

# 101 : Groupe opérant sur un ensemble. Exemples d'applications.

Dans cette leçon,  $G$  désigne un groupe de neutre 1, et  $X$  désigne un ensemble.

## I. Action d'un groupe sur un ensemble

### A. Définitions et premiers exemples

**Définition 1** ([R] 19, [U] 27). Une action de  $G$  sur  $X$  est une application  $G \times X \rightarrow X$  définie par  $(g, x) \mapsto g \cdot x$  vérifiant

1.  $\forall (g, g') \in G^2, \forall x \in X, g' \cdot (g \cdot x) = (g'g) \cdot x$
2.  $\forall x \in X, 1 \cdot x = x$

Pour signifier que  $G$  agit sur  $X$ , on note  $G \curvearrowright X$ .

**Exemple 2** ([R] 19, [U] 28). —  $\mathfrak{S}(X) \curvearrowright X$  par  $\sigma \cdot x = \sigma(x)$   
— Si  $E$  est un espace vectoriel, alors  $GL(E) \curvearrowright E$  par  $\varphi \cdot x = \varphi(x)$   
—  $(g, x) \mapsto x$  est une action de  $G$  sur  $X$ , appelée action triviale.

**Proposition 3** ([R] 19, [U] 28). La donnée d'une action  $(g, x) \mapsto g \cdot x$  de  $G$  sur  $X$  équivaut à la donnée d'un morphisme  $\varphi : G \rightarrow \mathfrak{S}(X)$ ,  $g \mapsto [x \mapsto g \cdot x]$ , appelé morphisme associé à l'action de  $G$  sur  $X$ .

**Définition 4** ([R] 19/21, [U] 29). Soit  $x \in X$ . Alors :

- L'orbite de  $x$  est l'ensemble  $\text{Orb}(x) = \{g \cdot x \mid g \in G\}$  (aussi noté  $G \cdot x$ );
- Le stabilisateur de  $x$  est l'ensemble  $\text{Stab}(x) = \{g \in G \mid g \cdot x = x\}$ .

**Proposition 5** ([U] 34/37). 1.  $G \curvearrowright G$  par  $g \cdot h = ghg^{-1}$  (on l'appelle action par conjugaison). Le stabilisateur de  $h \in G$  est appelé centralisateur de  $h$ , et est noté  $C(h)$ .

2.  $G$  agit sur l'ensemble de ses sous-groupes par  $g \cdot H = gHg^{-1}$  (action par conjugaison). Le stabilisateur de  $H \leq G$  est appelé normalisateur de  $H$ , et est noté  $N(H)$ .

**Définition 6** ([R] 20, [U] 29/31). On dit que l'action de  $G$  sur  $X$  est transitive si elle n'a qu'une seule orbite, i.e. si  $\forall (x, y) \in X^2, \exists g \in G : g \cdot x = y$ .

On dit que l'action de  $G$  sur  $X$  est fidèle si  $\varphi$  est injective.

**Exemple 7** ([U] 31). —  $\mathfrak{S}_n \curvearrowright [1, n]$  transitivement par  $\sigma \cdot i = \sigma(i)$

- $G \curvearrowright G$  fidèlement par  $g \cdot h = gh$  (on l'appelle action par translation à gauche)
- Soit  $H$  un sous-groupe de  $G$ . L'action de  $G$  sur  $G/H$  définie par  $g \cdot xH = gxH$ , appelée action par translation à gauche, est transitive.

**Proposition 8** ([R] 21). Pour tout  $x \in X$ ,  $\text{Stab}(x)$  est un sous-groupe de  $G$ .

**Proposition 9** ([U] 30).  $x \mathcal{R} y \iff \exists g \in G : y = g \cdot x$  définit une relation d'équivalence sur  $X$  dont les classes sont les orbites de l'action de  $G$  sur  $X$ .

**Corollaire 10** ([U] 30). Les orbites partitionnent  $X$ .

**Exemple 11** ([U] 41). Soit  $\sigma \in \mathfrak{S}_n$ . Le groupe  $\langle \sigma \rangle$  agit sur  $[1, n]$  par  $\sigma^k \cdot i = \sigma^k(i)$ . Les orbites non ponctuelles sont les supports des cycles dans la décomposition en produit de cycles à supports disjoints de  $\sigma$ .

## B. Cas d'un groupe et d'un ensemble finis

Dans ce paragraphe, on suppose  $G$  et  $X$  finis. On pose  $n = \text{Card}(G)$ .

**Théorème 12** (de Cayley - [R] 21, [U] 31).  $G$  s'identifie à un sous-groupe de  $\mathfrak{S}_n$ .

**Proposition 13** ([R] ?, [U] ?).  $\forall (x, y) \in X^2, y \in \text{Orb}(x) \implies \exists g \in G : \text{Stab}(y) = g \text{Stab}(x) g^{-1}$ .

**Théorème 14** (Relation orbite-stabilisateur - [R] 21). Pour tout  $x \in X$ ,  $G/\text{Stab}(x)$  et  $\text{Orb}(x)$  sont équipotents (cela reste vrai si  $G$  est infini). Par conséquent,

$$\text{Card}(G) = \text{Card}(\text{Stab}(x)) \text{Card}(\text{Orb}(x))$$

**Théorème 15** (Équation aux classes - [R] 21). Soit  $\{x_1, \dots, x_r\}$  un système de représentants pour les orbites. Alors,

$$\text{Card } X = \sum_{i=1}^r \text{Card}(\text{Orb}(x_i)) = \sum_{i=1}^r \frac{\text{Card } G}{\text{Card}(\text{Stab}(x_i))}$$

**Exemple 16** ([R] 22). Si  $\text{Card } G$  est une puissance d'un nombre premier, alors son centre  $Z(G) := \{g \in G \mid \forall h \in G, ghg^{-1} = h\}$  n'est pas réduit à  $\{1\}$ .

Corollaire ([R] 23) : tout groupe d'ordre  $p^2$  avec  $p$  premier est abélien.

**Théorème 17** (Formule de Burnside - [R] 35). L'action de  $G$  sur  $X$  possède  $\frac{1}{\text{Card } G} \sum_{g \in G} \text{Card}(\text{Fix}(g))$  orbites, où  $\text{Fix}(g) = \{x \in X \mid g \cdot x = x\}$ .

**Exemple 18** ([C] 132). En moyenne, une permutation de  $[1, n]$  tirée aléatoirement a 1 point fixe.

**Exemple 19** ([C] 132). Si  $G$  n'est pas abélien, alors la probabilité de tirer simultanément deux éléments qui commutent vaut  $\frac{k}{n}$ , avec  $k$  le nombre de classes de conjugaison de  $G$ .

**Théorème 20** (de Cauchy - [R] 23). Soit  $p$  un nombre premier. Si  $p \mid \text{Card } G$ , alors  $G$  admet un élément d'ordre  $p$ .

## II. Applications

### A. En géométrie : les isométries des polytopes

**Théorème 21** ([R] 94). L'ensemble des isométries du plan conservant un triangle équilatéral est un groupe isomorphe à  $\mathfrak{S}_3$ .

**Proposition 22** ([R] 82). Soit  $\mathcal{C}$  un cube. L'ensemble des isométries de l'espace conservant  $\mathcal{C}$  est un groupe, noté  $\text{Is}(\mathcal{C})$ . On note  $\text{Is}^+(\mathcal{C})$  le sous-groupe de  $\mathcal{C}$  formé de rotations.

**Théorème 23** ([R] 85).  $\text{Is}^+(\mathcal{C}) \cong \mathfrak{S}_4$  et  $\text{Is}(\mathcal{C}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ .

**Théorème 24** ([R] 95). En notant  $\mathcal{T}$  le tétraèdre régulier, on a  $\text{Is}^+(\mathcal{T}) \cong \mathcal{A}_4$  et  $\text{Is}(\mathcal{T}) \cong \mathfrak{S}_4$ .

## B. Du côté des matrices

Dans ce paragraphe,  $K$  désigne un corps. On fixe  $(n, m) \in (\mathbb{N}^*)^2$ .

**Proposition 25** ([R] 184/185/199/195/206). *Les applications suivantes sont des actions :*

1. Translation à gauche :  $GL_n(K) \times \mathcal{M}_{n,m}(K) \rightarrow \mathcal{M}_{n,m}(K), (P, A) \mapsto PA$
2. Translation à droite :  $GL_n(K) \times \mathcal{M}_{n,m}(K) \rightarrow \mathcal{M}_{n,m}(K), (P, A) \mapsto AP^{-1}$
3. Similitude (ou conjugaison) :  $GL_n(K) \times \mathcal{M}_n(K) \rightarrow \mathcal{M}_n(K), (P, A) \mapsto PAP^{-1}$
4. Équivalence (ou action de Steiniz) :  $(GL_n(K) \times GL_m(K)) \times \mathcal{M}_{n,m}(K) \rightarrow \mathcal{M}_{n,m}(K), ((P, Q), A) \mapsto PAQ^{-1}$
5. Congruence :  $GL_n(K) \times \mathcal{M}_n(K) \rightarrow \mathcal{M}_n(K), (P, A) \mapsto {}^tPAP$

**Proposition 26** ([R] 184/185/?/195/207). *Dans l'ordre de la proposition précédente, les orbites sont caractérisées par :*

1. le noyau de  $A$
2. l'image de  $A$
3. les polynômes minimal et caractéristique de  $A$
4. Ça dépend de  $K$ ...

**Exemple 27.**  $\text{Diag}(1, 2, 2)$  et  $\text{Diag}(1, 1, 2)$  ont même polynôme minimal mais ne sont pas semblables : il faut donc bien les deux informations !

## C. Théorèmes de Sylow

Dans ce paragraphe, on se donne  $p$  premier, et on note  $\text{Card } G = p^\alpha m, m \wedge p = 1$ .

**Définition 28** ([U] 85). *Un  $p$ -Sylow de  $G$  est un sous-groupe de  $G$  de cardinal  $p^\alpha$ .*

$\text{Syl}_p(G)$  désigne l'ensemble des  $p$ -Sylow de  $G$ , et  $n_p := \text{Card}(\text{Syl}_p(G))$ .

**Théorème 29** (de Sylow - [U] 87). *Soit  $G$  un groupe d'ordre  $p^\alpha m, m \wedge p = 1$ . Alors,*

1.  $\text{Syl}_p(G) \neq \emptyset$
2.  $G$  agit transitivement sur  $\text{Syl}_p(G)$  par conjugaison
3.  $n_p \equiv 1 [p]$

**Définition 30.** *On dit que  $G$  est simple si les seuls sous-groupes de  $G$  distingués (i.e. fixe par l'action par conjugaison de  $G$ ) sont  $\{1\}$  et  $G$ .*

**Théorème 31** ([S] 277). *Si  $G$  est simple et d'ordre 60, alors  $G \cong A_5$ .*

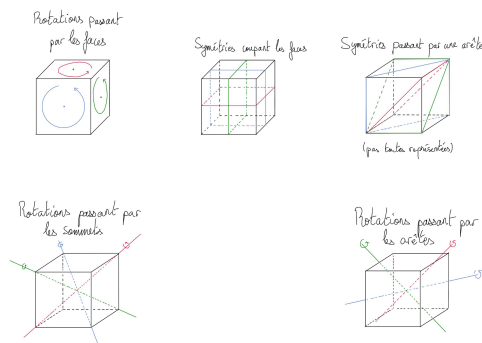
## Développements

- Développement 1 : Théorème 23
- Développement 2 : Théorème 31

## Références

- U *Théorie des groupes*, Félix Ulmer
- R *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition
- S *Algèbre pour la licence 3*, Szpirglas
- C *Carnets de voyage en Algèbre*, Caldero

FIGURE : Isométries du cube



# 105 : Groupe des permutations d'un ensemble fini. Applications.

## I. Permutations d'un ensemble fini

### A. Introduction

**Définition 1** ([R] 37). Soit  $E$  un ensemble. On note  $\mathfrak{S}(E)$  l'ensemble des bijections de  $E$  dans  $E$ . On l'appelle groupe symétrique de  $E$ . On notera plus simplement  $\mathfrak{S}_n = \mathfrak{S}([1, n])$ . On appelle permutation de  $E$  un élément de  $\mathfrak{S}(E)$ .

