ALGÈBRE - LEÇON 123 : CORPS FINIS. APPLICATIONS

SIMON RICHE

1. Commentaires du jury (rapport 2025)

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 téléscopique, les injections des divers $\mathbf{F}_q$ sont incontournables. La structure du groupe multiplicatif doit aussi être connue.

Des applications des corps finis (y compris pour $\mathbf{F}_q$ 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.

2. Plan

Une référence incontournable est [Pe]. La lecture du Chapitre 5 de [Pa] est également instructive.

2.1. **Remarques préliminaires.**

2.1.1. Le contenu du début du plan est clair : il faut commencer par expliquer l'existence et l'unicité (à isomorphisme près !) des corps finis, puis parler de leurs propriétés. La question de l'existence d'un corps de cardinal p^n est fortement liée à celle de l'existence d'un polynôme irréductible de degré n sur $\mathbb{F}_p$. Ces deux questions doivent être abordées, mais il faut choisir dans quel ordre on le fait. La présentation la plus classique (choisie dans [Pe] et dans [Pa]) est de démontrer d'abord l'existence d'un corps fini à p^n éléments (en montrant que le corps de décomposition de $X^{p^n}-X$ sur $\mathbb{F}_p$ a ce cardinal) puis d'en déduire l'existence d'un polynôme irréductible de degré n, en prenant par exemple le polynôme minimal sur $\mathbb{F}_p$ d'un générateur du groupe multiplicatif d'un corps à p^n éléments. Une autre option (choisie dans [De]) est de démontrer d'abord l'existence d'un polynôme irréductible de degré n (par un argument de dénombrement) puis d'en déduire l'existence d'un corps de cardinal p^n, construit comme corps de rupture d'un tel polynôme. Les deux stratégies sont raisonnables, mais il faut en choisir une et en être conscient. Par ailleurs, il est indispensable de comprendre (et de mentionner) ces deux constructions des corps finis, comme corps de décomposition et comme corps de rupture.

Date: Année 2025–2026.

2.1.2. Il est indispensable, dans le cadre de cette leçon, de bien maîtriser les définitions et propriétés des corps de rupture et corps de décomposition. Il peut être conseillé de mentionner ces questions en "rappels" au début du plan ; mais même si ce n'est pas le cas le jury pourra vous poser des questions pour vérifier que vous êtes à l'aise avec ces notions.

2.1.3. Il faut bien être conscient que la notation $\mathbb{F}_q$ (pour q une puissance d'un nombre premier avec exposant au moins 2) est abusive puisque ce corps n'est défini *qu'à isomorphisme près*. C'est un abus commun, et autorisé, mais qu'il faut garder en tête, notamment quand on veut manipuler les injections entre ces différents corps.

2.2. **Ce qui doit apparaître.** "Rappels" sur la théorie des corps :
- théorème de la base téléscopique, multiplicativité du degré ;
- corps de rupture ;
- corps de décomposition ;
- caractéristique.

Existence et unicité (à isomorphisme près) du corps à $q = p^n$ éléments.

Construction comme corps de décomposition de $X^q - X$ et/ou comme corps de décomposition d'un polynôme irréductible de degré n sur $\mathbb{F}_p$ (en démontrant qu'un tel polynôme existe).

Condition pour qu'il existe un morphisme de corps $\mathbb{F} \to \mathbb{F}'$ si $\mathbb{F}$ et $\mathbb{F}'$ sont des corps finis de même caractéristique.

Morphisme de Frobenius.

Application : petit théorème de Fermat.

Théorème de Wedderburn. [1]

Le groupe multiplicatif $\mathbb{F}^\times$ est cyclique.

Application : irréductibilité de polynômes à coefficients entiers (cf. critère d'Eisenstein notamment).

Carrés de $\mathbb{F}$.

Applications : nombres premiers de la forme $4m + 1$, théorème des deux carrés.

2.3. **Ce qui peut apparaître.** Algorithme de Berlekamp.

Loi de réciprocité quadratique.

Dénombrement (cardinal de $\mathrm{GL}_n(\mathbb{F})$, de $\mathrm{SL}_n(\mathbb{F})$, nombre de sous-espaces de dimension donnée dans $\mathbb{F}^n$).

Isomorphismes exceptionnels entre groupes linéaires sur des corps finis et groupes symétriques / alternés.

