123 : Corps finis. Applications.

Pandou

23 avril 2022

1 Propriétés des corps finis

1.1 Caractéristique et cardinal

Théorème 1 (Wedderburn). *Tout anneau intègre fini est un corps commutatif.*

Proposition 2. *L'anneau $\mathbb{Z}/p\mathbb{Z}$ est un corps si, et seulement si, p est premier et dans ce cas, on note $\mathbb{F}_p$ ce corps.*

Définition 3. *Soit A un anneau, le générateur positif de $\mathrm{Ker}(\mathbb{Z} \longrightarrow A)$ est appelé caractéristique de A.*

Proposition 4. *La caractéristique d'un corps est soit nulle, soit un nombre premier.*

Proposition 5. *Soit K un corps fini, alors K est de caractéristique p pour p premier. D*

Remarque 6 : Il existe des corps de caractéristique p qui sont infinis : $\mathbb{F}_p(X)$.

Proposition 7. *Soit K un corps de caractéristique p premier. L'application $F : x \in K \longmapsto x^p \in K$ est un morphisme de corps, appelé morphisme de Frobenius.*
Si K est fini, alors F est un automorphisme.

Corollaire 8. *Soit K un corps fini de caractéristique p premier, alors K est muni d'une structure de $\mathbb{F}_p$-espace vectoriel. En particulier, $\mathrm{Card}(K) = p^n$ pour un certain entier n.*

1.2 Construction et réalisation

Théorème 9. *Soit p un nombre premier et $n \geqslant 1$, on note $q = p^n$.*

1. *Il existe un corps K à q éléments, par exemple le corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.*
2. *Le corps K est unique à isomorphisme près. On le note $\mathbb{F}_q$.*

Théorème 10 (Admis). *Soit K un corps. Alors, K admet une clôture algébrique.*

Proposition 11. *Soit $\overline{\mathbb{F}_p}$ une clôture algébrique de $\mathbb{F}_p$, $q = p^n$. Alors, $\overline{\mathbb{F}_p}$ admet un unique sous-corps de cardinal q : c'est l'ensemble des racines de $X^q - X$.*

Corollaire 12. *Soit $n, m \geqslant 1$. On a $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ si, et seulement si, $n|m$.*

Exemple 13 : Le seul sous-corps propre de $\mathbb{F}_8$ est $\mathbb{F}_2$.

Lemme 14. *La clôture algébrique de $\mathbb{F}_{p^n}$ coincide avec celle de $\mathbb{F}_p$.*

Théorème 15.

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

1.3 Groupe multiplicatif $\mathbb{F}_q^\times$

Définition 16. *On rappelle que l'indicatrice d'Euler $\varphi(n)$ est le nombre d'inversibles de $\mathbb{Z}/n\mathbb{Z}$.*

Lemme 17. *Soit $n \geqslant 1$, alors $n = \sum_{d|n} \varphi(d)$.*

Proposition 18. *$\mathbb{F}_q^\times$ est un groupe cyclique, donc isomorphe à $\mathbb{Z}/(q-1)\mathbb{Z}$.*

DEVELOPPEMENT 1

Application 19 : Soit $p \geqslant 3$ un nombre premier, $n \geqslant 1$, on note $q = p^n$. Alors, $SO_2(\mathbb{F}_q)$ est un groupe cyclique. Plus précisément :

$$SO_2(\mathbb{F}_q) = \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } -1 \text{ est un carré dans } \mathbb{F}_q^\times \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{sinon} \end{cases}$$

Proposition 20 (Élément primitif). *Soit K un corps fini de caractéristique p, ξ un générateur de $K^\times$. Alors, $K = \mathbb{F}_p(\xi)$. Plus précisément, si $n = [K : \mathbb{F}_p]$, alors*

$$K = \bigoplus_{i=0}^{n-1} \mathbb{F}_p \xi^i$$

Remarque 21 : Toutefois, en général trouver un générateur de $\mathbb{F}_q^\times$ est difficile.

2 Application en arithmétique

2.1 Carrés de $\mathbb{F}_q$

Définition 22. *On note $\mathbb{F}_q^{(2)}$ l'ensemble des carrés de $\mathbb{F}_q$ et $\mathbb{F}_q^{*(2)}$ l'ensemble des carrés non nuls de $\mathbb{F}_q$.*

Proposition 23.
- *Si $p = 2$, $\mathbb{F}_q^{(2)} = \mathbb{F}_q$.*
- *Si $p \geqslant 3$, $\mathrm{Card}\left(\mathbb{F}_q^{*(2)}\right) = \dfrac{q-1}{2}$.*

Corollaire 24. *Si $p \geqslant 3$, alors*

$$x \in \mathbb{F}_q^{*(2)} \iff x^{\frac{q-1}{2}} = 1$$

Application 25 : Si $p \geqslant 3$, alors -1 est un carré dans $\mathbb{F}_q$ si, et seulement si, $q = 1 \mod (4)$.

Application 26 : Il existe une infinité de nombres premiers de la forme $4n+1$.