**Proposition 2.**  $\mathfrak{S}(E)$  est un groupe pour la composition, de neutre l'identité de  $E$ .

**Proposition 3** ([R] 39). Si  $E$  et  $F$  sont deux ensembles équipotents, alors  $\mathfrak{S}(E)$  et  $\mathfrak{S}(F)$  sont isomorphes (en tant que groupes).

**Proposition 4** ([R] 39). Pour  $n \geq 3$ ,  $\mathfrak{S}_3$  n'est pas commutatif.

Dans toute la suite, on étudiera  $\mathfrak{S}_n$  pour  $n \geq 3$ .

**Proposition 5** ([R] 40).  $\#\mathfrak{S}_n = n!$

**Notation** ([U] 41). Soit  $\sigma \in \mathfrak{S}_n$ . On représentera  $\sigma$  par la matrice  $2 \times n$  :

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

### B. Action naturelle de $\mathfrak{S}_n$ sur $[1, n]$ , conséquences

**Proposition 6** ([U] 41).  $\mathfrak{S}_n$  agit naturellement sur  $[1, n]$  par  $\sigma \cdot i = \sigma(i)$ . Le morphisme associé est l'identité de  $\mathfrak{S}_n$ .

**Définition 7** ([U] 42). On note  $\text{Fix}(\sigma)$  l'ensemble des points fixes de  $\sigma \in \mathfrak{S}_n$ . Son complémentaire dans  $[1, n]$  est appelé support de  $\sigma$ , et est noté  $\text{Supp}(\sigma)$ .

**Proposition 8** ([U] 43). Soit  $\sigma \in \mathfrak{S}_n$ . Le sous-groupe  $\langle \sigma \rangle$  agit sur  $[1, n]$  par restriction de l'action de  $\mathfrak{S}_n$ . Les orbites de cette action sont appelées  $\sigma$ -orbites. La réunion des  $\sigma$ -orbites ponctuelles est  $\text{Fix}(\sigma)$ . Les  $\sigma$ -orbites non ponctuelles partitionnent  $\text{Supp}(\sigma)$ .

**Exemple 9.** Soit  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$ . On a  $\text{Supp}(\sigma) = \{1, 2\} \sqcup \{4, 5\} = \langle \sigma \rangle \cdot \{1\} \sqcup \langle \sigma \rangle \cdot \{4\}$ .

**Définition 10** ([U] 43). Un  $k$ -cycle ( $2 \leq k \leq n$ ) est une permutation n'ayant qu'une seule  $\sigma$ -orbite non ponctuelle  $\{i_1, \dots, i_k\}$ . On la note  $\sigma = (i_1, \dots, i_k)$  pour signifier que  $\forall j \notin \{i_1, \dots, i_k\}, \sigma(j) = j$  et  $\sigma(i_j) = i_{j+1}$  en regardant les indices modulo  $k$ .

Un 2-cycle est appelé transposition.

**Proposition 11** ([U] 43).  $(i_1, i_2, \dots, i_k) = (i_2, i_3, \dots, i_k, i_1) = \dots = (i_k, i_1, i_2, \dots, i_{k-1})$

**Proposition 12.** Un  $k$ -cycle est d'ordre  $k$ .

### C. Décomposition d'une permutation, conséquences

**Proposition 13** ([U] 42). Deux permutations à supports disjoints commutent.

**Théorème 14** ([U] 43). Toute permutation se décompose de manière unique (à l'ordre des facteurs près) comme produit de cycles à supports disjoints.

**Algorithme 15** ([U] 43). Pour trouver une telle décomposition, il suffit de trouver les  $r$ -orbites.

1. On calcule  $\sigma(1), \sigma^2(1), \dots$  jusqu'à trouver  $\sigma^{k_1}(1) = 1$  (NB :  $k_1 \leq n$ );
2. On pose  $i_2 = \min([1, n] \setminus \langle \sigma \rangle \cdot \{1\})$ , et de même on calcule  $\sigma(i_2), \sigma^2(i_2), \dots$  jusqu'à trouver  $\sigma^{k_2}(i_2) = i_2$ ;
3. On itère jusqu'à épuiser  $[1, n]$ .

On a alors  $\sigma = (1, \sigma(1), \dots, \sigma^{k_1-1}(1)) \circ (i_2, \sigma(i_2), \dots, \sigma^{k_2-1}(i_2)) \circ \dots \circ (i_j, \sigma(i_j), \dots, \sigma^{k_j-1}(i_j))$

**Exemple 16.**  $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix} = (1, 3, 4)(5, 6)$

**Proposition 17** ([R] 44).  $(i_1, \dots, i_k) = (i_1, i_2)(i_2, i_3) \dots (i_{k-1}, i_k)$

**Corollaire 18** ([R] 44). Les transpositions engendrent  $\mathfrak{S}_n$ .

**Proposition 19** ([R] 45).  $\mathfrak{S}_n = \langle (i, i+1), 1 \leq i \leq n \rangle = \langle (1, i), 2 \leq i \leq n \rangle = \langle (1, 2), (1, 2, \dots, n) \rangle$

**Définition 20** ([U] 45). On appelle type de  $\sigma \in \mathfrak{S}_n$  la liste croissante des cardinaux des  $\sigma$ -orbites.

**Exemple 21.** Le type de  $(1, 2, 5)(3, 4)(7, 8) \in \mathfrak{S}_8$  est la liste  $[1, 2, 2, 3]$ .

**Proposition 22** ([U] 46). Deux permutations sont conjuguées dans  $\mathfrak{S}_n$  si, et seulement si, elles ont le même type. Cela décrit donc les classes de conjugaison de  $\mathfrak{S}_n$ .

**Proposition 23** ([U] 45). Si  $\sigma$  est du type  $[l_1, \dots, l_k]$ , alors  $\text{ord}(\sigma) = l_1 \vee \dots \vee l_k$ .

### D. Signature d'une permutation, groupe alterné

**Proposition 24** ([R] 47). Il existe un unique morphisme  $\varepsilon : \mathfrak{S}_n \rightarrow \{\pm 1\}$  qui envoie les transpositions sur  $-1$ . On appelle signature de  $\sigma$  la quantité  $\varepsilon(\sigma)$ .

**Corollaire 25.** La signature d'un  $k$ -cycle est  $(-1)^{k+1}$ .

**Proposition 26** ([R] 48).  $\forall \sigma \in \mathfrak{S}_n$ ,

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

En particulier, la signature mesure le nombre d'inversions.

**Définition 27** ([R] 48). On appelle  $n$ -ième groupe alterné le sous-groupe  $\mathcal{A}_n = \text{Ker}(\varepsilon)$ . C'est l'ensemble des permutations dîtes paires.

**Exemple 28.**  $\mathcal{A}_3 = \{\text{id}, (1, 2, 3), (1, 3, 2)\}$ .

**Proposition 29.**  $\#\mathcal{A}_n = \frac{n!}{2}$

**Théorème 30** ([R] 49). Pour  $n \geq 3$ , les 3-cycles engendrent  $\mathcal{A}_n$ , et  $y$  sont conjugués.

**Théorème 31** ([R] 50). Pour  $n \geq 5$ ,  $\mathcal{A}_n$  n'admet pas de sous-groupe distingué non trivial.

## II. Quelques applications du groupe symétrique

### A. En géométrie : les isométries des polytopes

**Théorème 32** ([R] 94). *L'ensemble des isométries du plan conservant un triangle équilatéral est un groupe isomorphe à  $\mathfrak{S}_3$ .*

**Proposition 33** ([R] 82). *Soit  $\mathcal{C}$  un cube. L'ensemble des isométries de l'espace conservant  $\mathcal{C}$  est un groupe, noté  $\text{Is}(\mathcal{C})$ . On note  $\text{Is}^+(\mathcal{C})$  le sous-groupe de  $\text{Is}(\mathcal{C})$  formé des rotations.*

**Théorème 34** ([R] 85).  $\text{Is}^+(\mathcal{C}) \cong \mathfrak{S}_4$  et  $\text{Is}(\mathcal{C}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ .

**Théorème 35** ([R] 95). *En notant  $\mathcal{T}$  le tétraèdre régulier, on a :  $\text{Is}(\mathcal{T}) \cong \mathfrak{S}_4$  et  $\text{Is}^+(\mathcal{T}) \cong \mathcal{A}_4$ .*

### Chez les (actions de) groupes

**Théorème 36** (de Cayley - [R] 53). *Tout groupe fini d'ordre  $n$  est isomorphe à un sous-groupe de  $\mathfrak{S}_n$ .*

**Proposition 37**. *Comme pour tout corps (commutatif)  $K$ ,  $\mathfrak{S}_n \curvearrowright GL_n(K)$ , tout groupe de garde  $n$  est isomorphe à un sous-groupe de  $GL_n(K)$ .*

**Exemple 38**. Soit  $D_{2 \times 4}$  le groupe des isométries du carré. Comme  $\#D_{2 \times 4} = 8$ ,  $D_{2 \times 4}$  est isomorphe à un sous-groupe de  $\mathfrak{S}_8$ . Noton  $\varphi$  un tel isomorphisme. Comme  $D_{2 \times 4} = \langle r, s \rangle$  où  $\text{ord}(r) = 4$ ,  $\text{ord}(s) = 2$  et  $\text{ord}(rs) = 2$ , on a  $\varepsilon \circ \varphi(s) = \varepsilon \circ \varphi(rs) = -1$ , donc  $\varepsilon \circ \varphi(r) = 1$ .

### C. Polynômes symétriques

**Définition 39** ([R] 55). *Un polynôme symétrique est un polynôme  $P \in K[X_1, \dots, X_n]$  tel que  $\forall \sigma \in \mathfrak{S}_n$ ,  $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$ .*

**Définition 40** ([R] 55). *Les polynômes symétriques élémentaires sont les*

$$\Sigma_{k,n} = \sum_{1 \leq i_1 \leq \dots \leq i_k \leq n} X_{i_1} \dots X_{i_k} \in K[X_1, \dots, X_n]$$

**Théorème 41** (ADMIS - [R] 55). *Pour tout polynôme symétrique  $P \in K[X_1, \dots, X_n]$ , il existe un unique polynôme  $Q \in K[\Sigma_{1,n}, \dots, \Sigma_{n,n}]$  tel que  $P(X_1, \dots, X_n) = Q(\Sigma_{1,n}, \dots, \Sigma_{n,n})$ .*

### D. En algèbre (multi-)linéaire

Dans ce paragraphe,  $E$  est un  $\mathbb{K}$ -espace vectoriel de dimension finie  $n$ . On fixe une base  $\mathcal{B} = (e_1, \dots, e_n)$  de  $E$ .

**Définition 42** ([R] 545). *Une forme  $k$ -linéaire sur  $E$  est une application  $\varphi : E^k \rightarrow \mathbb{K}$  telle que pour tout  $i \in \llbracket 1, n \rrbracket$ , pour tout  $(x_1, \dots, x_k) \in E^k$ ,  $\varphi(x_1, \dots, x_{i-1}, \cdot, x_{i+1}, \dots, x_k)$  est linéaire.*

On note  $\bigotimes^k E^*$  l'ensemble des formes  $k$ -linéaires sur  $E$ .

**Proposition 43** ([R] 546).  $(e_{i_1}^* \otimes \dots \otimes e_{i_k}^*)_{1 \leq i_1 < \dots < i_k \leq n}$  est une base de  $\bigotimes^k E^*$ , où pour  $(x_1, \dots, x_k) \in E^k$ ,  $e_{i_1}^* \otimes \dots \otimes e_{i_k}^*(x_1, \dots, x_k) = e_{i_1}^*(x_1) \dots e_{i_k}^*(x_k)$ .

