Leçon 123 : Corps finis. Applications.

Matei Lefebvre

2025/2026

$\mathbb{K}$, $\mathbb{L}$ et $\mathbb{M}$ seront des corps (commutatifs). On notera $\mathcal{P}$ l'ensemble des nombres premiers.

1 Construction des corps finis.

1.1 Extensions de corps et caractéristique.

[Per96], III.1.a et III.2.a

Proposition 1. *Si $\mathbb{L}/\mathbb{K}$ est une extension de corps avec $\mathbb{K}$ et $\mathbb{L}$ des corps finis, alors $|\mathbb{L}| = |\mathbb{K}|^n$ où $n = [\mathbb{L} : \mathbb{K}]$.*

Proposition 2 (Base télescopique)**.** *Supposons que $\mathbb{M}/\mathbb{L}$ et $\mathbb{L}/\mathbb{K}$ soient deux extensions finies avec $(y_1, \dots, y_m)$ une $\mathbb{L}$-base de $\mathbb{M}$ et $(x_1, \dots, x_l)$ une $\mathbb{K}$-base de $\mathbb{L}$. Alors, $(x_i y_j)_{(i,j)\in[\![1;l]\!]\times[\![1;m]\!]}$ est une $\mathbb{K}$-base de $\mathbb{M}$. En particulier, $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.*

Définition 3. *On appelle **sous-corps premier** de $\mathbb{K}$ le plus petit sous-corps de $\mathbb{K}$ et on le note $\mathbb{K}_0$.*

Proposition/Définition 4. $\varphi : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{K} \\ k & \mapsto & k.1 \end{array}$ *est un morphisme d'anneau. Son noyau est de la forme $n\mathbb{Z}$ avec $n = 0$ ou $n \in \mathcal{P}$. On note $n = \mathrm{car}(\mathbb{K})$ et on l'appelle la **caractéristique** de $\mathbb{K}$. On dit que $\mathbb{K}$ est de **caractéristique non nulle** lorsque $n = p \in \mathcal{P}$. De plus, φ induit un isomorphisme $\bar{\varphi} : \mathrm{Frac}(\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\sim} \mathbb{K}_0$.*

Remarque 5. *Si $\mathrm{car}(\mathbb{K}) = 0$, alors $\mathbb{K}_0 \simeq \mathbb{Q}$. Sinon, $\mathrm{car}(\mathbb{K}) = p \in \mathcal{P}$ et $\mathbb{K}_0 \simeq \mathbb{Z}/p\mathbb{Z}$ (on note également $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ vu en tant que corps).*

Proposition 6. *Si $|\mathbb{K}| < \infty$, alors :*

1. *$\mathrm{car}(\mathbb{K}) = p \in \mathcal{P}$ et donc $\mathbb{K}_0 \simeq \mathbb{F}_p$;*
2. *$|\mathbb{K}| = p^n$ avec $n \in \mathbb{N}^*$.*

Contre-exemple 7. *$\mathbb{F}_p(X)$ est un corps infini de caractéristique p.*

Remarque 8. *Les ensembles $\{p^n, n \in \mathbb{N}^*\}$ pour $p \in \mathcal{P}$ sont deux-à-deux disjoints donc $|\mathbb{K}| = p^n$ force $\mathrm{car}(\mathbb{K}) = p$.*

1.2 Morphisme de Frobenius.

[Per96], III.2.a
Dans cette partie, on suppose $\mathrm{car}(\mathbb{K}) = p \in \mathcal{P}$.

Proposition/Définition 9. *On note* $F = F_{\mathbb{K}} : \begin{array}{ccc} \mathbb{K} & \to & \mathbb{K} \\ x & \mapsto & x^p \end{array}$ *et on l'appelle* ***morphisme de Frobenius*** *de* $\mathbb{K}$*. C'est un morphisme de corps.*

Exemple 10. *Si* $\mathbb{K}$ *est fini, alors* F *est un automorphisme. Si* $\mathbb{K} = \mathbb{F}_p$*, alors* $F = \mathrm{id}_{\mathbb{F}_p}$.

Lemme 11. *Pour* $n \in \mathbb{N}^*$*, on note* $\mathrm{Fix}(F^{\circ n}) = \{x \in \mathbb{K}, F^{\circ n}(x) = x\}$*. C'est un sous-corps de* $\mathbb{K}$ *de cardinal au plus* p^n *avec égalité ssi* $X^{p^n} - X$ *est scindé sur* $\mathbb{K}$*. En outre,* $\mathrm{Fix}(F) = \mathbb{K}_0$.