Nombre de matrices nilpotentes, de matrices diagonalisables.

(Pour tout ceci, voir [CG1, CG2].)

Classification des formes quadratiques sur un corps fini de cardinal impair.

Calcul du cardinal du groupe orthogonal associé. (Voir [CG1, §IV.2].)

Calcul du nombre de polynômes unitaires irréductibles de degré n.

1. Attention ! Dans cet énoncé il ne faut pas parler de "corps", puisque les corps sont supposés commutatifs ! Un énoncé possible est que "tout anneau intègre fini est un corps".

Théorème de l'élément primitif pour un corps fini (et lien avec la cyclicité du groupe multiplicatif).

Irréductibilité des polynômes cyclotomiques (sur $\mathbb{Z}$, et éventuellement sur $\mathbb{F}_q$). [2]

Codes correcteurs.

Exemple de polynôme irréductible sur $\mathbb{Z}$ mais réductible modulo chaque nombre premier. [3]

3. Quelques questions bêtes auxquelles il faut absolument savoir répondre rapidement

(1) Que peut-on dire du groupe $(\mathbb{F}_q, +)$ si $q = p^r$ avec p premier ?

(2) Combien existe-t-il d'applications linéaires injectives de $\mathbb{F}^n$ dans $\mathbb{F}^m$? Même question pour les applications surjectives.

(3) Montrer que tout groupe fini s'injecte dans un groupe $\mathrm{GL}_n(\mathbb{F})$ avec $\mathbb{F}$ corps fini.

(4) Donner une construction explicite du corps à 9 éléments. Même chose pour 8 éléments.

(5) Est-il vrai que tout corps de caractéristique p est fini ?

(6) Est-il vrai que si $f \in \mathbb{F}_p[X]$ est irréductible de degré n, la classe de X dans le corps $K = \mathbb{F}_p[X]/(f)$ est un générateur de $K^\times$? (*Indication* : on pourra considérer le polynôme $X^2 + 1 \in \mathbb{F}_3[X]$.) D'un autre point de vue, étant donné n, existe-t-il toujours un polynôme f irréductible de degré n tel que cette propriété est satisfaite ?

(7) Si $\mathbb{F}$ est un corps fini, pour quelles valeurs de $n \in \mathbb{Z}_{\geq 1}$ existe-t-il un polynôme irréductible de degré n dans $\mathbb{F}[X]$?

4. Exercices

4.1. **Automorphismes et applications.**

Exercice 1. Soit $\mathbb{F}$ un corps de cardinal q, et $\mathbb{F}'$ une extension de $\mathbb{F}$ de degré n.

(1) Montrer que l'application

$$\sigma : \mathbb{F}' \to \mathbb{F}'$$

définie par $\sigma(x) = x^q$ est un automorphisme de corps d'ordre n, tel que $\sigma(x) = x$ pour tout $x \in \mathbb{F}$.

(2) On note G le groupe des automorphismes de corps τ de $\mathbb{F}'$ qui vérifient $\tau(x) = x$ pour tout $x \in \mathbb{F}$. Montrer que $\#G \leq n$. (*Indication* : on pourra utiliser le théorème de l'élément primitif.)

(3) En déduire que $G \cong \mathbb{Z}/n\mathbb{Z}$.

(4) Montrer que si $P \in \mathbb{F}[X]$ est un polynôme irréductible, et si P admet une racine dans $\mathbb{F}'$, alors P est scindé à racines simples dans $\mathbb{F}'[X]$. (*Indication* : on pourra se ramener au cas où $\mathbb{F}'$ est le corps de rupture de P.)

2. Pour cela, voir [Pa, §5.4] ou [Pe, §III.4].

3. Voir par exemple [Pa, Ex. 5.1, correction p. 191].

Exercice 2. Si $\mathbb{F}$ et $\mathbb{F}'$ sont deux corps finis, combien existe-t-il de morphismes de corps de $\mathbb{F}$ vers $\mathbb{F}'$? (*Indication* : déterminer quand de tels morphismes existent, puis quand c'est le cas montrer que leur image ne dépend pas du choix de morphisme. Enfin, on pourra utiliser l'Exercice 1.)