**Définition 44** ([R] 546). *Une forme  $k$ -linéaire alternée est une forme  $k$ -linéaire  $\varphi \in \bigotimes^k E^*$  telle que  $\forall \sigma \in \mathfrak{S}_k$ ,  $\forall (x_1, \dots, x_k) \in E^k$ ,  $\varphi(x_{\sigma(1)}, \dots, x_{\sigma(k)}) = \varepsilon(\sigma)\varphi(x_1, \dots, x_k)$ .*

On note  $\bigwedge^k E^*$  l'espace des formes  $k$ -linéaires alternées sur  $E$ .

**Proposition 45**.  $(e_{i_1}^* \wedge \dots \wedge e_{i_k}^*)_{1 \leq i_1 < \dots < i_k \leq n}$  est une base de  $\bigwedge^k E^*$ , où pour  $(x_1, \dots, x_k) \in E^k$ ,  $e_{i_1}^* \wedge \dots \wedge e_{i_k}^*(x_1, \dots, x_k) = \sum_{\sigma \in \mathfrak{S}_k} \varepsilon(\sigma) e_{i_1}^*(x_{\sigma(1)}) \dots e_{i_k}^*(x_{\sigma(k)})$ .

**Corollaire 46**. On a  $\dim \left( \bigwedge^k E^* \right) = \binom{n}{k}$ .

**Définition 47**. On appelle déterminant dans la base  $\mathcal{B}$  l'unique forme  $n$ -linéaire alternée  $\det_{\mathcal{B}}$  sur  $E$  vérifiant  $\det_{\mathcal{B}}(\mathcal{B}) = 1$ . (La famille  $(\det_{\mathcal{B}})$  est une base de  $\bigwedge^n E^*$ .)

**Proposition 48** ([R] 547).  $\forall (x_1, \dots, x_n) \in E^n$ ,  $\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) e_1^*(x_{\sigma(1)}) \dots e_n^*(x_{\sigma(n)})$ .

### E. Résultats en probabilités

**Définition 49** ([R] 51). On appelle dérangement une permutation sans point fixes.

**Proposition 50**. Notons  $d_n$  le nombre de dérangements de  $\llbracket 1, n \rrbracket$ . Alors  $d_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$ . En particulier, la probabilité de choisir un dérangement en tirant au hasard une permutation de  $\llbracket 1, n \rrbracket$  tend vers  $\frac{1}{e}$  quand  $n \rightarrow +\infty$ .

**Proposition 51** ([C]). Soit  $X$  la variable aléatoire qui compte le nombre de points fixes d'une permutation aléatoirement choisie dans  $\mathfrak{S}_n$ . Alors  $\mathbb{E}[X] = \mathbb{V}[X] = 1$ .

### F. Groupes simples d'ordre 60

Dans ce paragraphe, on se donne  $p$  premier, et on note  $\#G = p^\alpha m$ ,  $m \wedge p = 1$ .

**Définition 52** ([U] 85). *Un  $p$ -Sylow de  $G$  est un sous-groupe de  $G$  de cardinal  $p^\alpha$ .*

**Notation**.  $\text{Syl}_p(G)$  désigne l'ensemble des  $p$ -Sylow de  $G$ , et  $n_p = \# \text{Syl}_p(G)$ .

**Théorème 53** (de Sylow - [U] 87). *Soit  $G$  un groupe d'ordre  $p^\alpha m$ ,  $p$  premier et  $m \wedge p = 1$ .*

1.  $\text{Syl}_p(G) \neq \emptyset$
2.  $G$  agit transitivement sur  $\text{Syl}_p(G)$  par conjugaison
3.  $n_p \equiv 1 [p]$  (donc  $n_p \mid m$ ).

**Définition 54**. On dit que  $G$  est simple si les seuls sous-groupes de  $G$  distingués (i.e. fixe par l'action par conjugaison de  $G$ ) sont  $\{1\}$  et  $G$ .

**Théorème 55** ([S] - 277). *Si  $G$  est simple et d'ordre 60, alors  $G \cong \mathcal{A}_5$ .*

### Développements

- Développement 1 : Théorème 34
- Développement 2 : Théorème 55

### Références

- R *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition
- U *Théorie des groupes*, Félix Ulmer
- S *Algèbre pour la licence 3*, Szpirglas
- C *Carnets de voyage en Algèbre*, Caldero

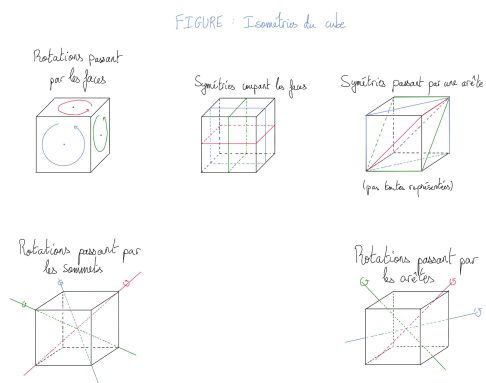


FIGURE 1.1 – Isométries du cube



# 106 : Groupe linéaire d'un espace vectoriel de dimension finie $E$ , sous-groupes de $GL(E)$ . Applications

Dans cette leçon,  $K$  est un corps commutatif, et  $E$  est un  $K$ -espace vectoriel de dimension finie  $n \geq 1$ .

## I. Endomorphismes inversibles d'un espace vectoriel

### A. Introduction au groupe linéaire

**Théorème 1** ([Rb] 139). — L'ensemble  $\mathcal{L}(E)$  des endomorphismes de  $E$  est un anneau pour  $+$  et  $\circ$ , dont le groupe des inversibles est noté  $GL(E)$ , et est appelé groupe linéaire de  $E$ .

— Similairement, l'ensemble  $\mathcal{M}_n(K)$  des matrices carrées de taille  $n \times n$  est un anneau pour  $+$  et  $\times$ , dont le groupe des inversibles est noté  $GL_n(K)$ , appelé groupe linéaire d'ordre  $n$  sur  $K$ .

**Remarque 2** ([Rb] 140). Étant donnée une base  $\mathcal{B}$ , l'application  $u \mapsto \text{Mat}_{\mathcal{B}}(u)$  induit un isomorphisme entre  $GL(E)$  et  $GL_n(K)$ .

**Définition 3** ([Rb] 141). On note  $SL(E)$  (resp.  $SL_n(K)$ ) le noyau du morphisme  $\det$  de  $GL(E)$  (resp.  $GL_n(K)$ ) dans  $K^\times$ . On l'appelle groupe spécial linéaire de  $E$  (resp. groupe spécial linéaire d'ordre  $n$  sur  $K$ ).

**Théorème 4** ([Rb] 140). Soit  $u \in \mathcal{L}(E)$ . Comme  $\dim E < +\infty$ , sont équivalentes :

1.  $u \in GL(E)$
2. (a)  $u$  est injectif  
(b)  $\text{Ker } u = \{0\}$   
(c)  $\exists v \in \mathcal{L}(E) : v \circ u = \text{id}_E$
3. (a)  $u$  est surjectif  
(b)  $\text{Im } u = E$   
(c)  $\exists v \in \mathcal{L}(E) : u \circ v = \text{id}_E$
4. L'image par  $u$  d'une base de  $E$  est une base de  $E$
5.  $\det(u) \neq 0$

**Remarque 5.** Une matrice  $A$  est inversible si, et seulement si, ses colonnes forment une base de  $K^n$ , et si, et seulement si, ses lignes forment une base de  $K^n$ .

**Définition 6.** On dit que  $u \in \mathcal{L}(E)$  est une homothétie de rapport  $\lambda \in K^\times$  si  $\forall x \in E, u(x) = \lambda x$ .

**Proposition 7.** Une homothétie de rapport  $\lambda \in K^\times$  est inversible, d'inverse l'homothétie de rapport  $1/\lambda$ .

**Proposition 8** ([Rb] e168). Les homothéties sont les seuls endomorphismes à stabiliser toute droite.

### B. Opérations élémentaires

Soit  $A \in \mathcal{M}_n(K)$ . On note  $L_1, \dots, L_p$  les lignes de  $A$ , et  $C_1, \dots, C_n$  ses colonnes.

**Définition 9** ([Bu] 315-317). Soient  $\alpha \in K^\times, (i, j) \in \llbracket 1, n \rrbracket^2$  tel que  $i \neq j$  et  $\sigma \in \mathfrak{S}_n$ . On définit les matrices suivantes :

— Matrice de dilatation  $D_i(\alpha) = \text{diag}(1, \dots, 1, \alpha, 1, \dots, 1) \in GL_n(K)$  ( $\alpha$  est à la  $i$ -ième position)

— Matrice de transvection  $T_{i,j}(\alpha) = I_n + \alpha E_{i,j} \in GL_n(K)$

— Matrice de permutation  $P_\sigma = (\delta_{i, \sigma(j)})_{1 \leq i, j \leq n} \in GL_n(K)$

**Définition 10.** On définit les opérations élémentaires sur les colonnes :

- $C_i \leftarrow \alpha C_i$  : on remplace  $C_i$  par  $\alpha C_i$
- $C_i \leftarrow C_i + \alpha C_j$  : on remplace  $C_i$  par  $\alpha C_i + \alpha C_j$
- $C_i \longleftrightarrow C_j$  : on échange  $C_i$  et  $C_j$

**Théorème 11** ([Bu] 315-318). On a les correspondances suivantes entre opérations élémentaires et multiplication matricielle :

- $D_i(\alpha)A \iff L_i \leftarrow \alpha L_i$
- $T_{i,j}(\alpha)A \iff L_i \leftarrow L_i + \alpha L_j$
- $P_{(i,j)}A \iff L_i \longleftrightarrow L_j$

et

- $AD_i(\alpha) \iff C_i \leftarrow \alpha C_i$
- $AT_{i,j}(\alpha) \iff C_i \leftarrow C_i + \alpha C_j$
- $AP_{(i,j)} \iff C_i \longleftrightarrow C_j$

**Proposition 12.**  $\sigma \mapsto P_\sigma$  est un morphisme de groupes injectif de  $\mathfrak{S}_n$  dans  $GL_n(K)$ .

## II. Structure de $GL(E)$ , sous-groupe orthogonal

### A. Structure de groupe

**Théorème 13** (Pivot de Gauss - [Rb] 191). Pour toute matrice de rang  $r$ , il existe une suite d'opérations élémentaires qui transforme cette matrice en la matrice  $J_{n,r} = \text{diag}(I_r, O_{n-r})$ . Plus précisément, si  $\text{rg } A = n$ , alors il existe  $\sigma \in \mathfrak{S}_n$  et des matrices de transvection  $T_1, \dots, T_p$  telles que  $A = P_\sigma T_1 \dots T_p D_\alpha$  où  $D_\alpha$  est la matrice de dilatation  $D_\alpha$  de rapport  $\alpha = \det A$ .

**Corollaire 14** ([Rb] 154, 153). — Les matrices de transvection et de dilatation engendrent  $GL_n(K)$  ;

— Les matrices de transvection engendrent  $SL_n(K)$ .

**Corollaire 15** ([Rb] 141).  $GL(E)/SL(E) \cong K^\times$

**Corollaire 16** ([Rb] 141). —  $Z(GL(E)) = K^\times \text{id}_E$  (c'est l'ensemble des homothéties) ;

—  $Z(SL(E)) = \mathbb{U}_n(K) \text{id}_E$ , où  $\mathbb{U}_n(K) = \{\lambda \in K^\times \mid \lambda^n = 1\}$ .

### B. Le groupe spécial orthogonal

Soit  $q$  une forme quadratique sur  $E$ , de forme polaire  $\varphi$ . Supposons  $\text{car } K \neq 2$ .

**Définition 17** ([P] 123-124). — Le groupe orthogonal de  $(E, q)$  est  $O(q) = \{u \in \mathcal{L}(E) \mid q \circ u = q\}$

- Le groupe spécial orthogonal de  $(E, q)$  est  $SO(q) = \{u \in O(q) \mid \det u = 1\}$
- Lorsque  $\varphi$  est le produit scalaire canonique relativement à une base donnée, on note  $O(E) = O(q) = \{u \in \mathcal{L}(E) \mid {}^t u \circ u = \text{id}_E\}$  et  $SO(E) = SO(q) = \{u \in O(E) \mid \det u = 1\}$ .
- On note également  $O_n(K) = \{M \in \mathcal{M}_n(K) \mid {}^t M M = I_n\}$  et  $SO_n(K) = \{M \in O_n(K) \mid \det M = 1\}$ .