1.3 Corps de rupture et corps de décomposition.

[Goz09], V
Ici, P est un polynôme de $\mathbb{K}[X]$.

Définition 12. *Supposons que* $\mathbb{L}/\mathbb{K}$ *et* $\mathbb{M}/\mathbb{K}$ *soient deux extensions de corps. Un morphisme* $\varphi : \mathbb{L} \to \mathbb{M}$ *est appelé un* $\mathbb{K}$***-morphisme*** *lorsque* $\forall x \in \mathbb{K}, \varphi(x) = x$.

Définition 13. *Supposons* P *irréductible sur* $\mathbb{K}$*. Un* ***corps de rupture*** *de* P *sur* $\mathbb{K}$ *est une extension* $\mathbb{L}/\mathbb{K}$ *telle que* $\mathbb{L} = \mathbb{K}(\alpha)$ *où* α *est une racine de* P *dans* $\mathbb{L}$.

Théorème 14. *Si* P *est irréductible sur* $\mathbb{K}$*, alors* $\mathbb{K}[X]/(P)$ *est un corps de rupture de* P *sur* $\mathbb{K}$*. De plus, deux corps de rupture de* P *sur* $\mathbb{K}$ *sont* $\mathbb{K}$*-isomorphes.*

Exemple 15. $\mathbb{C} = \mathbb{R}(i)$ *est le corps de rupture de* $X^2 + 1$ *sur* $\mathbb{R}$.

Définition 16. *Un* ***corps de décomposition*** *de* P *sur* $\mathbb{K}$ *est une extension* $\mathbb{L}/\mathbb{K}$ *telle que* P *soit scindé sur* $\mathbb{L}$ *et* $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_n)$ *où* $\alpha_1, \ldots, \alpha_n$ *sont les racines de* P *dans* $\mathbb{L}$.

Théorème 17. *Il existe un corps de décomposition de* P *sur* $\mathbb{K}$*, unique à* $\mathbb{K}$*-isomorphisme près. On le note* $\mathcal{D}_{\mathbb{K}}(P)$ *et on a* $[\mathcal{D}_{\mathbb{K}}(P) : \mathbb{K}] \leqslant (\deg P)!$.

1.4 Existence et unicité des corps finis.

[Goz09], VII.2 et VII.5 et [Per96], III.2.b
Soient $p \in \mathcal{P}$, $n \in \mathbb{N}^*$ et $q = p^n$.

Théorème 18. $\mathcal{D}_{\mathbb{F}_p}(X^q - X)$ *est un corps à* q *éléments. Réciproquement, si* $|\mathbb{K}| = q$*, alors* $\mathbb{K} = \mathcal{D}_{\mathbb{K}_0}(X^q - X)$ *(et on rappelle que* $\mathbb{K}_0 \simeq \mathbb{F}_p$*). En particulier, il existe un unique corps de cardinal* q *à isomorphisme près, on le note* $\mathbb{F}_q$ *(dans la suite, on notera abusivement* $\mathbb{K} = \mathbb{F}_q$ *pour tout corps* $\mathbb{K}$ *de cardinal* q*).*

Exemple 19. $P = 1 + X + X^2$ *est irréductible sur* $\mathbb{F}_2$ *donc* $\mathbb{F}_2[X]/(P)$ *est un corps de cardinal* $2^2 = 4$*, ainsi :* $\mathbb{F}_4 = \mathbb{F}_2[X]/(P)$*. C'est cette méthode qui est utilisée en pratique pour construire des corps de cardinal fini.*

Remarque 20. *Soit* $\mathbb{L}$ *un corps de cardinal* q *et* $\mathbb{K}$ *un sous-corps de* $\mathbb{L}$*. On a* $\mathbb{L}_0 = \mathbb{K}_0 = \mathbb{F}_p$ *donc* $|\mathbb{K}| = p^d$ *pour* $d \geqslant 1$ *et* $n = [\mathbb{L} : \mathbb{F}_p] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}_p] = [\mathbb{L} : \mathbb{K}]d$*. Ainsi,* $d \mid n$.

Lemme 21. *Soit* $d \mid n$*, alors* $X^{p^d} - X \mid X^{p^n} - X$ *dans* $\mathbb{K}[X]$ *(sans hypothèse sur* $\mathbb{K}$*).*

Théorème 22. *1. Si* $\mathbb{K}$ *est un sous-corps de* $\mathbb{F}_q$*, alors il existe* $d \mid n$ *tel que* $|\mathbb{K}| = p^d$ *;*

2. $\forall d \mid n$*, il existe un unique sous-corps* $\mathbb{K}$ *de cardinal* p^d *de* $\mathbb{F}_q$*. On a* $\mathbb{K} = \mathrm{Fix}(F^{\circ d})$.

