

II.3 Carrés dans un corps fini et symbole de Legendre

Théorème 34 : [Rombaldi, p.427]
* Il y a $\frac{q-1}{2}$ carrés et $\frac{q-1}{2}$ non carrés dans $\mathbb{F}_q^*$.
* Les carrés de $\mathbb{F}_q^*$ sont les racines de $X^{\frac{q-1}{2}} - 1$ et les non carrés sont les racines de $X^{\frac{q-1}{2}} + 1$.

Corollaire 35 : [Rombaldi, p.427]
∗ Le produit de deux carrés ou de deux non carrés de $\mathbb{F}_q^*$ est un carré et le produit d'un carré et d'un non carré est un non carré.
∗ -1 est un carré dans $\mathbb{F}_q^*$ si, et seulement si, q est congru à 1 modulo 4.

Définition 36 : Symbole de Legendre [Rombaldi, p.428] :
Pour tout $a \in \mathbb{F}_q^*$, on appelle **symbole de Legendre** l'entier :

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

Théorème 37 : [Rombaldi, p.428]
Pour tout $a \in \mathbb{F}_p^*$, on a $a^{\frac{p-1}{2}} = \overline{\left(\frac{a}{p}\right)}$ dans $\mathbb{F}_p^*$ et l'application $a \longmapsto \left(\frac{a}{p}\right)$ est l'unique morphisme de groupes non trivial de $\mathbb{F}_p^*$ dans $\{-1;1\}$.

Corollaire 38 : [Rombaldi, p.429]
Soient $n \in \mathbb{N}^*$ et p un nombre premier impair.
L'application :

$$\Psi : \left| \begin{array}{ccc} \mathrm{GL}_n(\mathbb{F}_p) & \longrightarrow & \{-1;1\} \\ A & \longmapsto & \left(\frac{\det(A)}{p}\right) \end{array} \right.$$

est l'unique morphisme de groupes non trivial de $\mathrm{GL}_n(\mathbb{F}_p)$ dans $\{-1;1\}$.

Théorème 39 : Théorème de Frobenius-Zolotarev [Rombaldi, p.430] :
Soient $n \in \mathbb{N}^*$ et p un nombre premier impair.
Pour tout $A \in \mathrm{GL}_n(\mathbb{F}_p)$ on a $\varepsilon(A) = \left(\frac{\det(A)}{p}\right)$.

Théorème 40 : Loi de réciprocité quadratique [Rombaldi, p.434] :
Pour tous nombres $p, q \in \mathcal{P}$ impairs distincts, $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

III Application aux polynômes et corps finis

III.1 Quelques outils d'irréductibilité

Proposition 41 : Critère d'irréductibilité d'Eisenstein [Perrin, p.76] :
Soit $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$.
S'il existe un élément irréductible p tel que :
∗ p ne divise pas a_n. ∗ Pour tout $i \in [\![0; n-1]\!]$, p divise a_i.
∗ p^2 ne divise pas a_0.
alors P est irréductible dans $\mathrm{Frac}(A)[X]$.

Exemple 42 :
Les polynômes $X^n - 2$ et $X^4 - 6X^3 + 3X^2 - 12X + 3$ sont irréductibles dans $\mathbb{Q}[X]$.

Proposition 43 : Critère de réduction [Perrin, p.77] :
Soient I un idéal premier de A et $P \in A[X]$ unitaire.
Si $\overline{a}_n \neq 0$ dans A/I et si $\overline{P}$ est irréductible sur A/I ou $\mathrm{Frac}(A/I)$, alors le polynôme P est irréductible sur $\mathrm{Frac}(A)$.

Exemple 44 : [Perrin, p.77]
Le polynôme $X^3 + 462X^2 + 2433X - 67691$ est irréductible dans $\mathbb{Q}[X]$ par le critère de réduction.

III.2 Polynômes irréductibles de $\mathbb{F}_q[X]$

Proposition 45 : [Perrin, p.78]
Soit $P \in \mathbb{K}[X]$ de degré $n > 0$.
P est irréductible sur $\mathbb{K}$ si, et seulement si, P n'a pas de racines dans toute extension $\mathbb{L}$ de $\mathbb{K}$ qui vérifie $[\mathbb{L} : \mathbb{K}] \leq \frac{n}{2}$.

Exemple 46 : [Perrin, p.78]
Le polynôme $X^4 + X + 1$ est irréductible sur $\mathbb{F}_2$.

Proposition 47 : [Perrin, p.79]
Soient $\mathbb{K}$ un corps commutatif quelconque, $P \in \mathbb{K}[X]$ un polynôme irréductible de degré n et $\mathbb{L}/\mathbb{K}$ une extension de corps de degré m.
Si $\mathrm{PGCD}(n, m) = 1$, alors P est encore irréductible dans $\mathbb{L}$.

Exemple 48 : [Perrin, p.79]
Le polynôme $X^3 + 4X + 2$ est irréductible sur $\mathbb{Q}[i]$ comme sur $\mathbb{Q}$.

IV Application au dénombrement sur les corps finis

IV.1 Polynômes irréductibles unitaires de degré n

Définition 49 : Fonction de Möbius [Berhuy, p.151] :
On appelle **fonction de Möbius**, la fonction μ définie par :

$$\mu : \left| \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & \begin{cases} (-1)^r & \text{si } n \text{ est produit de } r \text{ nombres premiers distincts} \\ 0 & \text{s'il existe un nombre premier } p \text{ tel que } p^2 \text{ divise } n \end{cases} \end{array} \right.$$

Développement 1 : [cf. FRANCINOU]

Lemme 50 : [Francinou, p.93]
Pour tout $n \in \mathbb{N}^*$, on a :

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$$

Théorème 51 : Formule d'inversion de Möbius [Francinou, p.93] :
Soient A un groupe abélien et $f : \mathbb{N}^* \longrightarrow A$.
Si l'on pose $g(n) = \sum_{d|n} f(d)$, alors $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$.