**Proposition 18** ([Rb] 722). Si  $\mathcal{B}$  est une base orthonormale de  $E$ , alors  $u \in O(E) \iff \text{Mat}_{\mathcal{B}}(u) \in O_n(K)$ .

**Théorème 19** (de réduction des isométries - [Rb] 727). Soit  $u \in O(\mathbb{R}^n)$ . Il existe une base orthonormale  $\mathcal{B}$  de  $\mathbb{R}^n$  telle que  $\text{Mat}_{\mathcal{B}}(u) = \text{diag}(R(\theta_1), \dots, R(\theta_r), \varepsilon_1, \dots, \varepsilon_p)$  où  $R(\theta_i) = \begin{pmatrix} \cos \theta_i & -\sin \theta_i \\ \sin \theta_i & \cos \theta_i \end{pmatrix}$  et  $\varepsilon_i = \pm 1$ .

**Remarque 20** ([P] 146).  $SO_2(\mathbb{R}) = \{R(\theta) \mid \theta \in \mathbb{R}\} \cong \mathbb{R}/2\pi\mathbb{Z}$ .

**Théorème 21** ([C] 50). Soient  $p$  premier,  $r \geq 1$  et  $q = p^r$ .

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

**Définition 22** ([P] 125). Soit  $u \in O(q)$  telle que  $u^2 = \text{id}_E$ .

On dit que  $u$  est une réflexion si  $\dim(\text{Ker}(u + \text{id}_E)) = 1$ , i.e. si  $u$  est une symétrie par rapport à un hyperplan.

On dit que  $u$  est un renversement si  $\dim(\text{Ker}(u + \text{id}_E)) = 2$ , i.e. si  $u$  est une symétrie par rapport à un plan.

On suppose désormais que  $E$  est un  $\mathbb{R}$ -espace vectoriel de dimension finie  $n \geq 1$ , et que  $q$  est définie positive.

**Théorème 23** ([P] 143). Tout élément de  $O(q)$  est produit d'au plus  $n$  réflexions.

**Lemme 24**. Si  $n \geq 3$ , alors pour toutes réflexions  $\tau_1$  et  $\tau_2$ , il existe deux renversements  $\sigma_1$  et  $\sigma_2$  tels que  $\tau_1 \tau_2 = \sigma_1 \sigma_2$ .

**Théorème 25**. Pour  $n \geq 3$ , tout élément de  $SO(q)$  est produit d'au plus  $n$  renversements.

**Remarque 26**. Ces théorèmes restent vrais si  $E$  est un espace vectoriel de dimension finie sur un corps  $K$  de caractéristique  $\neq 2$ , et si  $q$  est non dégénérée (Cartan, Dieudonné).

### III. Topologie dans $GL(E)$

Dans ce paragraphe,  $K$  désigne  $\mathbb{R}$  ou  $\mathbb{C}$ .

**Proposition 27** ([Rb] 160-161).  $GL(E)$  est ouvert dans  $(\mathcal{L}(E), \|\cdot\|)$  et  $u \mapsto u^{-1}$  est continue.

**Proposition 28**. —  $GL_n(\mathbb{C})$  et  $SL_n(K)$  sont connexes ;  
—  $GL_n(\mathbb{R})$  a deux composantes connexes.

**Proposition 29**.  $O_n(\mathbb{R})$  et  $SO_n(\mathbb{R})$  sont compacts.

**Théorème 30** (Décomposition polaire - [Rb] 740).

$$O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R}) \rightarrow GL_n(\mathbb{R}) \\ (H, S) \mapsto HS$$

est un homéomorphisme.

## Développements

- Développement 1 : Théorème 21
- Développement 2 : Théorème 23, Lemme 24 et Théorème 25

## Références

- Rb *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition
- P *Cours d'algèbre*, Perrin
- B *Algèbre et géométrie : CAPES et Agrégation*, Pierre Burg
- C *Nouvelles histoires hédonistes de groupes et géométries*, P. Caldero, J. Germoni

# 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$ . Applications.

Dans toute la leçon,  $n \in \mathbb{N} \setminus \{0, 1\}$  et  $p$  est un nombre premier.

## I. L'anneau $\mathbb{Z}/n\mathbb{Z}$

### A. Rappels d'arithmétique des entiers

**Théorème 1** (division euclidienne - [R] 279).  $\forall(a, b) \in \mathbb{Z}^2, \exists!(q, r) \in \mathbb{Z}^2 :$

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

**Définition 2** ([R] 279). Soit  $(a, b) \in \mathbb{Z}^2$ . On dit que  $a$  est congru à  $b$  modulo  $n$ , et on note  $a \equiv b[n]$  si  $n$  divise  $b - a$ .

**Proposition 3** ([R] 280). Soit  $(a, b, c, d) \in \mathbb{Z}^4$  tel que  $a \equiv b[n]$  et  $c \equiv d[n]$ . Alors  $a + c \equiv b + d[n]$  et  $ac \equiv bd[n]$ .

### B. Construction

**Lemme 4.** Tout idéal de  $\mathbb{Z}$  est principal, et admet un unique générateur positif.

**Définition 5** ([R] 280). Le quotient de l'anneau  $(\mathbb{Z}, +, \times)$  par son idéal  $n\mathbb{Z}$  est l'anneau noté  $\mathbb{Z}/n\mathbb{Z}$ . On note  $\bar{a}$  l'image de  $a \in \mathbb{Z}$  dans  $\mathbb{Z}/n\mathbb{Z}$ .

**Remarque 6.**  $\bar{a} = \bar{b} \iff a \equiv b[n]$

**Proposition 7** ([R] 280).  $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ , et les lois sont données par Prop 3 et Rq 6.

**Exemple 8.**  $\mathbb{Z}/3\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}\} = \{\bar{9}, \bar{64}, \bar{-7}\}$ , et on a  $\bar{1} + \bar{2} = \overline{1+2} = \bar{3} = \bar{0}$ , mais aussi  $\bar{1} \times \bar{2} = \overline{1 \times 2} = \bar{2}$ .

### C. Structure d'anneau

**Proposition 9** ([R] 283). L'ensemble des inversibles  $\mathbb{Z}/n\mathbb{Z}$  est :

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{k} \in \mathbb{Z}/n\mathbb{Z} \mid k \wedge n = 1\}$$

L'ensemble des diviseurs de 0 de  $\mathbb{Z}/n\mathbb{Z}$  est :

$$D_0(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z} \setminus [(\mathbb{Z}/n\mathbb{Z})^\times \cup \{0\}]$$

**Exemple 10.**  $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ , et  $D_0(\mathbb{Z}/8\mathbb{Z}) = \{\bar{2}, \bar{4}, \bar{6}\}$ .

**Proposition 11** ([R] 241 et 281). Les idéaux propres de  $\mathbb{Z}/n\mathbb{Z}$  sont les  $d\mathbb{Z}/n\mathbb{Z}$  avec  $d \mid n$ ,  $d \notin \{1, n\}$ . De plus,  $(d\mathbb{Z}/n\mathbb{Z}, +) \cong (\mathbb{Z}/\frac{n}{d}\mathbb{Z}, +)$ .

**Corollaire 12.**  $\mathbb{Z}/n\mathbb{Z}$  est principal.

**Corollaire 13.** L'ensemble des générateurs de  $\mathbb{Z}/n\mathbb{Z}$  est  $(\mathbb{Z}/n\mathbb{Z})^\times$ .

**Exemple 14.** Les idéaux propres de  $\mathbb{Z}/6\mathbb{Z}$  sont  $2\mathbb{Z}/6\mathbb{Z}$  et  $3\mathbb{Z}/6\mathbb{Z}$ , respectivement isomorphes à  $\mathbb{Z}/3\mathbb{Z}$  et  $\mathbb{Z}/2\mathbb{Z}$ .

**Proposition 15** ([R] 295-282).  $\forall n, m \geq 2$ ,

$$\text{Hom}_{gr}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n \wedge m)\mathbb{Z},$$

$$\text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times,$$

$$\text{Hom}_{Ann}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \begin{cases} \{k \bmod n \mapsto k \bmod m\} & \text{si } m \mid n \\ \emptyset & \text{sinon} \end{cases}$$

## D. Le corps $\mathbb{Z}/p\mathbb{Z}$

**Théorème 16.** Les assertions suivantes sont équivalentes :

1.  $\mathbb{Z}/n\mathbb{Z}$  est un corps ;
2.  $\mathbb{Z}/n\mathbb{Z}$  est intègre ;
3.  $n$  est premier.

**Corollaire 17** ([R] 292).  $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ .

**Contre-exemple 18.** C'est très faux pour  $n$  non premier !  $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$  n'a même pas 7 éléments !

## II. Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

### A. Préambule : le théorème des restes chinois

**Théorème 19** (des restes chinois - [R] 285). Soit  $(a_1, \dots, a_d) \in (\mathbb{N} \setminus \{0, 1\})^d$ . Les entiers,  $a_1, \dots, a_d$  sont deux à deux premiers si, et seulement si, les anneaux  $\mathbb{Z}/a_1 \dots a_d \mathbb{Z}$  et  $\mathbb{Z}/a_1 \mathbb{Z} \times \dots \times \mathbb{Z}/a_d \mathbb{Z}$  sont isomorphes.

Le cas échéant, il existe  $(u_1, \dots, u_d) \in \mathbb{Z}^d$  tel que  $\sum_{i=1}^d a_i b_i = 1$ , où  $b_i = \frac{a_1 \dots a_d}{a_i}$ . L'application :

$$\begin{aligned} \bar{\varphi} : \mathbb{Z}/a_1 \dots a_d \mathbb{Z} &\rightarrow \mathbb{Z}/a_1 \mathbb{Z} \times \dots \times \mathbb{Z}/a_d \mathbb{Z} \\ x \bmod a_1 \dots a_d &\mapsto (x \bmod a_1, \dots, x \bmod a_d) \end{aligned}$$

est un isomorphisme d'anneaux, de réciproque :

$$\bar{\varphi}^{-1} : (x_1 \bmod a_1, \dots, x_d \bmod a_d) \mapsto \sum_{i=1}^d x_i a_i b_i \bmod a_1 \dots a_d$$

### B. Fonction indicatrice d'Euler

**Définition 20** ([R] 283). L'indicatrice d'Euler est :  $\varphi : n \mapsto \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{k \in [1, n] \mid k \wedge n = 1\}$ .

**Exemple 21.**  $\varphi(8) = 4$  d'après Exemple 10.

**Proposition 22** ([R] 288). Si  $a \wedge b = 1$ , alors  $\varphi(ab) = \varphi(a)\varphi(b)$ . Pour tout  $\alpha \in \mathbb{N}^*$ ,  $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ .

**Corollaire 23** ([R] 288). Si  $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$  est la décomposition de  $n$  en produit de facteurs premiers, alors :

$$\varphi(n) = \prod_{i=1}^r p_i^{\alpha_i-1}(p_i-1) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

**Exemple 24.**  $\varphi(90) = \varphi(3^2)\varphi(2)\varphi(5) = 3(3-1)(2-1)(5-1) = 24$

**Théorème 25** (d'Euler - [R] 283). Si  $a \wedge n = 1$ , alors  $a^{\varphi(n)} \equiv 1[n]$ .

**Théorème 26** (de Fermat - [R] 284). Si  $a \wedge p = 1$ , alors  $a^{p-1} \equiv 1[p]$ . De manière générale,  $a^p \equiv a[p]$ .

**Proposition 27** ([R] 284).

$$n = \sum_{d \mid n} \varphi(d)$$



**Théorème 28** ([R] 292). Si  $p \geq 3$ , alors  $\forall \alpha \geq 1$ ,  $(\mathbb{Z}/p^\alpha \mathbb{Z})^\times$  est cyclique.

**Théorème 29** (ADMIS - [R] 294).  $(\mathbb{Z}/n\mathbb{Z})^\times$  est cyclique si, et seulement si,  $n \in \{2, 4, p^\alpha, 2p^\alpha\}$  avec  $p \geq 3$  (premier) et  $\alpha \geq 1$ .