Corollaire 23. $\mathbb{F}_{q'}$ *est un sous corps de* $\mathbb{F}_q \Leftrightarrow q$ *est une puissance de* q'.

Exemple 24. *Structure des sous-corps de* $\mathbb{F}_{12}$ *et* $\mathbb{F}_{30}$*, cf annexe ([Ulm18], XI.2).*

2 Structure interne.

On a toujours $p \in \mathcal{P}, n \in \mathbb{N}^*$ et $q = p^n$.

2.1 Étude du groupe multiplicatif.

[Goz09], VII.1

Théorème 25. *Tout sous-groupe fini du groupe multiplicatif $\mathbb{K}^*$ est cyclique (sans hypothèse sur $\mathbb{K}$).*

Corollaire 26. *$\mathbb{F}_q^*$ est cyclique.*

Exemple 27. *Tableau des $g = \min\{k \in [\![1, p-1]\!]\,,\ \bar{k}$ engendre $\mathbb{F}_p^\times\}$ pour $p \leqslant 50$ premier.*

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
g	1	2	2	3	2	2	3	2	5	2	3	2	6	3	5

Corollaire 28 (Théorème de l'élément primitif pour les corps finis)**.** *Si $\mathbb{K}$ et $\mathbb{L}$ sont deux corps finis avec $\mathbb{K} \subseteq \mathbb{L}$, alors $\exists \alpha \in \mathbb{L}$, $\mathbb{L} = \mathbb{K}(\alpha)$.*

Proposition 29. *Le produit des éléments de $\mathbb{F}_q^*$ vaut -1.*

Corollaire 30 (Théorème de Wilson)**.** *Soit $m \in \mathbb{N}, m \geqslant 2$, alors $m \in \mathcal{P} \Leftrightarrow (m-1)! \equiv -1[m]$.*

2.2 Carrés dans $\mathbb{F}_q$ et loi de réciprocité quadratique.

[Goz09], VII.7 et [Goz09], XII.2

Proposition 31.

- *Si $p = 2$, alors $\mathbb{F}_q^{*2} = \mathbb{F}_q^*$.*
- *Sinon $\mathbb{F}_q^{*2}$ est un sous-groupe d'indice 2 de $\mathbb{F}_q^*$. C'est le noyau du morphisme* $\begin{array}{ccc} \mathbb{F}_p^\times & \to & \{\pm 1\} \\ x & \mapsto & x^{\frac{q-1}{2}} \end{array}$.

  En particulier, $-1 \in \mathbb{F}_q^{*2} \Leftrightarrow q \equiv 1[4]$.

Corollaire 32. *Il existe une infinité de nombres premiers congrus à 1 modulo 4.*

On suppose dans la suite de cette partie que p et p' sont deux entiers premiers impairs distincts.

Définition 33 (Symboles de Legendre)**.** *Pour $x \in \mathbb{F}_p^*$, on définit le* ***symbole de Legendre*** *:*
$\left(\frac{x}{p}\right) = \begin{cases} 1 \text{ si } x \in \mathbb{F}_p^{*2} \\ -1 \text{ si } x \notin \mathbb{F}_p^{*2} \end{cases}$

Proposition 34. $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}}$

Remarque 35. *$x \mapsto \left(\frac{x}{p}\right)$ est donc un morphisme de groupe et ainsi, pour calculer $\left(\frac{x}{p}\right)$, il suffit de calculer $\left(\frac{a}{p}\right)$ pour a facteur premier de x.*

Définition 36 (Sommes de Gauss)**.** *Supposons que $\mathbb{K}$ est un corps de caractéristique* $\mathrm{car}(\mathbb{K}) \notin \{2; p\}$ *et contenant un élément $\omega \in \mathbb{K}^*$ d'ordre p ($\Leftrightarrow p \,|\, |\mathbb{K}| - 1$ si $\mathbb{K}$ est fini). Pour $a \in \mathbb{F}_p^*$, on pose $s(a) \coloneqq \sum_{x \in \mathbb{F}_p^*} \left(\frac{x}{p}\right) \omega^{ax}$, c'est la* ***somme de Gauss*** *associée à a. (Analogie avec la transformée de Fourier).*

D1

Proposition 37. *On a* $s(a) = \left(\frac{a}{p}\right) s(1)$ $\forall a \in \mathbb{F}_p^*$ *et* $s(1)^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p \in \mathbb{K}$.