Théorème 52 : [Francinou, p.189]
Si l'on note $A(n,q)$ l'ensemble des polynômes irréductibles, unitaires et de degré n sur $\mathbb{F}_q$, alors $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P(X)$

Corollaire 53 : [Francinou, p.189]
En notant $I(n,q) = \text{Card}(A(n,q))$, on a :

$$I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \text{ et } \forall q \geq 2,\ I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$$

Remarque 54 : [Berhuy, p.654]
On a donc en particulier pour tous $n, q \in \mathbb{N}^*$, $I(n,q) \geq 1$. Ainsi, il existe au moins un polynôme irréductible de degré quelconque n dans $\mathbb{F}_p$ (c'est-à-dire que $\mathbb{F}_{p^n}$ existe toujours en tant que corps).

IV.2 Matrices à coefficients dans un corps fini

Dans toute cette sous-partie, on considère un corps $\mathbb{K}$ commutatif fini à $q = p^r$ éléments (avec p un nombre premier et $r \in \mathbb{N}^*$) et E un $\mathbb{K}$-espace vectoriel de dimension finie $n \geq 1$. On utilisera l'identification de $\text{GL}(E)$ avec $\text{GL}_n(\mathbb{K})$.

Proposition 55 : [Rombaldi, p.156]

$$\text{Card}(\text{GL}_n(\mathbb{F}_q)) = \prod_{k=0}^{n-1} \left(q^n - q^k\right) \text{ et } \text{Card}(\text{SL}_n(\mathbb{F}_q)) = \frac{1}{q-1} \prod_{k=0}^{n-1} \left(q^n - q^k\right)$$

Proposition 56 : [Perrin, p.105]
Le centre de $\text{GL}_n(\mathbb{F}_q)$ est de cardinal égal à $q-1$ et celui de $\text{SL}_n(\mathbb{F}_q)$ est de cardinal égal à $\text{PGCD}(n, q-1)$.

Théorème 57 : [Rombaldi, p.154]
Pour $n \geq 2$, on a :
$*$ $D(\text{SL}_n(\mathbb{K})) \subseteq D(\text{GL}_n(\mathbb{K})) \subseteq \text{SL}_n(\mathbb{K})$.
$*$ Pour $n \geq 3$, $D(\text{SL}_n(\mathbb{K})) = D(\text{GL}_n(\mathbb{K})) = \text{SL}_n(\mathbb{K})$.
$*$ Pour $n = 2$, $\mathbb{K} \neq \mathbb{F}_2$ et $\mathbb{K} \neq \mathbb{F}_3$, $D(\text{SL}_n(\mathbb{K})) = D(\text{GL}_n(\mathbb{K})) = \text{SL}_n(\mathbb{K})$.

Remarque 58 : [Rombaldi, p.155]
$*$ Pour $\mathbb{K} = \mathbb{F}_2$, on a $\text{GL}_n(\mathbb{K}) = \text{SL}_n(\mathbb{K})$.
$*$ Pour $n = 2$ et $\mathbb{K} = \mathbb{F}_2$, on a $D(\text{SL}_n(\mathbb{K})) \cong \mathfrak{A}_3$.
$*$ Pour $n = 2$ et $\mathbb{K} = \mathbb{F}_3$, on a $D(\text{SL}_n(\mathbb{K})) \cong \mathbb{H}_8$.

Proposition 59 : [Rombaldi, p.158]
Si G est un groupe fini de cardinal $n \in \mathbb{N}^*$, alors pour tout nombre premier p, G est isomorphe à un sous-groupe de $\text{GL}_n(\mathbb{F}_p)$.

Proposition 60 : [Perrin, p.106]
On a $\text{GL}_2(\mathbb{F}_2) = \text{SL}_2(\mathbb{F}_2) = \text{PSL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$.

Théorème 61 : [Perrin, p.106]
On a les isomorphismes suivants :
$*$ $\text{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$ et $\text{PSL}_2(\mathbb{F}_3) \cong \mathfrak{A}_4$. $*$ $\text{PGL}_2(\mathbb{F}_4) = \text{PSL}_2(\mathbb{F}_4) \cong \mathfrak{A}_5$.
$*$ $\text{PGL}_2(\mathbb{F}_5) \cong \mathfrak{S}_5$ et $\text{PSL}_2(\mathbb{F}_5) \cong \mathfrak{A}_5$.

Développement 2 : [cf. CALDERO]

Théorème 62 : [Caldero, p.74]
Si $\mathbb{K}$ est un corps fini commutatif de cardinal q, alors il y a $n_d = q^{d(d-1)}$ matrices nilpotentes de taille $d \times d$ à coefficients dans $\mathbb{K}$.

Remarques sur la leçon

— Il faut être capable de faire des calculs dans $\mathbb{F}_q$ et de pouvoir trouver un générateur et des inverses dans $\mathbb{F}_q^*$.

— Savoir déterminer $\mathbb{F}_3(x)$ avec x qui vérifie des conditions données.

Liste des développements possibles

— Dénombrement des polynômes unitaires irréductibles sur $\mathbb{F}_q$.

— Dénombrement des endomorphismes nilpotents sur un corps fini.

Bibliographie

— Daniel Perrin, *Cours d'algèbre*.

— Xavier Gourdon, *Les maths en tête, Algèbre et Probabilités*.

— Grégory Berhuy, *Algèbre : le grand combat*.

— Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et Géométrie*.

— Serge Francinou, *Exercices de mathématiques pour l'agrégation, Algèbre 1*.

— Philippe Caldero, *Carnet de voyage en Algébrie*.