### III. Applications

#### A. Résolution de systèmes de congruence

**Théorème 30** ([R] 290). L'équation  $ax \equiv b[n]$  d'inconnue  $x \in \mathbb{Z}$  admet des solutions si, et seulement si,  $a \wedge n \mid b$ .

Le cas échéant,  $S(ax \equiv b[n]) = \frac{b}{a \wedge n} x_0 + \frac{n}{a \wedge n} \mathbb{Z}$ , où  $x_0$  est une solution particulière de l'équation.

**Remarque 31.** Le théorème des restes chinois permet de résoudre des systèmes de congruences.

**Exemple 32** ([R] 291).  $S \left( \begin{cases} x \equiv 2[4] \\ x \equiv 3[5] \\ x \equiv 1[9] \end{cases} \right) = 118 + 180\mathbb{Z}$

**Remarque 33** ([R] 291).  $S \left( \begin{cases} x \equiv x_1[a_1] \\ x \equiv x_2[a_2] \end{cases} \right) = \begin{cases} \emptyset & \text{si } a_1 \wedge a_2 \nmid x_1 - x_2 \\ x_0 + (a_1 \vee a_2)\mathbb{Z} & \text{sinon} \end{cases}$

#### B. Carrés de $\mathbb{Z}/p\mathbb{Z}$

Soit  $c : \bar{x} \in \mathbb{Z}/p\mathbb{Z} \mapsto \bar{x}^2$ . On s'intéresse à  $\text{Im } c$ .

**Proposition 34.** Tous les éléments de  $\mathbb{Z}/2\mathbb{Z}$  sont des carrés.

On supposera désormais  $p \geq 3$ .

**Proposition 35** ([R] 426). Soit  $l : \bar{x} \in \mathbb{Z}/p\mathbb{Z} \mapsto \bar{x}^{\frac{p-1}{2}}$ .

- $\forall \bar{x} \in \mathbb{Z}/p\mathbb{Z}$ ,  $c \circ l(\bar{x}) = l \circ c(\bar{x}) = \bar{1}$
- $\text{Ker } c = \text{Im } l = \{\pm 1\}$  et  $\text{Im } c = \text{Ker } l$ .

**Corollaire 36.** Il y a  $\frac{p+1}{2}$  carrés dans  $\mathbb{Z}/p\mathbb{Z}$ .

**Théorème 37** (de Wilson - [R] 325).  $n$  est premier  $\iff (n-1)! \equiv -1[n]$

**Proposition 38** ([P] 75).  $-1$  est un carré modulo  $p$  si, et seulement si,  $p \equiv 1[4]$ . Le cas échéant  $-1 \equiv (2 \times 3 \times \dots \times \frac{p-1}{2})^2[p]$ .

**Théorème 39** (des deux carrés de Fermat - [P] 56).  $p$  s'écrit comme somme de deux carrés d'entiers si, et seulement si,  $p = 2$  ou  $p \equiv 1[4]$ .

#### C. Algorithme de chiffrement RSA

**Algorithme 40** ([G] 37). Alice veut envoyer à Bob un message représenté par un nombre entier  $m$ , en toute sécurité.

- Bob choisit en secret deux nombres premiers distincts  $p$  et  $q$  et calcule leur produit  $n = pq$ .
- Il choisit ensuite un entier  $c < \varphi(n) = (p-1)(q-1)$  premier à  $\varphi(n)$ .
- Il trouve ensuite un entier  $d$  tel que  $cd \equiv 1[\varphi(n)]$ .
- La clé publique de Bob est  $(n, c)$ , qu'il donne à Alice, et sa clé privée est  $(n, d)$ , qu'il garde secrète.
- Alice envoie à Bob le message  $m^c \bmod n$ .
- Pour décoder le message, Bob calcule  $(m^c)^d \equiv m[n]$ .

### Développements

- Développement 1 : Théorème 19 (restes chinois) et exemple 32
- Développement 2 : Théorème 28 (cyclicité des inversibles de  $\mathbb{Z}/p^\alpha \mathbb{Z}$ )

### Références

- Rb *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition
- P *Cours d'algèbre*, Perrin
- G *Les maths en tête - Algèbre et probabilités*, Xavier Gourdon, 3e édition

# 121 : Nombres premiers. Applications.

Pour un entier  $n$ ,  $\text{Div}(n)$  désigne l'ensemble des diviseurs positifs de  $n$ .

## I. Résultats fondamentaux sur les nombres premiers

### A. Notion de nombre premier, propriétés élémentaires

**Définition 1** ([R] 303). On dit que  $p \in \mathbb{N}$  est premier si  $\text{Div}(p) = \{1, p\}$ . On dit que  $n$  est composé si  $n \neq 0$  et si  $\exists a \in \mathbb{N} \setminus \{1, n\} : a \mid n$ .

Dans la suite,  $\mathcal{P}$  désignera l'ensemble des nombres premiers.

**Lemme 2** (d'Euclide).  $\forall (a, b) \in \mathbb{N}^2, \forall p \in \mathcal{P}, p \mid ab \implies (p \mid a) \text{ ou } (p \mid b)$ .

**Lemme 3** ([R] 303).  $\forall n \geq 2, \exists p \in \mathcal{P} : p \mid n$

**Proposition 4** ([R] 304). Tout entier composé  $n$  admet un facteur premier entre 2 et  $\sqrt{n}$ .

**Théorème 5** (fondamental de l'Arithmétique - [R] 306).  $\forall n \in \mathbb{N}^*, \exists! (v_p(n))_{p \in \mathcal{P}} \in \mathbb{N}^{\mathcal{P}}$  :

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$$

Cette écriture est appelée "(la) décomposition en produit de facteurs premiers de  $n$ ".

**Définition 6** ([R] 306). Dans la décomposition en produit de facteurs premiers de  $n$ , l'entier  $v_p(n)$  ( $p \in \mathcal{P}$ ) est appelé valuation  $p$ -adique de  $n$ .

**Proposition 7** ([R] 307).  $\forall (a, b) \in (\mathbb{N}^*)^2, a \mid b \iff \forall p \in \mathcal{P}, v_p(a) \leq v_p(b)$

**Proposition 8** ([R] 319).  $\forall (a, b) \in (\mathbb{N}^*)^2, v_p(ab) = v_p(a) + v_p(b)$

**Proposition 9** ([R] 307).  $\forall (a, b) \in (\mathbb{N}^*)^2, \forall p \in \mathcal{P}$ ,

$$\begin{aligned} v_p(a \vee b) &= \max(v_p(a), v_p(b)) \\ v_p(a \wedge b) &= \min(v_p(a), v_p(b)) \end{aligned}$$

### B. Répartition des nombres premiers

**Théorème 10** (Euclide - [R] 305). Il existe une infinité de nombres premiers.

**Théorème 11** (de la progression arithmétique, Dirichlet, ADMIS). Pour tout  $(a, b) \in (\mathbb{N}^*)^2$  tel que  $a \wedge b = 1$ , il existe une infinité de nombres premiers congrus à  $a$  modulo  $b$ .

**Conjecture 12** (des nombres premiers jumeaux). Il existe une infinité de nombres premiers  $p$  tels que  $p+2$  est premier.

**Proposition 13**. Il existe des intervalles de longueur arbitrairement grande ne contenant aucun nombre premier.

**Théorème 14** (Bertrand - ADMIS - [R] 325). Il existe toujours un nombre premier compris entre n'importe quel entier naturel non nul et son double.

**Théorème 15** (des nombres premiers - ADMIS - [R] 308).

$$\#\mathcal{P} \cap [1, n] \sim_{x \rightarrow +\infty} \frac{n}{\ln n}$$

## II. Tests de primalité

**Proposition 16** (Crible d'Ératosthène - ANNEXE). Le procédé suivant permet de trouver la liste croissante des nombres premiers : on part de la liste des entiers plus grands que 2. À chaque itération, on garde le plus petit nombre, et on supprime tous ses multiples.

**Proposition 17**.  $n$  est premier si, et seulement si,  $\forall d \leq \lfloor \sqrt{n} \rfloor, d \nmid n$ . La complexité au pire de ce test est donc en  $O(\sqrt{n})$ .

**Théorème 18** (de Fermat). Si  $p$  est premier, alors  $\forall a \in \mathbb{N}, a \wedge p = 1 \implies a^{p-1} \equiv 1 [p]$ .

**Remarque 19**. On en déduit donc un test de non primalité.

**Définition 20** ([R] 329). Un nombre  $n$  composé satisfaisant le test du théorème de Fermat est appelé nombre de Carmichael.

**Exemple 21** ([R] 329). 561 est un nombre de Carmichael.

**Théorème 22** (de Korselt - [R] 330).  $n$  est un nombre de Carmichael si, et seulement si, pour tout diviseur premier  $p$  de  $n$ ,  $(p-1) \mid (n-1)$  et  $p^2 \nmid n$ .

**Théorème 23** (de Wilson - [R] 326).  $n$  est premier si, et seulement si,  $(n-1)! \equiv -1 [n]$ . C'est un test de primalité qui requiert  $n-1$  multiplications dans  $\mathbb{Z}/n\mathbb{Z}$ .

## III. Applications des nombres premiers

### A. Fonctions spéciales

**Définition 24** ([R] 283). L'indicatrice d'Euler est :  $\varphi : n \mapsto \#(\mathbb{Z}/n\mathbb{Z})^\times = \#\{k \in [1, n] \mid k \wedge n = 1\}$ .

**Proposition 25** ([R] 288).  $\forall (a, b) \in (\mathbb{N}^*)^2, a \wedge b = 1$ , alors  $\varphi(ab) = \varphi(a)\varphi(b)$ . Pour tout  $\alpha \in \mathbb{N}^*, \varphi(p^\alpha) = p^{\alpha-1}(p-1)$ .

**Corollaire 26** ([R] 288).  $\forall n \in \mathbb{N}^*$ ,

$$\varphi(n) = \prod_{\substack{p \in \mathcal{P} \\ v_p(n) \geq 1}} p^{v_p(n)-1}(p-1) = n \prod_{\substack{p \in \mathcal{P} \\ v_p(n) \geq 1}} \left(1 - \frac{1}{p}\right)$$

**Définition 27**. La fonction  $\zeta$  de Riemann est définie par :

$$\zeta : \{z \in \mathbb{C} \mid \Re(z) > 1\} \rightarrow \mathbb{C}$$

$$s \mapsto \sum_{n=0}^{+\infty} \frac{1}{n^s}$$

**Proposition 28** ([KG] 461). On a :

$$\zeta(s) = \prod_{p \in \mathcal{P}} \frac{1}{1 - \frac{1}{p^s}}$$

Cette écriture est appelé "produit eulérien".

**Théorème 29** ([KG] 461, [R] 343).  $\sum_{p \in \mathcal{P}} \frac{1}{p} = +\infty$

**Définition 30** ([R] 331). La fonction de Moëbius est définie par :

$$\mu : n \in \mathbb{N}^* \mapsto \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n = p_1 \dots p_r, \text{ avec } p_1, \dots, p_r \text{ distincts} \\ 0 & \text{sinon} \end{cases}$$

**Théorème 31** (Cesàro - ADMIS [R] 334). La probabilité de choisir au hasard  $r \geq 2$  entiers entre 1 et  $n$  qui sont premiers entre eux vaut  $\frac{1}{\zeta(r)}$ .

## B. Algorithme de chiffrement RSA

**Théorème 32** (d'Euler - [R] 283).  $\forall (a, b) \in (\mathbb{N}^*)^2$ , si  $a \wedge n = 1$ , alors  $a^{\varphi(n)} \equiv 1 [n]$ .

De la complexité des tests de primalité découle la grande difficulté de la recherche de la décomposition en produit de facteurs premiers d'un entier donné. Ce principe est à la base de la sécurité de l'algorithme de chiffrement RSA, détaillé ci-dessous :

**Algorithme 33** ([G] 37). Alice veut envoyer à Bob un message représenté par un nombre entier  $m$ , en toute sécurité.