Exercice 3. (1) Soit K un corps fini, et soit L une extension de K.
   (a) Montrer que tout automorphisme de corps de L stabilise K.
   (b) Montrer que pour tout automorphisme de corps σ de K, il existe un endomorphisme de corps de L dont la restriction à K est σ. (*Indication* : on pourra utiliser l'Exercice 1.)

(2) Soit K un corps fini, et soient L et L' deux extensions finies de K, de degrés respectifs n et n'. Montrer l'équivalence entre les deux propriétés suivantes :
   (a) n divise n' ;
   (b) il existe un morphisme de corps $L \to L'$ qui est un morphisme de K-algèbres.

(3) Soit K un corps fini, soit $P \in K[X]$ un polynôme irréductible de degré n, et soit L une extension de K de degré m. Déterminer à quelle condition sur n et m le polynôme P admet une racine dans L. (*Indication* : on pourra relier cette condition à l'existence d'un morphisme K-linéaire du corps de rupture de P sur K vers L.)

4.2. **Matrices à coefficients dans un corps fini.**

Exercice 4. Soit $\mathbb{F}$ un corps fini. Décrire toutes les matrices nilpotentes dans $\mathrm{M}_2(\mathbb{F})$. Montrer en particulier qu'il en existe q^2. (*Indication* : on pourra remarquer qu'une matrice de taille n est nilpotente ssi son polynôme caractéristique est X^n, puis en déduire des conditions sur les coefficients dans notre cadre.)

Exercice 5. Soit p un nombre premier, $n \in \mathbb{Z}_{\geq 0}$, et q une puissance de p. Déterminer un p-Sylow du groupe $\mathrm{GL}_n(\mathbb{F})$ si $\mathbb{F}$ est un corps de cardinal q. Dénombrer ces sous-groupes. (*Indication* : commencer par déterminer la plus grande puissance de p divisant $\#\mathrm{GL}_n(\mathbb{F}_q)$. Puis considérer des matrices triangulaires supérieures et unipotentes.)

Référence : [CG2, Chap. VIII, Prop. 1.4].

Exercice 6. Soit $\mathbb{F}$ un corps fini.

(1) Déterminer le nombre de matrices M dans $\mathrm{M}_n(\mathbb{F})$ qui sont nilpotentes et telles que $M^{n-1} \neq 0$. (On pourra commencer par montrer qu'une telle matrice est semblable à un bloc de Jordan de taille n, puis utiliser l'action de $\mathrm{GL}_n(\mathbb{F})$ sur $\mathrm{M}_n(\mathbb{F})$ par conjugaison.)

(2) Déterminer le cardinal de la classe de conjugaison d'une matrice diagonalisable dans $\mathrm{M}_n(\mathbb{F})$.

(3) En déduire le nombre de matrices diagonalisables à valeurs propres distinctes dans $\mathrm{M}_n(\mathbb{F})$.

Référence : [CG2, Chap. VIII, Ex. B.4 et B.6].

Exercice 7. Soit $\mathbb{F}$ un corps fini.

(1) Rappeler comment se calcule le cardinal de $\mathrm{SL}_n(\mathbb{F})$.

(2) Montrer que si $\mathbb{F}'$ est un corps et s'il existe un isomorphisme de groupes entre $\mathrm{SL}_n(\mathbb{F})$ et $\mathrm{SL}_n(\mathbb{F}')$, alors les corps $\mathbb{F}$ et $\mathbb{F}'$ sont isomorphes.

Référence : sujet MG 2013, question I.C.2(c).

4.3. **Construction des corps finis.**

Exercice 8. (1) Déterminer la liste des polynômes irréductibles de degré ≤ 4 sur $\mathbb{F}_2$.

(2) Que peut-on dire de la factorisation sur $\mathbb{F}_4$ d'un polynôme irréductible de degré 4 sur $\mathbb{F}_2$? (On pourra considérer les racines d'un tel polynôme.)

(3) En déduire le nombre de polynômes irréductibles de degré 2 sur $\mathbb{F}_4$.

(4) Faire la liste de ces polynômes.

(5) En déduire plusieurs constructions possibles du corps $\mathbb{F}_{16}$.

Référence : Fiche de P. Boyer mentionnée en Partie 6 (Exercice 3).

4.4. **Carrés et cubes dans les corps finis.**

Exercice 9. Soit p un nombre premier.