Définition 27. *Soit p un nombre premier impair et $a \in \mathbb{F}_p^\times$. On définit*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \text{ est divisible par } p \\ 1 & \text{si } a \text{ est un résidu quadratique modulo } p \\ -1 & \text{si } a \text{ n'est pas un résidu quadratique modulo } p \end{cases}$$

Proposition 28.

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

Corollaire 29.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Quelques formules 30 :

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 & \text{si } n = 1 \mod (4) \\ -1 & \text{si } n = -1 \mod (4) \end{cases}$$

et,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & \text{si } n = \pm 1 \mod (8) \\ -1 & \text{si } n = \pm 5 \mod (8) \end{cases}$$

Théorème 31 (Loi de réciprocité quadratique (admis))**.** *Soit p et q deux nombres premiers impairs distincts, alors*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Application 32 : Ce théorème permet de calculer $\left(\dfrac{a}{p}\right)$ pour tout $a \in \mathbb{Z}$.

2.2 Polynômes irréductibles

Proposition 33. *Un corps fini n'est jamais algébriquement clos.*

Théorème 34. *Soit p premier et $n \geqslant 1$ et $q = p^n$. Alors, $\mathbb{F}_q \simeq \mathbb{F}_p[X]/(\pi)$ où π est un polynôme irréductible quelconque de degré n sur $\mathbb{F}_p$.*

Corollaire 35. *Il existe des polynômes irréductibles de tout degré dans $\mathbb{F}_p[X]$.*

DEVELOPPEMENT 2

Lemme 36. *Soit $P \in \mathbb{F}_p[X]$ irréductible unitaire de degré m, alors P divise $X^{p^n} - X$ si, et seulement si, m divise n.*

Proposition 37. *Soit $P \in \mathbb{F}_p[X]$ irréductible de degré m, alors toutes les racines de P dans $\overline{\mathbb{F}_p}$ sont de la forme $\alpha, \alpha^p, ..., \alpha^{p^{m-1}}$ où α est une racine de P.*

Théorème 38. *$\mathrm{Aut}_{\mathbb{F}_p}\left(\mathbb{F}_{p^m}\right)$ est un groupe cyclique engendré par le morphisme de Frobenius.*

Application 39 (du lemme 36) : Si $\mathrm{Irr}(\mathbb{F}_p, m)$ est l'ensemble des polynômes irréductibles unitaires de degré m sur $\mathbb{F}_p$, alors

$$X^{p^n} - X = \prod_{m|n} \prod_{Q \in \mathrm{Irr}(\mathbb{F}_p, m)} Q(X)$$

En utilisant l'inversion de Möbius, on en déduit que

$$\mathrm{Card}\left(\mathrm{Irr}(\mathbb{F}_p, n)\right) = \frac{1}{n} \sum_{m|n} \mu\left(\frac{n}{m}\right) p^m \sim \frac{p^n}{n}$$

Théorème 40 (Critère d'Eisenstein)**.** *Soit $P(X) = a_n X^n + ... + a_0 \in \mathbb{Q}[X]$. On suppose qu'il existe p un nombre premier tel que*
- *p divise tous les a_i avec $i \leqslant n-1$.*
- *p ne divise pas a_n.*
- *p^2 ne divise pas a_0.*

Alors, P est irréductible dans $\mathbb{Q}[X]$.

Exemple 41 : Soit p un nombre premier, $\Phi_p(X) = X^{p-1} + ... + X + 1$ est irréductible.

Théorème 42 (Réduction)**.** *Soit $P = a_n X^n + ... + a_0 \in \mathbb{Z}[X]$ et p un nombre premier tel que $a_n \neq 0 \mod (p)$. Si $\overline{P}$ est irréductible dans $\mathbb{F}_p$, alors P est irréductible sur $\mathbb{Q}$.*

Application 43 : $X^p - X - 1$ est irréductible sur $\mathbb{Z}$.

Remarque 44 : La réciproque est fausse : X^4+1 est irréductible sur $\mathbb{Z}$, mais réductible dans tous les $\mathbb{F}_p$.

3 Algèbre linéaire sur un corps fini

Soit E un k-espace vectoriel de dimension n. On suppose que k est de caractéristique $\neq 2$ dans la partie 3.3.

3.1 Une famille de groupes simples

Proposition 45. *Le centre de $GL(E)$ est l'ensemble des homothéties de rapport non nul, il est isomorphe à k^*. Le centre de $SL(E)$ est isomorphe au groupe $\mu_n(k)$ des racines n-ièmes de l'unité.*
On définit alors $PGL(E) = GL(E)/k^*$ et $PSL(E) = SL(E)/\mu_n(k)$.