- Bob choisit en secret deux nombres premiers distincts  $p$  et  $q$  et calcule leur produit  $n = pq$ .
- Il choisit ensuite un entier  $c < \varphi(n) = (p-1)(q-1)$  premier à  $\varphi(n)$ .
- Il trouve ensuite un entier  $d$  tel que  $cd \equiv 1 [\varphi(n)]$ .
- La clé publique de Bob est  $(n, c)$ , qu'il donne à Alice, et sa clé privée est  $(n, d)$ , qu'il garde secrète.
- Alice envoie à Bob le message  $m^c \bmod n$ .
- Pour décoder le message, Bob calcule  $(m^c)^d \equiv m [n]$ .

## C. Corps finis

**Définition 34** ([R] 415). La caractéristique d'un anneau  $A$  est l'unique générateur positif du noyau du morphisme  $\varphi : \mathbb{Z} \rightarrow A, n \mapsto n1_A$ .

**Lemme 35** ([R] 415). La caractéristique d'un corps est nulle ou première.

**Exemple 36.**  $\mathbb{Z}/p\mathbb{Z}$  est un corps de caractéristique  $p$ .

**Théorème 37** ([R] 421). Il existe un corps fini de cardinal  $q$  si, et seulement si,  $q$  est une puissance d'un nombre premier. Le cas échéant, un tel corps est unique à isomorphisme près, et on note  $\mathbb{F}_q$  le corps fini à  $q$  éléments. Par ailleurs,  $p = \text{car } \mathbb{F}_q$  est un nombre premier, et  $q$  est une puissance de  $p$ .

## D. Le théorème des deux carrés de Fermat

**Lemme 38** ([P] 75).  $-1$  est un carré dans  $\mathbb{F}_p$  si, et seulement si,  $p \equiv 1 [4]$ .

**Théorème 39** (des deux carrés de Fermat - [P] 56). Soit  $E = \{n \in \mathbb{N}^* \mid \exists (a, b) \in \mathbb{N}^2 : n = a^2 + b^2\}$ . Alors,  $n \in E \iff \forall p \in \mathcal{P}, p \equiv 3 [4] \implies v_p(n) \text{ est pair}$ .

## E. En théorie des groupes

**Définition 40** ([R] 22). Un  $p$ -groupe est un groupe de cardinal une puissance de  $p$ .

**Proposition 41** ([R] 22). Si un  $p$ -groupe  $G$  agit sur un ensemble fini  $X$ , alors  $\#X \equiv \#X^G [p]$  où  $X^G$  est l'ensemble des éléments de  $X$  fixes par l'action de  $G$ .

**Corollaire 42** ([R] 23). Le centre d'un  $p$ -groupe n'est pas trivial.

**Définition 43** ([U] 85). Soit  $G$  un groupe fini de cardinal  $p^\alpha m$ ,  $m \wedge p = 1$ . Un  $p$ -Sylow de  $G$  est un sous- $p$ -groupe de  $G$  de cardinal  $p^\alpha$ .

**Théorème 44** (de Sylow - ADMIS [U] 87). Soit  $G$  un groupe d'ordre  $p^\alpha m$ ,  $m \wedge p = 1$ . Alors,

1.  $\text{Syl}_p(G) \neq \emptyset$
2.  $G$  agit transitivement sur  $\text{Syl}_p(G)$  par conjugaison
3.  $n_p \equiv 1 [p]$

**Théorème 45** ([R] 292). Si  $p \geq 3$ , alors  $\forall \alpha \geq 1, (\mathbb{Z}/p^\alpha \mathbb{Z})^\times$  est cyclique.

**Proposition 46** ([R] 23). Tout groupe d'ordre  $p^2$  est abélien.

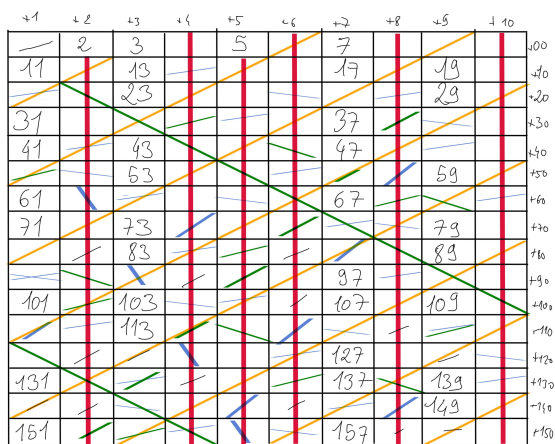
## Développements

- Développement 1 : Lemme 38, et théorème 39
- Développement 2 : Théorème 45 (cyclicité des inversibles de  $\mathbb{Z}/p^\alpha \mathbb{Z}$ )

## Références

- Rb *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition
- U *Théorie des groupes*, Félix Ulmer
- G *Les maths en tête - Algèbre et probabilités*, Xavier Gourdon, 3e édition
- KG *De l'intégration aux probabilités*, Olivier Garet, Aline Kurtzmann, 2e édition augmentée

## Crible d'ÉRATOSTHÈNE



4/4

FIGURE 1.2 – Crible d'Eratosthène

# 123 : Corps finis. Applications.

## I. Des corps finis

### A. Prérequis sur les extensions de corps

Soit  $L/M/K$  une tour d'extensions de corps (commutatifs).

**Proposition/Définition 1** ([P] 65).  $L$  est un  $K$ -espace vectoriel, sa dimension est appelée degré de  $L/K$ , et est notée  $[L : K]$ .

**Théorème 2** (de la base télescopique - [P] 65). Soient  $(e_i)_{i \in I}$  une base  $K$ -base de  $M$  et  $(f_j)_{j \in K}$  une  $M$ -base de  $L$ , alors  $(e_i f_j)_{(i,j) \in I \times J}$  est une  $K$ -base de  $L$ . En particulier,  $[L : K] = [L : M] \times [M : K]$  (dans  $\mathbb{N} \cup \{+\infty\}$ ).

**Définition 3** ([P] 70). Soit  $P \in K[X]$  non constant. Supposons  $P$  irréductible sur  $K$ . On dit que  $L$  est un corps de rupture (CDR) de  $P$  sur  $K$  s'il existe  $\alpha \in L$  tel que  $P(\alpha) = 0$  et  $L = K(\alpha)$ .

On dit que  $L$  est un corps de décomposition (CDD) de  $P$  sur  $K$  s'il existe  $(\alpha_1, \dots, \alpha_n) \in L^n$  tel que  $L = K(\alpha_1, \dots, \alpha_n)$  et  $P$  est scindé sur  $L$ .

**Théorème 4** ([P] 70-71).  $P$  admet un unique corps de rupture à  $K$ -isomorphisme près. Plus précisément,  $K[X]/\langle P \rangle$  est un corps de rupture de  $P$  sur  $K$ .

$P$  admet un unique corps de décomposition  $D$  à  $K$ -isomorphisme près. Celui-ci vérifie  $[D : K] \leq \deg(P)!$ .

### B. Construction des corps finis : existence et unicité

Dans ce paragraphe  $K$  désigne un corps fini commutatif.

**Exemple 5.** Soit  $p$  un nombre premier. L'anneau  $(\mathbb{Z}/p\mathbb{Z}, +, \times)$  est un corps fini commutatif. On le note  $\mathbb{F}_p$ .

**Théorème/Définition 6** ([P] 72). Il existe un nombre premier  $p$  rendant le diagramme suivant commutatif :

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{n \mapsto n \cdot 1_K} & K \\ & \searrow & \nearrow \\ & \mathbb{Z}/p\mathbb{Z} & \end{array}$$

L'entier  $p$  est appelé caractéristique de  $K$  notée car  $K$  et  $\mathbb{F}_p$  est appelé sous-corps premier de  $K$ . C'est le plus petit sous-corps de  $K$ .

On notera  $p$  la caractéristique de  $K$ .

**Corollaire 7** ([P] 72).  $\#K = p^{[K : \mathbb{F}_p]}$

**Remarque 8.** Il n'existe pas de corps fini commutatif à 6 éléments !

**Lemme/Définition 9** ([P] 73).  $\text{Fr} : K \rightarrow K, x \mapsto x^p$  est un morphisme de corps, appelé morphisme de Frobenius.

**Théorème 10** ([P] 73). Soient  $r \in \mathbb{N}^*$ ,  $p$  premier et  $q = p^r$ . Il existe un corps fini commutatif à  $q$  éléments. Un tel corps est un CDD de  $X^q - X$ . En particulier, les classes d'isomorphisme de corps finis commutatifs sont caractérisées par le cardinal de ces derniers. On note  $\mathbb{F}_q$  un représentant de la classe d'isomorphisme des corps finis commutatifs à  $q$  éléments.

**Théorème 11** (de Wedderburn - [P] 82). Tout corps fini est commutatif.

**Exemple 12.**  $\mathbb{F}_4 = \mathbb{F}_2[X]/\langle X^2 + X + 1 \rangle = \{0, 1, \bar{X}, 1 + \bar{X}\}$ .  
 $\mathbb{F}_9 = \mathbb{F}_3[X]/\langle X^3 + X^2 + X + 1 \rangle$ .

### C. Propriétés des corps finis

Soient  $p$  un nombre premier,  $r \in \mathbb{N}^*$  et  $q = p^r$ .

**Proposition 13** (FIG. 1).  $\forall (m, n) \in (\mathbb{N}^*)^2, \mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \iff n \mid m$ .

**Proposition 14** ([P] e73). —  $\overline{\mathbb{F}_p} = \bigcup_{n \in \mathbb{N}^*} \mathbb{F}_{p^n}$  est une clôture algébrique de  $\mathbb{F}_p$ .

— Si  $K$  est une extension de  $\mathbb{F}_q$ , alors  $\mathbb{F}_q = \{x \in K \mid x^q = x\}$ . En particulier,  $\mathbb{F}_q$  est l'unique sous-corps de  $\overline{\mathbb{F}_p}$  de cardinal  $q$ .

**Théorème 15** ([P] 74).  $\mathbb{F}_q^\times$  est cyclique.

**Proposition 16** ([P] 73).  $\text{Fr}$  est un automorphisme de  $\mathbb{F}_q$ .

**Théorème 17** ([R] 425). Le groupe des automorphismes de  $\mathbb{F}_q$  est cyclique d'ordre  $r$ , engendré par  $\text{Fr}$ .

**Remarque 18.** Pour tout  $\theta \in \mathbb{F}_q$ , il existe  $d \in \mathbb{N}^*$  tel que  $\text{Fr}^d(\theta) = \theta^{d^p} = \theta$ . Le polynôme minimal de  $\theta$  sur  $\mathbb{F}_p$  est  $\prod_{k=1}^d (X - \text{Fr}^k(\theta))$ .

**Exemple 19.** Soit  $\beta = \bar{X}^2 + \bar{X} \in \mathbb{F}_2[X]/\langle X^4 + X + 1 \rangle$ . On a  $P_{\beta, \mathbb{F}_2} = X^2 + X + 1$ .

## II. Carrés dans un corps fini

Soient  $p$  un nombre premier impair,  $r \in \mathbb{N}^*$  et  $q = p^r$ . On pose  $c : \mathbb{F}_q \rightarrow \mathbb{F}_q, x \mapsto x^2$  et  $l : \mathbb{F}_q \rightarrow \mathbb{F}_q, x \mapsto x^{\frac{q-1}{2}}$ .

**Proposition 20.**  $\text{Im } l = \text{Ker } c = \{\pm 1\}$  et  $\text{Ker } l = \text{Im } c = \{x^2 \mid x \in \mathbb{F}_q^\times\}$ .

**Corollaire 21** (Critère d'Euler - [P] 75).  $x \in \mathbb{F}_q^\times$  est un carré si, et seulement si  $x^{\frac{q-1}{2}} = 1$ .

**Corollaire 22** ([P] 74). Il y a  $\frac{q-1}{2}$  carrés inversibles dans  $\mathbb{F}_q$  (et  $\frac{q+1}{2}$  carrés).