(1) Soit $P \in \mathbb{F}_p[X]$ un polynôme irréductible de degré n, et soit K un corps de cardinal p^m. Déterminer à quelle condition sur n et m le polynôme P admet une racine dans K.[4] (*Indication* : on pourra relier cette condition à l'existence d'un morphisme du corps de rupture de P vers K.)

(2) Soit $n \in \mathbb{Z}_{\geq 0}$, K un corps de cardinal p^n, et $x \in \mathbb{F}_p$.

(a) Montrer que x est un carré dans K si et seulement si il vérifie l'une ou l'autre des conditions suivantes :
- x est un carré dans $\mathbb{F}_p$;
- x n'est pas un carré dans $\mathbb{F}_p$ et n est pair.

(b) En déduire que x est un carré dans K si et seulement si $\left(\frac{x}{p}\right)^n = 1$.

Exercice 10. Soit K un corps fini, de cardinal $q = p^n$ où p est premier, avec $p \neq 3$.

(1) Montrer l'équivalence entre les propriétés suivantes :

(a) tout élément de K est un cube ;

(b) le polynôme $1 + X + X^2$ est irréductible dans $K[X]$;

(c) $3 \nmid q - 1$.

(*Indication* : on pourra utiliser la utiliser la cyclicité de $K^\times$.)

(2) Montrer que si $p \neq 2$, ces conditions sont également équivalentes aux suivantes :

(d) -3 n'est pas un carré dans $\mathbb{F}_p$ et n est impair ;

(e) -3 n'est pas un carré dans K.

(*Indication* : on pourra utiliser la loi de réciprocité quadratique et l'Exercice 9.)

(3) Montrer que si $p = 2$, ces conditions sont vérifiées si et seulement n est impair.

(4) Montrer que si ces conditions ne sont pas vérifiées, alors le nombre de cubes dans K est $\frac{q+2}{3}$.

(5) Que peut-on dire si $p = 3$?

4. Cette question est une version simplifiée d'une question de l'exercice 3, qui peut se traiter directement et plus facilement.

4.5. **Irréductibilité des polynômes cyclotomiques sur les corps finis.**

Exercice 11. Pour p un nombre premier et $n \geq 1$, on note $\varphi_{n,p} \in \mathbb{F}_p[X]$ l'image du n-ième polynôme cyclotomique φ_n par le morphisme naturel $\mathbb{Z}[X] \to \mathbb{F}_p[X]$. On rappelle [5] que si n est premier à p, alors $\varphi_{n,p} = \prod_{\zeta \in \mu_n^\circ(\mathbb{F})}(X - \zeta)$ où $\mathbb{F}$ est une clôture algébrique de $\mathbb{F}_p$ et $\mu_n^\circ(\mathbb{F})$ est l'ensemble des racines primitives n-ièmes de l'unité dans $\mathbb{F}$. Le but de cet exercice est de démontrer que pour $n \geq 2$ fixé, il existe p premier tel que $\varphi_{n,p}$ soit irréductible (dans $\mathbb{F}_p[X]$) si et seulement si $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique.

(1) Rappeler pourquoi si $\mathbb{K}$ est un corps, un polynôme $P \in \mathbb{K}[X]$ est réductible si et seulement si il admet une racine dans une extension de $\mathbb{K}$ de degré $< \deg(P)$ [6].

(2) En déduire que si n est premier à p, $\varphi_{n,p}$ est réductible (dans $\mathbb{F}_p[X]$) si et seulement si l'ordre de l'image de p dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est $< \phi(n)$ (où ϕ est l'indicatrice d'Euler). (On pourra utiliser le fait que le groupe des inversibles d'un corps fini est cyclique.)

(3) On suppose que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique, et on fixe $a \in \mathbb{Z}$ dont la classe dans $\mathbb{Z}/n\mathbb{Z}$ est un générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$. Montrer que si p est un nombre premier [7] tel que $p \equiv a \mod n$, alors $\varphi_{n,p}$ est irréductible.