Théorème 38 (Loi de réciprocité quadratique et deuxième loi complémentaire)**.** .

1. $\left(\frac{p}{p'}\right)\left(\frac{p'}{p}\right) = (-1)^{\frac{(p-1)(p'-1)}{4}}$
2. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

[Goz09], XII.2 et [Zav13], II.6
Remarque : besoin de définir les sommes de Gauss.

Remarque 39. *La seconde loi complémentaire se réécrit :* 2 *est un carré modulo* $p \Leftrightarrow 16 \mid p^2 - 1$. *Or, en écrivant* $p = a + 8k$, *on trouve :* $16 \mid p^2 - 1 \Leftrightarrow p \equiv \pm 1[8]$.

Exemple 40. $\left(\frac{67}{83}\right) = (-1)^{33.41}\left(\frac{83}{67}\right) = -\left(\frac{16}{67}\right) = -\left(\frac{2}{67}\right)^4 = -1$ *donc 67 n'est pas un carré modulo 83.*
$\left(\frac{47}{61}\right) = (-1)^{23.30}\left(\frac{61}{47}\right) = \left(\frac{14}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{7}{47}\right) \underset{47=6.8-1}{=} (-1)^{23.3}\left(\frac{47}{7}\right) = -\left(\frac{5}{7}\right) = -(-1)^{2.3}\left(\frac{2}{5}\right) = (-1)^2 = 1$ *donc 47 est un carré modulo 61.*

Corollaire 41 (Test de Pépin, 1877)**.** *Soit* $k \in \mathbb{N}^*$ *et* $F_k \coloneqq 2^{2^k} + 1$ *le k-ième* ***nombre de Fermat****. Alors,* F_k *est premier ssi* $3^{\frac{F_k-1}{2}} \equiv -1[F_k]$.

2.3 Groupe des automorphismes de $\mathbb{F}_q$.

[Goz09], VII.3
On rappelle que $q = p^n$.

Proposition 42. $\mathrm{Aut}(\mathbb{F}_q) = \mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$ *où le deuxième ensemble est l'ensemble des* $\mathbb{F}_p$*-automorphismes de* $\mathbb{F}_q$ *(i.e., tout automorphisme de* $\mathbb{F}_q$ *fixe* $\mathbb{F}_p$*).*

Théorème 43. $\mathrm{Aut}(\mathbb{F}_q)$ *est un groupe cyclique d'ordre n engendré par le morphisme de Frobenius F. [Rom21]*

3 Structure externe.

3.1 Polynômes irréductibles sur $\mathbb{F}_q$ et application aux polynômes irréductibles sur $\mathbb{Z}$.

[Goz09], VII.4 et [Per96], III.3 et III.exos

Définition 44. *On note* $\mathcal{K}(q,d)$ *l'ensemble des polynômes irréductibles de degré* $d \in \mathbb{N}^*$ *sur* $\mathbb{F}_q$ *et* $I(q,d) \coloneqq |\mathcal{K}(q,d)|$.

Théorème 45. *Soit* $m \in \mathbb{N}^*$, *alors* $X^{q^m} - X = \prod_{d \mid m} \prod_{P \in \mathcal{K}(q,d)} P$.

Application 46. *Supposons* $\mathbb{K} = \bigcup_{m\in\mathbb{N}^*} \mathbb{F}_{p^{m!}}$ *(qui est bien muni d'une structure naturelle de corps car l'union est croissante). Alors,* $\mathbb{K}$ *est algébriquement clos (tout polynôme sur* $\mathbb{K}$ *est scindé).*

Remarque 47. *En regardant les degrés dans le théorème, on trouve* $q^m = \sum_{d\,|\,m} I(q,d)$.

Définition 48 (Fonction d'inversion de Möbius)**.** *On définit* $\mu : \mathbb{N}^* \to \{-1;0;1\}$ *la* ***fonction d'inversion de Möbius*** *par* $\mu(n) = \begin{cases} 1 & si\ n = 1 \\ 0 & si\ n\ contient\ un\ facteur\ carré \\ (-1)^r & si\ n = p_1 \dots p_r\ avec\ p_1, \dots, p_r \in \mathcal{P}\ deux\text{-}à\text{-}deux\ distincts \end{cases}$

Proposition 49. $mI(q,m) = \sum_{d\,|\,m} \mu(\frac{m}{d}) q^d$

Exemple 50. $I(2,2) = 1$ *donc il n'y a qu'un seul polynôme irréductible de degré 2 sur* $\mathbb{F}_2$*, c'est* X^2+X+1. $I(3,2) = 3$ *donc il y a 3 polynômes irréductibles de degré 2 sur* $\mathbb{F}_3$*, ce sont* X^2+1, X^2+X+2 *et* X^2+2X+2.