**Proposition 23** ([P] 74). Tous les éléments de  $\mathbb{F}_{2^r}$  sont des carrés.

**Proposition 24** ([P] 75).  $-1$  est un carré dans  $\mathbb{F}_p$  si, et seulement si,  $p \equiv 1 \pmod{4}$ .

**Application 25** ([P] 56).  $p$  est la somme de deux carrés si, et seulement si,  $p = 2$  ou  $p \equiv 1 \pmod{4}$ .

**Définition 26** ([R] 428). Le symbole de Legendre de  $a \in \mathbb{Z}$  modulo  $p$  est défini par :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } a \in p\mathbb{Z} \\ 1 & \text{si } a \text{ est un carré inversible modulo } p \\ -1 & \text{sinon} \end{cases}$$

**Proposition 27** ([R] 428).  $\forall a \in \mathbb{Z}, \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ . En particulier,  $\left(\frac{\cdot}{p}\right)$  est un morphisme du groupe  $\mathbb{F}_p^\times$ .



**Proposition 28** ([R] 431-434). Soit  $a \in \mathbb{F}_p^\times$ . L'équation de  $ax^2 = 1$  a  $1 + \left(\frac{a}{p}\right)$  solutions dans  $\mathbb{F}_p$ .

**Théorème 29** (Loi de réciprocité quadratique - [R] 431-434). Soient  $p$  et  $q$  deux nombres premiers impairs distincts.

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

**Application 30.**  $\left(\frac{11}{23}\right) = \left(\frac{23}{11}\right)(-1)^{11 \cdot 5} = -\left(\frac{1}{11}\right) = -1$  donc 11 n'est pas un carré modulo 23.

**Proposition 31** ([R] e438, [C] 307).  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

**Proposition 32.** Soit  $(a, b, c) \in \mathbb{F}_q^3$  avec  $a \neq 0$ . L'équation  $ax^2 + bx + c = 0$  dans  $\mathbb{F}_q$  possède des solutions si, et seulement si,  $b^2 - 4ac$  est un carré dans  $\mathbb{F}_q$ . Le cas échéant, si  $\delta \in \sqrt{b^2 - 4ac}$ , alors les solutions de cette équation sont  $\frac{-b \pm \delta}{2a}$ .

**Remarque 33.** Dans  $\mathbb{F}_{2^r}$ , l'équation  $ax^2 + bx + c = 0$  est bien plus difficile à résoudre, en dehors des cas triviaux !

### III. Algèbre (bi)linéaire sur les corps finis

Soient  $p$  un nombre premier impair,  $r \in \mathbb{N}^*$ ,  $q = p^r$  et  $n \in \mathbb{N}$ .

**Proposition 34** ([R] 155). —  $\#GL_n(\mathbb{F}_q) = (q^n - 1)(q^n - q) \dots (q^n - q^{n-1}) = q^{\frac{n(n-1)}{2}} \prod_{k=1}^{n-1} (q^k - 1)$   
—  $\#SL_n(\mathbb{F}_q) = \#GL_n(\mathbb{F}_q)/(q - 1)$

**Théorème 35** ([C] 50).

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

**Remarque 36.**  $SO_2(\mathbb{F}_{2^r}) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \mathbb{F}_{2^r} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ , puis  $SO_2(\mathbb{F}_{2^r}) \cong (\mathbb{Z}/2\mathbb{Z})^r$ .

Soit  $E$  un  $\mathbb{F}_q$ -espace vectoriel de dimension finie.

**Définition 37** ([R] 463). Le discriminant d'une forme quadratique  $f$  sur  $E$  est l'image de son déterminant dans une base quelconque modulo les carrés de  $\mathbb{F}_q^\times$ .

**Théorème 38** ([R] e482). Il y a deux classes d'équivalence de formes quadratiques non-dégénérées sur  $E$ . Plus précisément, soient  $\alpha \in \mathbb{F}_q^\times$  qui n'est pas un carré, et  $f$  une forme quadratique sur, de matrice  $M$  dans la base canonique.

- Si  $\det M$  est un carré dans  $\mathbb{F}_p^\times$ , alors  $M$  est congruente à la matrice  $\text{diag}(1, 1, \dots, 1, 1)$ .
- Sinon,  $M$  est congruente à  $\text{diag}(1, 1, \dots, 1, \alpha)$ .

**Application 39.** Loi de réciprocité quadratique (Thm 29).

### IV. Polynômes et corps finis

**Théorème 40** (Critère d'Eisenstein - [P] 76). Soit  $P = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X]$ . Soit  $p$  un nombre premier. Si  $p \nmid a_n$ , si  $\forall k \in \llbracket 0, n-1 \rrbracket$ ,  $p \mid a_k$  et  $p^2 \nmid a_0$ , alors  $P$  est irréductible dans  $\mathbb{Q}[X]$ .

**Exemple 41.** Pour tout  $p$  premier,  $\Phi_p = X^{p+1} + \dots + X + 1$  est irréductible sur  $\mathbb{Q}$ .

**Théorème 42** ([P] 77). Soit  $P = \sum_{k=0}^n a_k X^k \in \mathbb{Z}[X]$ ,  $n \geq 1$ ,  $a_n \neq 0$ . Soit  $p \in \mathbb{Z}$  premier. Si  $p \nmid a_n$  et si l'image  $\overline{P}$  de  $P$  dans  $\mathbb{F}_p[X]$  est irréductible, alors  $P$  est irréductible sur  $\mathbb{Z}$ .

**Remarque 43.** La réciproque est fautive : considérer  $X^4 + 1$ .

### Développements

- Développement 1 : Proposition 28, et théorème 29 : loi de réciprocité quadratique (par les formes quadratiques)
- Développement 2 : Théorème 35

### Références

- R *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition  
P *Cours d'algèbre*, Perrin  
C *Nouvelles histoires hédonistes de groupes et géométries*, P. Caldero, J. Germoni

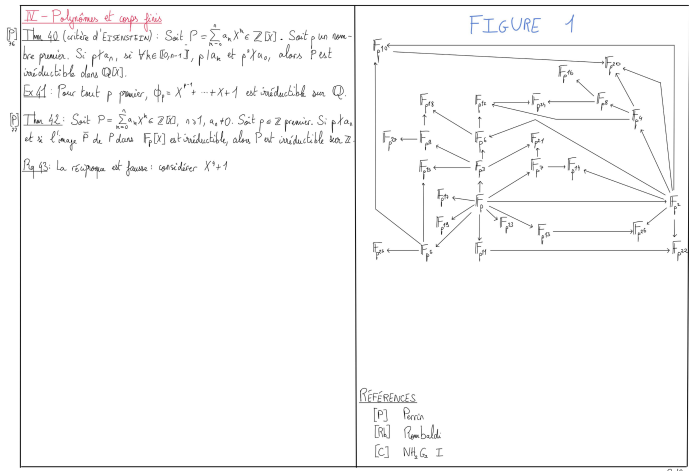


FIGURE 1.3 – Diagramme des extensions de corps finis

# 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Soient  $A$  un anneau unitaire intègre commutatif, et  $L/K$  une extension de corps commutatif. Soit  $P \in A[X]$ .

## I. Polynômes irréductibles

### A. Notion d'irréductibilité pour les polynômes

**Définition 1** ([R] 370). On dit que  $P$  est irréductible sur  $A$  si  $P \notin A[X]^\times = A^\times$ , si  $P \neq 0$  et si  $\forall (P_1, P_2) \in A[X]^2$ ,  $P = P_1 P_2 \implies P_1 \in A^\times$  ou  $P_2 \in A^\times$ .

**Exemple 2** ([R] 370). Tout polynôme de degré 1 est irréductible ; et les polynômes réels de degré 2 de discriminant  $< 0$  sont irréductibles.

**Proposition 3** ([R] 371). — Si  $P \in K[X]$  est irréductible et si  $\deg P > 1$ , alors  $P$  n'a pas de racine dans  $K$ .  
— Si  $P \in K[X]$  n'a pas de racine dans  $K$  et si  $\deg P \leq 3$ , alors  $P$  est irréductible sur  $K$ .

**Exemple 4.** —  $(x^2+1)^2$  est réductible sur  $\mathbb{R}$  et sans racine dans  $\mathbb{R}$ .  
— Les polynômes irréductibles de petit degré de  $\mathbb{F}_2[X]$  sont  $X, X+1, X^2+X+1$ .

### B. Propriétés de $A[X]$

**Proposition 5** ([R] 374).  $A[X]$  euclidien  $\iff A[X]$  principal  $\iff A$  est un corps.

**Proposition 6** ([R] e375). Si  $P \in K[X]$  est irréductible, alors  $K[X]/\langle P \rangle$  est un corps.

On suppose  $A$  factoriel.

**Définition 7** ([S] 547-548; [P] 51). Le contenu de  $P \in A[X] \setminus \{0\}$ , noté  $c(P)$ , est un PGCD des coefficients de  $P$ . On dit que  $P$  est primitif si  $c(P) \in A^\times$ .

**Théorème 8** ([P] 51; [S] 548). Soit  $P \in A[X]$  primitif non constant.  $P$  est irréductible dans  $A[X] \iff A$  est irréductible dans  $K[X]$ .

**Exemple 9.** Soient  $a_1, \dots, a_n$  des entiers distincts. Le polynôme  $(X - a_1) \dots (X - a_n) - 1$  est irréductible sur  $\mathbb{Q}$ .

**Lemme 10.** Un produit de polynômes primitifs est primitif.

**Lemme 11** (de Gauss - [S] 548; [P] 51).  $c(PQ) = c(P)c(Q)$

**Théorème 12** ([R] 358; [S] 548; [P] 51).  $A[X]$  est factoriel  $\iff A$  est factoriel.

### C. Critères d'irréductibilité

**Théorème 13** (Critère d'Eisenstein - [S] 549; [P] 76). Écrivons  $P = \sum_{k=0}^n a_k X^k$ ,  $a_n \neq 0$ . S'il existe  $p \in A$  premier non nul tel que  $\forall k \in \llbracket 1, n-1 \rrbracket$ ,  $p \mid a_k$ ,  $p^2 \nmid a_0$  et  $p \nmid a_n$ , alors  $P$  est irréductible dans  $\text{Frac}(A)[X]$ .

**Exemple 14.**  $\forall n \geq 2, \forall d \in \mathbb{N}^*$  sans facteur carré,  $X^n - d$  est irréductible dans  $\mathbb{Z}[X]$ .

**Théorème 15** ([P] 77). Soit  $I$  un idéal de  $A$ . Écrivons  $P = \sum_{k=0}^n a_k X^k$ ,  $a_n \neq 0$ . Si  $a_n \not\equiv 0 \pmod I$  et si  $P \pmod I$  est irréductible dans  $(A/I)[X]$  alors  $P$  est irréductible dans  $A[X]$ .

**Exemple 16** ([P] 77). Pour tout  $p$  premier,  $X^p - X - 1$  est irréductible sur  $\mathbb{Q}$ .

## II. Polynômes et extensions de corps

Soient  $L$  et  $K$  deux corps commutatifs. Soit  $P \in K[X]$ .

### A. Extensions de corps, éléments algébriques

**Définition 17** ([P] 65). On dit que  $L$  est une extension de  $K$ , et on note  $L/K$ , si  $K \subseteq L$ .

**Proposition/Définition 18** ([P] 65).  $L$  est un  $K$ -espace vectoriel dont on note  $[L : K]$  la dimension, que l'on appelle degré de l'extension  $L/K$ . On dit que  $L/K$  est finie si  $[L : K]$  est fini.

**Théorème 19** (de la base télescopique - [P] 65). Soient  $(e_i)_{i \in I}$  une base  $K$ -base de  $M$  et  $(f_j)_{j \in K}$  une  $M$ -base de  $L$ , alors  $(e_i f_j)_{(i,j) \in I \times J}$  est une  $K$ -base de  $L$ .

**Corollaire 20** (Multiplicativité des degrés - [P] 65).  $[L : K] = [L : M] \times [M : K]$

**Définition 21** ([P] 66). On dit que  $\alpha \in L$  est algébrique sur  $K$  s'il existe  $P \in K[X]$  tel que  $P(\alpha) = 0$ . Sinon, on dit que  $\alpha$  est transcendant.