(4) On suppose maintenant que $(\mathbb{Z}/n\mathbb{Z})^\times$ n'est pas cyclique.
   (a) Montrer que si p ne divise pas n, alors $\varphi_{n,p}$ est réductible.
   (b) On suppose à partir de maintenant que $p \mid n$, et on écrit $n = p^\alpha m$ avec $\alpha \geq 1$ et $m \geq 1$ premier à p. On suppose par l'absurde que $\varphi_{n,p}$ est irréductible. Montrer que $\varphi_{n,p}$ divise $X^m - 1$ dans $\mathbb{F}_p[X]$. (*Indication* : on pourra utiliser les propriétés du morphisme de Frobenius.)
   (c) En déduire qu'alors il existe un diviseur d de m tel que $\varphi_{n,p}$ divise $\varphi_{d,p}$.
   (d) Montrer qu'on a nécessairement $p = 2$, $\alpha = 1$, et $d = m$. (*Indication* : considérer les degrés de polynômes appropriés.)
   (e) Montrer qu'alors $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times$, et trouver une absurdité.

Référence : [Pe, Chap. III, Théorème 4.14 et Proposition 4.16].

Notons que pour $n = 8$, le polynôme cyclotomique est $X^4 + 1$, et $(\mathbb{Z}/8\mathbb{Z})^\times$ n'est pas cyclique. On retrouve donc par cet exercice le fait classique que $X^4 + 1$ est irréductible sur $\mathbb{Q}$ mais est réductible sur chaque corps fini.

5. Complément : Groupe spécial orthogonal d'un corps fini

Référence : [CG2, p. 50–53].

On considère un nombre premier impair p, et un corps fini $\mathbb{F}$ de caractéristique p, et donc de cardinal une puissance q de p. On s'intéresse au groupe spécial orthogonal $\mathrm{SO}_2(\mathbb{F})$, qu'on peut définir comme le sous-groupe de $\mathrm{GL}_2(\mathbb{F})$ constitué des matrices M telles que

$$ {}^{\mathrm{t}}M \cdot M = \mathrm{I}_2, \qquad \det(M) = 1. $$

Notre but est de démontrer l'énoncé suivant.

5. Voir par exemple [Pe, Chap. III, Proposition 4.8].

6. On peut raffiner cette condition en disant un degré $\leq \deg(P)/2$, mais cela ne sera pas utile pour les considérations de cet exercice.

7. L'existence d'un tel nombre premier n'est pas évidente. Mais le théorème de la progression arithmétique de Dirichlet (qu'on admettra ici) assure que c'est bien le cas.

Théorème 1. Il existe un isomorphisme de groupes

$$\mathrm{SO}_2(\mathbb{F}) \cong \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } -1 \text{ est un carré dans } \mathbb{F}\,; \\ \mathbb{Z}/(q+1)\mathbb{Z} & \text{si } -1 \text{ n'est pas un carré dans } \mathbb{F}. \end{cases}$$

Remarque. Si on propose cet énoncé en développement, il faudra bien sûr savoir expliquer rapidement comment on détermine si oui ou non -1 est un carré dans $\mathbb{F}$, en fonction de q.

5.1. **Préliminaires.** On commence par un résultat facile et classique.

Lemme 1. Soit $\mathbb{F}$ un corps fini de caractéristique p impaire. Alors pour tout $a \in \mathbb{F}$ et tous $b, c \in \mathbb{F}^\times$ il existe $x, y \in \mathbb{F}$ tels que

$$a = bx^2 + cy^2.$$

Démonstration. Soit q le cardinal de $\mathbb{F}$. Rappelons qu'il existe $\frac{q+1}{2}$ carrés dans $\mathbb{F}$ (puisque tout carré non nul est le carré d'exactement deux éléments de $\mathbb{F}$, qui sont opposés). Donc

$$\#\{a - bx^2 : x \in \mathbb{F}\} = \frac{q+1}{2} = \#\{cy^2 : y \in \mathbb{F}\}.$$

Comme $\frac{q+1}{2} + \frac{q+1}{2} > q$ ces deux sous-ensembles de $\mathbb{F}$ s'intersectent, ce qui fournit une solution à l'équation. □