Théorème 46.
- *Les transvections engendrent $SL(E)$.*
- *Les transvections et les diltations engendrent $GL(E)$.*

Proposition 47.
- *Si $n \geqslant 3$, les transvections sont conjugués dans $SL(E)$.*
- *Toute transvection est conjuguée dans $SL_2(k)$ à une matrice $\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix}$ pour $\lambda \in k^*$.*
  De plus, $\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix}$ et $\begin{pmatrix}1 & \mu\\ 0 & 1\end{pmatrix}$ sont conjuguées dans $SL_2(k)$ si, et seuleemnt si, $\frac{\lambda}{\mu}$ est un carré dans k.

Théorème 48. *Le groupe $PSL_n(k)$ est simple, sauf pour $PSL_2(\mathbb{F}_2)$ et $PSL_2(\mathbb{F}_3)$.*

Proposition 49. *Les cardinaux des groupes linéaires sur $\mathbb{F}_q$ sont*

1. $\mathrm{Card}\big(GL_n(\mathbb{F}_q)\big) = (q^n-1)(q^n-q)...(q^n-q^{n-1})$.
2. $\mathrm{Card}\big(SL_n(\mathbb{F}_q)\big) = \mathrm{Card}\big(PGL_n(\mathbb{F}_q)\big) = \dfrac{(q^n-1)(q^n-q)...(q^n-q^{n-1})}{q-1}$.
3. $\mathrm{Card}\big(PSL_n(\mathbb{F}_q)\big) = \dfrac{(q^n-1)(q^n-q)...(q^n-q^{n-1})}{(q-1)\times \mathrm{pgcd}(n,q-1)}$.

Théorème 50. *On a les isomorphismes exceptionnels suivants :*

1. $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$.
2. $PGL_2(\mathbb{F}_3) = \mathfrak{S}_4$ *et* $PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$.
3. $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathfrak{A}_5$.
4. $PGL_2(\mathbb{F}_5) \simeq \mathfrak{S}_5$ *et* $PSL_2(\mathbb{F}_5) \simeq \mathfrak{A}_5$.

3.2 Réduction et dénombrement

Proposition 51. *Une matrice $M \in M_n(\mathbb{F}_q)$ est diagonalisable si, et seulement si, $M^q = M$.*

Corollaire 52. *Le nombre de matrices diagonalisables dans $GL_n(\mathbb{F}_q)$ est*

$$\sum_{n_1+\ldots+n_{q-1}=n} \frac{\mathrm{Card}\big(GL_n(\mathbb{F}_q)\big)}{\prod_{i=1}^{q-1} \mathrm{Card}\big(GL_{n_i}(\mathbb{F}_q)\big)}$$

Remarque 53 : En fait, on peut aller plus loin en donnant le nombre de matrices diagonalisables dans $M_n(\mathbb{F}_q)$:

$$\sum_{n_1+\ldots+n_q=n} \frac{\mathrm{Card}\big(GL_n(\mathbb{F}_q)\big)}{\prod_{i=1}^{q} \mathrm{Card}\big(GL_{n_i}(\mathbb{F}_q)\big)}$$

DEVELOPPEMENT 3

Lemme 54 (Fitting). *Soit $u \in \mathcal{L}(E)$, alors il existe une décomposition $E = F \oplus G$ telle que*

1. *F et G sont stables par u.*
2. *$u_{|F}$ est un endomorphisme nilpotent de F.*
3. *$u_{|G}$ est un automorphisme de G.*

De plus, l'application $\Phi : u \in \mathcal{L}(E) \longmapsto (F, G, u_{|F}, u_{|G})$ à valeurs dans les quadruplets (F, G, v, w) tels que $E = F \oplus G$ et v est un nilpotent de F et w un automorphisme de G est une bijection.

Application 55 : Il y a $q^{n(n-1)}$ matrices nilpotentes dans $M_n(\mathbb{F}_q)$.

3.3 Formes quadratiques sur $\mathbb{F}_q$

Définition 56. *Soit q une forme quadratique sur E. Alors, le discrimiannt de q est $\delta(q) = \det(q) \mod \mathbb{F}_q^{(2)}$ où $\det(q)$ est le déterminant de la matrice associée à q dans une base quelconque.*

Remarque 57 : Le discriminant $\delta(q)$ est bien défini.

Lemme 58. *Soit $a, b \in \mathbb{F}_q^\times$. L'équation $ax^2 + by^2 = 1$ admet toujours au moins une solution dans $\mathbb{F}_q^2$.*

Théorème 59. *Soit q une forme quadratique non dégénérée sur E et $\delta \in \alpha \in \mathbb{F}_q^* \setminus \mathbb{F}_q^{*(2)}$. Alors, q est équivalente à l'une des deux formes quadratiques suivantes :*

1. $q_1(x) = x_1^2 + ... + x_{n-1}^2 + x_n^2$.
2. $q_2(x) = x_1^2 + ... + x_{n-1}^2 + \delta x_n^2$.

Références :

- Caldero-Germoni, NH2G2 Tome 2, pp. 50-51.
- Caldero-Germoni, H2G2, Tome 2.
- Demazure, Cours d'algèbre.
- FGN, Algèbre 1&3.
- Gozard, Théorie de Galois.
- Perrin, Cours d'algèbre.
- Serre, Cours d'arithmétique.