Corollaire 51. *Il existe des polynômes irréductibles de tout degré sur* $\mathbb{F}_q$ *et* $I(q,m) \underset{m\to\infty}{\sim} \frac{q^m}{m}$.

Proposition 52. $mI(q,m)$ *est le nombre d'éléments de* $\mathbb{F}_{q^m}$ *qui ne sont dans aucun sous-corps propre de* $\mathbb{F}_{q^m}$ *contenant* $\mathbb{F}_q$.

Théorème 53 (Critère de réduction modulo un premier)**.** *Soit* $P = a_d X^d + \dots + a_0 \in \mathbb{Z}[X]$ *avec* $d \geqslant 1$ *et supposons* $a_d \notin p\mathbb{Z}$*. Notons* $\bar{P} = \bar{a_d} X^d + \dots + \bar{a_0} \in \mathbb{F}_p$ *le polynôme obtenu en réduisant les coefficients de* P *modulo* p*. Si* $\bar{P}$ *est irréductible sur* $\mathbb{F}_p$*, alors* P *est irréductible sur* $\mathbb{Q}$*. En particulier, si* P *est de plus primitif, alors* P *est irréductible sur* $\mathbb{Z}$.

Exemple 54. $X^3 - 1287X^2 + 308X + 35$ *se réduit en* $X^3 - X^2 + 1$ *modulo 2. Ce deuxième polynôme n'a pas de racine dans* $\mathbb{F}_2$ *et est de degré 3, il est donc irréductible sur* $\mathbb{F}_2$*. Ainsi, le premier polynôme est irréductible sur* $\mathbb{Z}$ *par le théorème.*

Proposition 55. *Soit* $P \in \mathbb{K}$ *de degré* $m > 0$*. Alors,* P *irréductible sur* $\mathbb{K} \Leftrightarrow P$ *n'a pas de racine dans toute extension de degré au plus* $\frac{m}{2}$ *de* $\mathbb{K}$.

Application 56. $X^p - X - 1$ *est irréductible sur* $\mathbb{F}_p$ *et donc également sur* $\mathbb{Z}$ *par le théorème précédent.*

Application 57. $X^4 + 1$ *est réductible sur* $\mathbb{F}_p$ *(p premier quelconque).*

Remarque 58. *On montre par ailleurs que* $X^4 + 1$ *est irréductible sur* $\mathbb{Z}$*, et donc que la réciproque du critère de réduction modulo p est fausse.*

Dbon

Théorème 59 (Algorithme de Berlekamp)**.** *Soit* $P = P_1 \dots P_r \in \mathbb{F}_q[X]$ *avec* $P_1, \dots, P_r$ *irréductibles 2 à 2 premiers entre eux. On note* $\begin{array}{rcl} S_P : \mathbb{F}_q[X]/(P) & \to & \mathbb{F}_q[X]/(P) \\ \overline{Q} & \mapsto & \overline{Q}^q = \overline{Q(X^q)} \end{array}$ *, c'est une application* $\mathbb{F}_q$*-linéaire. On a alors* $r = \dim(\ker(S_P - id)) = \deg(P) - \mathrm{rg}(S_P - id)$*. Si de plus* $r \geqslant 2$ *et* $\overline{V} \in \ker(S_P - id) \backslash \mathbb{F}_q$*, alors* $P = \prod_{\alpha\in\mathbb{F}_q} \mathrm{pgcd}(P, V - \alpha)$ *est une décomposition non triviale de* P.

Lemme 60. *Soit* $P \in \mathbb{F}_q[X]$*, alors :*

1. $\mathrm{pgcd}(P, P') = 1 \Leftrightarrow P$ *n'a pas de facteur carré.*

2. $\text{pgcd}(P, P') = P \Leftrightarrow \exists R \in \mathbb{F}_q[X], P = R^p$.

3. *Si on est dans aucun des deux cas précédents, alors* $P = \text{pgcd}(P, P').\dfrac{P}{\text{pgcd}(P, P')}$ *est une décomposition non triviale de* P.