Le lemme suivant s'applique à tout corps $\mathbb{F}$ (pas nécessairement fini). On note

$$\mathrm{S}^1(\mathbb{F}) = \{(x, y) \in \mathbb{F}^2 \mid x^2 + y^2 = 1\}.$$

Lemme 2. L'application

$$(x, y) \mapsto \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

induit une bijection

$$\mathrm{S}^1(\mathbb{F}) \xrightarrow{\sim} \mathrm{SO}_2(\mathbb{F}).$$

Démonstration. Si

$$M = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{F}),$$

alors M appartient à $\mathrm{SO}_2(\mathbb{F})$ si et seulement si on a

$$\begin{cases} a^2 + b^2 &= 1 \\ ac + bd &= 0 \\ c^2 + d^2 &= 1 \\ ad - bc &= 1 \end{cases}.$$

En particulier, dans ce cas le couple (a, b) appartient à $\mathrm{S}^1(\mathbb{F})$. D'autre part, si on fixe $(a, b) \in \mathrm{S}^1(\mathbb{F})$, alors le système linéaire

$$\begin{cases} ac + bd &= 0 \\ -bc + ad &= 1 \end{cases}$$

d'inconnues (c, d) a pour déterminant $a^2 + b^2 = 1$, et admet la solution évidente

$$c = -b, \quad d = a.$$

Donc cette solution est l'unique solution du système, et elle vérifie automatiquement

$$c^2 + d^2 = 1.$$

On a donc montré que

$$\mathrm{SO}_2(\mathbb{F}) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : (a,b) \in \mathrm{S}^1(\mathbb{F}) \right\},$$

ce qui achève la preuve. □

On suppose de nouveau pour le reste de cette sous-partie que $\mathbb{F}$ est fini. On suppose également que -1 n'est pas un carré dans $\mathbb{F}$ (ce qui implique que la caractéristique de $\mathbb{F}$ est impaire). Alors le polynôme X^2+1 est irréductible dans $\mathbb{F}[X]$, et donc $\mathbb{F}' := \mathbb{F}[X]/(X^2+1)$ est un corps, de cardinal q^2. On notera $\mathbf{i}$ l'image de X dans $\mathbb{F}'$.

Lemme 3. (1) Il existe un unique automorphisme de corps $\mathbb{F}$-linéaire

$$\varphi : \mathbb{F}' \xrightarrow{\sim} \mathbb{F}'$$

tel que $\varphi(\mathbf{i}) = -\mathbf{i}$. De plus on a $\varphi \circ \varphi = \mathrm{id}$, et si $a \in \mathbb{F}'$ on a

$$a \in \mathbb{F} \quad \Leftrightarrow \quad \varphi(a) = a.$$

(2) On considère l'application

$$N : \mathbb{F}' \to \mathbb{F}'$$

définie par $N(x) = x\varphi(x)$. Alors :

(a) pour tous $a, b \in \mathbb{F}'$ on a $N(ab) = N(a)N(b)$;
(b) on a $N^{-1}(\{0\}) = \{0\}$;
(c) l'image de N est $\mathbb{F}$, et ses fibres au-dessus de tous les éléments de $\mathbb{F}^\times$ sont non vides et ont même cardinal.

Démonstration. (1) Puisque $(-X)^2 + 1 = X^2 + 1$, le morphisme composé

$$\mathbb{F}[X] \xrightarrow{P(X) \mapsto P(-X)} \mathbb{F}[X] \twoheadrightarrow \mathbb{F}'$$

se factorise en un morphisme de $\mathbb{F}$-algèbres

$$\varphi : \mathbb{F}' \to \mathbb{F}'.$$

Comme $\mathbb{F}'$ est un corps ce morphisme doit être injectif, et donc bijectif puisque $\#\mathbb{F}'$ est fini, et finalement un isomorphisme de corps. Ceci prouve l'existence de φ. L'unicité est évidente puisque $\mathbb{F}' = \mathbb{F} \oplus \mathbb{F} \cdot \mathbf{i}$.

Le morphisme $\varphi \circ \varphi$ est $\mathbb{F}$-linéaire et envoie $\mathbf{i}$ sur $\mathbf{i}$; il doit donc être égal à id. Ensuite, si $a \in \mathbb{F}'$, en écrivant $a = a' + a''\mathbf{i}$ on voit que

$$\begin{aligned} \varphi(a) = a &\Leftrightarrow a' + a''\mathbf{i} = a' - a''\mathbf{i} \\ &\Leftrightarrow a'' = 0 \\ &\Leftrightarrow a \in \mathbb{F}. \end{aligned}$$

(Ici on a utilisé que la caractéristique de $\mathbb{F}$ est impaire, c'est-à-dire que 2 est inversible dans $\mathbb{F}$.)