(L'algo suivant est sûrement à mettre en annexe).

Algorithme 61 (de factorisation d'un polynôme $P \in \mathbb{F}_q[X]$)**.** *Soit* $P \in \mathbb{F}_q[X]$.
.Si P *est constant :*
. *Fin de l'algorithme.*
.Sinon :
. *On calcule* $D \coloneqq \text{pgcd}(P, P')$.
. *Si* $D = 1$ *:*
. *On applique l'algorithme de Berlekamp à* P.
. *Si* $D = P$ *:*
. *On trouve* $R \in \mathbb{F}_q[X]$ *tq* $P = R^p$ *(il suffit de mettre les coefficients de* P *à la puissance* p^{n-1}*).*
. *On applique l'algorithme à* R.
. *Sinon :*
. *On applique l'algorithme à* D *et* $\dfrac{P}{D}$.

[BMP05], V.3.2 et [Dem09], IX.6

3.2 Algèbre linéaire sur $\mathbb{F}_q$

[Per96], IV.5

Proposition 62. *Soit* m *un entier strictement positif.*

- $|GL_m(\mathbb{F}_q)| = (q^m - 1)(q^m - q)(q^n - q^2)\dots(q^m - q^{m-1})$
- $GL_m(\mathbb{F}_q)/SL_m(\mathbb{F}_q) \simeq \mathbb{F}_q^*$ *et donc* $|SL_m(\mathbb{F}_q)| = \dfrac{|GL_m(\mathbb{F}_q)|}{q-1}$

D2

Théorème 63. *Si* p *est impair alors :*
$SO_2(\mathbb{F}_q) \simeq \begin{cases} \mathbb{Z}/(q-1)\mathbb{Z} & si\ -1 \in \mathbb{F}_q^{*2} \\ \mathbb{Z}/(q+1)\mathbb{Z} & si\ -1 \notin \mathbb{F}_q^{*2} \end{cases}$
De plus, $SO_2(\mathbb{F}_{2^n}) \simeq (\mathbb{Z}/2\mathbb{Z})^n$.

[CG18], VIII.3

Dbon

Théorème 64. *Soient* E *un* $\mathbb{K}$*-ev de dimension finie et* $u \in \mathcal{L}(E)$*. On note* $a(u) \coloneqq \inf\{p \in \mathbb{N}, \ker(u^p) = \ker(u^{p+1})\}$ *et* $d(u) \coloneqq \inf\{q \in \mathbb{N}, \text{im}(u^q) = \text{im}(u^{q+1})\}$*. On a alors*

$$a(u) = d(u) =: p,\ E = \ker(u^p) \oplus \text{im}(u^p),\ u|_{\ker(u^p)} \text{ est nilpotent et } u|_{\text{im}(u^p)} \text{ est inversible.}$$

De plus, une telle décomposition de E *caractérise entièrement* u.

Application 65. *Il y a $q^{d(d-1)}$ matrices nilpotentes dans $M_d(\mathbb{F}_q)$.*

[CP22], I.3.67

Références

[Per96] D. Perrin. *Cours d'algèbre (Agrégation).* ELLIPSES, 1996. ISBN : 9782729855529.

[BMP05] V. Beck, J. Malick et G. Peyré. *Objectif Agrégation.* H&K, 2005. ISBN : 9782914010924.

[Dem09] M. Demazure. *Cours d'algèbre.* CASSINI, 2009. ISBN : 9782842251277.

[Goz09] I. Gozard. *Théorie de Galois : Niveau L3-M1.* ELLIPSES, 2009. ISBN : 9782729842772.

[Zav13] M. Zavidovique. *Un max de math.* CALVAGE&MOUNET, 2013. ISBN : 9782916352299.

[CG18] P. Caldero et J. Germoni. *Nouvelles histoires hédonistes de groupes et de géométries Tome 2.* CALVAGE&MOUNET, 2018. ISBN : 9782916352671.

[Ulm18] F. Ulmer. *Anneaux, corps, résultants - Algèbre pour L3/M1/agrégation.* ELLIPSES, 2018. ISBN : 9782340025752.

[Rom21] J.E. Rombaldi. *Mathématiques pour l'agrégation - Algèbre et géométrie.* DEBOECK, 2021. ISBN : 9782807332201.

[CP22] P. Caldero et M. Peronnier. *Carnet de voyage en Algébrie.* CALVAGE&MOUNET, 2022. ISBN : 9782493230034.