(2) Les deux premières propriétés de N sont évidentes.

Pour la troisième, on remarque que pour tout $x \in \mathbb{F}'$ on a

$$\varphi(N(x)) = \varphi(x) \cdot \varphi \circ \varphi(x) = \varphi(x) \cdot x = N(x),$$

donc $N(x) \in \mathbb{F}$ d'après (1). Il reste à voir que les fibres de N au-dessus de tous les éléments de $\mathbb{F}^\times$ sont (i) non vides, et (ii) de même cardinal.

Pour (i), considérons $a \in \mathbb{F}^\times$. D'après le Lemme 1 il existe $x, y \in \mathbb{F}^2$ tels que $a = x^2 + y^2$. Alors $a = N(x + \mathbf{i}y)$, et donc $N^{-1}(\{a\}) \neq \varnothing$.

Pour (ii), considérons de nouveau $a \in \mathbb{F}^\times$, et fixons $a_0 \in \mathbb{F}'$ tel que $a = N(a_0)$. (On a nécessairement $a_0 \in (\mathbb{F}')^\times$.) Alors pour $x \in \mathbb{F}'$ on a

$$\begin{aligned} x \in N^{-1}(\{a\}) &\Leftrightarrow N(x) = a \\ &\Leftrightarrow N(x) = N(a_0) \\ &\Leftrightarrow N(x/a_0) = 1 \\ &\Leftrightarrow x/a_0 \in N^{-1}(1). \end{aligned}$$

Les applications $x \mapsto x/a_0$ et $y \mapsto a_0 y$ induisent donc des bijections réciproques

$$N^{-1}(\{a\}) \xrightarrow{\sim} N^{-1}(\{1\}).$$

Ceci montre que le cardinal de $N^{-1}(\{a\})$ ne dépend pas de a, ce qui achève la preuve. □

5.2. **Calcul du cardinal.** À partir de maintenant on se place dans la situation du Théorème 1, et on suppose donc $\mathbb{F}$ fini, de caractéristique p impaire. On va calculer le cardinal de $\mathrm{SO}_2(\mathbb{F})$ ou, de façon équivalente (d'après le lemme 2), de $\mathrm{S}^1(\mathbb{F})$.

Lemme 4. On a

$$\#\mathrm{S}^1(\mathbb{F}) = \begin{cases} q-1 & \text{si } -1 \text{ est un carré dans } \mathbb{F}\,; \\ q+1 & \text{si } -1 \text{ n'est pas un carré dans } \mathbb{F}. \end{cases}$$

Démonstration. Supposons tout d'abord que -1 est un carré dans $\mathbb{F}$. On peut alors choisir $\omega \in \mathbb{F}$ tel que $\omega^2 = -1$, et considérer la matrice

$$M = \begin{pmatrix} 1 & \omega \\ 1 & -\omega \end{pmatrix}.$$

Cette matrice a pour déterminant -2ω, qui est non nul puisque p est impair ; elle induit donc une bijection

$$\alpha : \mathbb{F}^2 \xrightarrow{\sim} \mathbb{F}^2.$$

Pour $(x, y) \in \mathbb{F}^2$, on observe que

$$\begin{aligned} (x,y) \in \mathrm{S}^1(\mathbb{F}) &\Leftrightarrow x^2 + y^2 = 1 \\ &\Leftrightarrow (x + \omega y)(x - \omega y) = 1 \\ &\Leftrightarrow \alpha(x,y) \in \{(z,t) \in \mathbb{F}^2 \mid zt = 1\}. \end{aligned}$$

Maintenant, il est clair que la projection sur la première coordonnée induit une bijection

$$\{(z,t) \in \mathbb{F}^2 \mid zt = 1\} \xrightarrow{\sim} \mathbb{F}^\times;$$

cet ensemble est donc de cardinal $q - 1$. Puisque α est une bijection, il en est de même pour $\mathrm{S}^1(\mathbb{F})$.

Supposons maintenant que -1 n'est pas un carré dans $\mathbb{F}$. Avec les notations du Lemme 3, on a alors pour $(x, y) \in \mathbb{F}^2$:

$$\begin{aligned} (x,y) \in \mathrm{S}^1(\mathbb{F}) &\Leftrightarrow x^2 + y^2 = 1 \\ &\Leftrightarrow (x + y\mathbf{i})(x - y\mathbf{i}) = 1 \\ &\Leftrightarrow x + y\mathbf{i} \in N^{-1}(\{1\}). \end{aligned}$$

Donc $\#\mathrm{S}^1(\mathbb{F}) = \#N^{-1}(\{1\})$. Maintenant puisque les fibres de N au-dessus de tous les éléments de $\mathbb{F}^\times$ sont de même cardinal, et celle au-dessus de 0 de cardinal 1 (voir le Lemme 3) on a

$$\#N^{-1}(\{1\}) = \frac{q^2-1}{q-1} = q+1,$$

ce qui achève la preuve. □

5.3. **Preuve du théorème.** On peut finalement démontrer le Théorème 1.

Preuve du Théorème 1. Supposons tout d'abord que -1 est un carré dans $\mathbb{F}$, et choisissons (comme dans le Lemme 4) $\omega \in \mathbb{F}$ tel que $\omega^2 = -1$. On considère alors l'application

$$\beta : \mathrm{SO}_2(\mathbb{F}) \to \mathbb{F}^\times$$

définie par

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mapsto a + \omega b.$$

pour $(a,b) \in \mathrm{S}^1(\mathbb{F})$. (Ici $a+\omega b$ est bien inversible puisque $(a+\omega b)(a-\omega b) = a^2+b^2 = 1$ si $(a,b) \in \mathrm{S}^1(\mathbb{F})$.) Pour (a,b) et (a',b') dans $\mathrm{S}^1(\mathbb{F})$ on a

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \cdot \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} aa'-bb' & -a'b-ab' \\ a'b+ab' & aa'-bb' \end{pmatrix}$$

et

$$(a+\omega b)(a'+\omega b') = (aa'-bb') + \omega(a'b+ab'),$$

de sorte que β est un morphisme de groupes.

Si $(a,b) \in \mathrm{S}^1(\mathbb{F})$ et $a+\omega b = 1$, alors $a-\omega b = (a+\omega b)^{-1} = 1$ ce qui implique que $2a = 2$ et $2b = 0$, c'est-à-dire $a = 1$ et $b = 0$ puisque p est impair. Le morphisme β est donc injectif. Puisque

$$\#\mathrm{SO}_2(\mathbb{F}) = q-1 = \#\mathbb{F}^\times$$

d'après le Lemme 4 c'est donc un isomorphisme, ce qui achève la preuve dans ce cas puisque $\mathbb{F}^\times$ est cyclique.

Supposons maintenant que -1 n'est pas un carré dans $\mathbb{F}$. Alors si $\mathbb{F}'$ est comme dans le lemme 3, $-1 = \mathbf{i}^2$ est un carré dans $\mathbb{F}'$, de sorte que $\mathrm{SO}_2(\mathbb{F}')$ est cyclique par le cas traité ci-dessus. Mais on a une injection naturelle

$$\mathrm{SO}_2(\mathbb{F}) \hookrightarrow \mathrm{SO}_2(\mathbb{F}'),$$

et tout sous-groupe d'un groupe cyclique est cyclique. Donc $\mathrm{SO}_2(\mathbb{F})$ est cyclique également. Comme il est de cardinal $q+1$ d'après le Lemme 4, ceci achève la preuve. □

6. Autres ressources sur cette leçon

`https://www.math.univ-paris13.fr/~boyer/enseignement/agreg/corps-finis.pdf`

Le sujet MG 2007 comporte 2 parties (III et V) proposant des calculs explicites dans le corps à 16 éléments, avec des applications à la cryptographie.

Références

[CG1] P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométries, Tome II*, Calvage & Mounet, 2015.

[CG2] P. Caldero, J. Germoni, *Nouvelles histoires hédonistes de groupes et de géométries, Tome II*, Calvage & Mounet, 2018.

[De] M. Demazure, *Cours d'algèbre : primalité, divisibilité, codes*, Cassini, 1997.

[Pe] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

[Pa] A. Paugam, *Agrégation de Mathématiques – Questions délicates en algèbre et géométrie*, Dunod, 2007. [8]

8. Attention ! Ce livre ne fait pas partie de la bibliothèque officielle du jury.