**Théorème/Définition 22** ([P] 66). Si  $\alpha \in L$  est algébrique sur  $K$ , alors  $\{P \in K[X] \mid P(\alpha) = 0\}$  est un idéal non nul, qui donc admet un unique générateur unitaire  $P_{\alpha,K}$  appelé polynôme minimal de  $\alpha$  sur  $K$ .

**Notation.**  $K[\alpha] = \{P(\alpha) \mid P \in K[X]\}$

**Théorème 23** ([P] 66). Soit  $\alpha \in L$ . Sont équivalentes :

1.  $\alpha$  est algébrique sur  $K$
  2.  $K[\alpha] = K(\alpha)$
  3.  $K[\alpha]$  est un  $K$ -espace vectoriel de dimension finie.
- Le cas échéant,  $\deg P_{\alpha,L} = [K(\alpha) : K]$ .

### B. Corps de rupture et de décomposition

**Définition 24** ([P] 70). Supposons  $P$  irréductible. On dit que  $L$  est un corps de rupture de  $P$  sur  $K$  s'il existe  $\alpha \in L$  tel que  $P(\alpha) = 0$  et  $L = K(\alpha)$ .

**Théorème 25** ([P] 70). Supposons  $P$  irréductible. Le corps  $K[X]/\langle P \rangle$  est un corps de rupture de  $P$  sur  $K$ , et c'est le seul à isomorphisme près.

**Exemple 26.**  $\mathbb{C}$  peut être défini comme  $\mathbb{R}[X]/\langle X^2 + 1 \rangle$ .

**Application 27.** Si  $P$  est irréductible et si  $\deg P \wedge [L : K]$ , alors  $P$  est irréductible sur  $L$ .

**Définition 28** ([P] 71). On dit que  $L$  est un corps de décomposition de  $P$  sur  $K$  si  $P$  est scindé sur  $L$  et si  $L = K(\alpha_1, \dots, \alpha_n)$  avec  $\alpha_1, \dots, \alpha_n$  les racines de  $P$ .

**Théorème 29** ([P] 71). *Il existe un corps de décomposition de  $P$  sur  $K$ , unique à isomorphisme près.*

**Exemple 30** ([P] 72).  $\mathbb{Q}(j, \sqrt[3]{2})$  est un corps de décomposition de  $X^3 - 2$  sur  $\mathbb{Q}$ .

**Théorème 31** (de l'élément primitif - [P] 87). *Toute extension finie d'un corps de caractéristique nulle est monogène.*

### C. Clôture algébrique

**Définition 32** ([P] 67). *On dit que  $K$  est algébriquement clos si tout polynôme non nul de  $K[X]$  est scindé, et si  $K$  n'admet pas d'extension algébrique non triviale.*

**Définition 33** ([P] 72). *On dit que  $L$  est une clôture algébrique de  $K$  si c'est une extension de  $K$  algébrique et algébriquement close.*

**Exemple 34** ([P] 68-72). —  $\mathbb{C}$  est algébriquement clos (théorème de d'Alembert-Gauss) ;

—  $\mathbb{C}$  est une clôture algébrique de  $\mathbb{R}$ .

**Exemple 35** ([G] 94). *Si  $L$  est algébriquement clos, alors l'ensemble des éléments de  $L$  algébriques sur  $K$  est un corps algébriquement clos.*

**Théorème 36.**  *$K$  admet une unique clôture algébrique à isomorphisme près.*

### III. Polynôme cyclotomiques

On note  $\mathbb{U} := \{z \in \mathbb{C} \mid z^n = 1\}$  le groupe des racines complexes  $n$ -ièmes de l'unité, et  $\mu_n^*$  l'ensemble de ses générateurs (que l'on appelle *racines primitives  $n$ -ièmes de l'unité*).

**Définition 37** ([P] 80 ; [R] 385). *Pour  $n \in \mathbb{N}^*$ , on définit le  $n$ -ième polynôme cyclotomique :*

$$\Phi_n = \prod_{\zeta \in \mu_n^*} X - \zeta$$

**Proposition 38** ([P] 80-83 ; [R] 386). *On a les propriétés suivantes :*

— Pour  $\zeta_n \in \mu_n^*$ ,

$$\Phi_n = \prod_{\substack{k=1 \\ k \wedge n=1}}^n X - \zeta_n^k$$

—  $X^n - 1 = \prod_{d|n} \Phi_d$

—  $\Phi_n \in \mathbb{Z}[X]$

**Exemple 39** ([P] 81). — Pour  $p$  premier,  $\Phi_p = X^{p-1} + \dots X + 1$

—  $\Phi_1 = X - 1$ ,  $\Phi_4 = X^2 + 1$ ,  $\Phi_6 = X^2 - X + 1$ ,  $\Phi_8 = X^4 + 1$

**Théorème 40** ([P] 82-83 ; [R] 392). *Soit  $\zeta_n \in \mu_n^*$ . Le polynôme minimal de  $\zeta_n$  sur  $\mathbb{Q}$  est  $\Phi_n$ .*

**Corollaire 41.**  $\Phi_n$  est irréductible sur  $\mathbb{Q}$  et  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$ .

### IV. Polynômes irréductibles des corps finis

**Définition 42** ([R] 331). *La fonction de Moëbius est définie par :*

$$\mu : n \in \mathbb{N}^* \mapsto \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n \text{ est le produit de } r \text{ facteurs premiers distincts} \\ 0 & \text{sinon} \end{cases}$$

**Théorème 43** (Formule d'inversion de Moëbius = [R] 333). *Soient  $(u_n)_{n \in \mathbb{N}^*} \in \mathbb{R}^{\mathbb{N}^*}$  et  $(v_n)_{n \in \mathbb{N}^*} \in \mathbb{R}^{\mathbb{N}^*}$ . Si  $\forall n \in \mathbb{N}^*$ ,  $u_n = \sum_{d|n} v_d$ , alors  $\forall n \in \mathbb{N}^*$ ,  $v_n = \sum_{d|n} \mu(\frac{n}{d}) u_d$ .*

**Théorème 44** ([R] 423).  $P_n := X^{p^n} - X = \prod_{d|n} \prod_{\mathcal{U}_d(p)} P$  où  $\mathcal{U}_d(p)$  est l'ensemble des polynômes irréductibles unitaires de degré  $d$  de  $\mathbb{F}_p[X]$ .

**Corollaire 45** ([R] 424).  $\#\mathcal{U}_n(p) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) p^d$

### Développements

— Développement 1 : Lemme de Gauss 11

— Développement 2 : Théorème 40 et Corollaire 41

— Développement 2 : Théorème 43, Théorème 44 et Corollaire 45

### Références

R *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition

P *Cours d'algèbre*, Perrin

G *Les maths en tête - Algèbre et probabilités*, Xavier Gourdon, 3e édition

S *Algèbre pour la licence 3*, Szpirglas

# 142 : PGCD et PPCM, algorithmes de calcul. Applications.

## I. Notion de PGCD et de PPCM dans différents types d'anneaux

Dans cette section,  $A$  est un anneau intègre (commutatif) et  $(a, b, a_1, \dots, a_r) \in A^{r+2}$ .

### A. Première définition, existence, cas des anneaux factoriels

**Définition 1.** Si  $a_1, \dots, a_r \neq 0$ , alors sous réserve d'existence, on appelle PGCD (resp. PPCM) de  $a_1, \dots, a_r$ , noté  $a_1 \wedge \dots \wedge a_r$  ou  $\text{pgcd}(a_1, \dots, a_r)$  (resp.  $a_1 \vee \dots \vee a_r$  ou  $\text{ppcm}(a_1, \dots, a_r)$ ) un plus grand minorant (resp. un plus grand majorant) de  $\{a_1, \dots, a_r\}$  pour la relation (binaire) de divisibilité. On pose par ailleurs  $0 \wedge 0 = 0 \vee a = 0$ .

En particulier, le PGCD et le PPCM sont associatifs et commutatifs :  $a \wedge b = b \wedge a$  et  $a_1 \wedge a_2 \wedge a_3 \wedge a_4 \wedge a_5 = (a_1 \wedge a_2) \wedge (a_3 \wedge a_4) \wedge a_5$ .

**Remarque 2.** Les PGCD (resp. PPCM) de  $a_1, \dots, a_r$  sont tous associés. L'écriture  $d = a_1 \wedge \dots \wedge a_r$  est un abus signifiant que  $d$  est un PGCD de  $a_1, \dots, a_r$ .

**Proposition 3** ([R] 246). Si  $a$  et  $b$  ont un PPCM alors ils ont un PGCD  $a \wedge b = ab(a \vee b)^{-1}$ .

**Exemple 4.** 3 et  $2 + i\sqrt{5}$  ont un PGCD mais pas de PPCM dans  $\mathbb{Z}[i\sqrt{5}]$ . 4 et  $2 + 2i\sqrt{3}$  n'ont pas de PGCD dans  $\mathbb{Z}[i\sqrt{3}]$ .

**Définition 5.** On dit que  $a_1, \dots, a_r$  sont premiers entre eux (dans leur ensemble) si  $a_1 \wedge \dots \wedge a_r = 1$ . On dit que  $a_1, \dots, a_r$  sont deux à deux premiers entre eux si  $\forall (i, j) \in \llbracket 1, r \rrbracket^2$ ,  $i \neq j \implies a_i \wedge a_j = 1$ .

**Théorème 6** (de Gauss - [R] 247).  $\forall (a, b, c) \in A^3$ ,  $a \mid bc$  et  $a \wedge b = 1 \implies a \mid c$ .

**Proposition 7** ([R] 246). Si toute paire d'éléments de  $A$  admet un PGCD (on dit alors que  $A$  est un anneau à PGCD), alors toute paire d'éléments de  $A$  admet un PPCM, et la réciproque est vraie.

**Proposition 8** ([P] 49). Supposons  $A$  factoriel, notons  $\mathcal{P}$  un système complet de représentants des irréductibles de  $A$ . Alors :

$\prod_{p \in \mathcal{P}} p^{\min(v_p(a), v_p(b))}$  est un PGCD de  $a$  et  $b$ .

$\prod_{p \in \mathcal{P}} p^{\max(v_p(a), v_p(b))}$  est un PPCM de  $a$  et  $b$ .

**Définition 9.** Si  $A = \mathbb{Z}$  (resp.  $A = K[X]$ ,  $K$  un corps), alors le PGCD de  $a$  et  $b$  est l'unique PGCD de  $a$  et  $b$  qui est positif (resp. unitaire).

### B. Situation dans les anneaux principaux

On suppose  $A$  principal.

**Proposition 10.**  $m \in A$  est un PPCM de  $a$  et  $b$  si, et seulement si,  $aA \cap bA = mA$ .

$d \in A$  est un PGCD de  $a$  et  $b$  si, et seulement si,  $aA + bA = dA$ .

**Théorème 11** (de Bézout).  $(\exists (u, v) \in A^2 : au + bv = 1) \iff a \wedge b = 1$

**Remarque 12.**  $\forall (a, b) \in A^2$ ,  $\exists (u, v) \in A^2 : au + bv = 1$ . Le théorème de Bézout indique que la réciproque est vraie si  $a \wedge b = 1$  (contre-exemple :  $3 \times (2) + 2 \times (-2) = 2$ , mais  $3 \wedge 2 \neq 1$ ).

**Définition 13** ([R] 247). Un couple  $(u, v) \in A^2$  tel que  $a \wedge b = au + bv$  est appelé couple de Bézout de  $(a, b)$ , et l'égalité est appelée relation de Bézout.

**Application 14.** Résolution de  $ax + by = c$  avec  $a \wedge b = 1$ .

**Application 15.** Lemme des noyaux : soit  $(P, Q) \in K[X]^2$  tel que  $P \wedge Q = 1$ . Soient  $V$  un  $K$ -espace vectoriel de dimension finie. Pour tout endomorphisme  $f$  de  $V$  ;  $\text{Ker}((PQ)(f)) = \text{Ker}(P(f)) \oplus \text{Ker}(Q(f))$ .

**Théorème 16** (des restes chinois - [R] 250). Si  $a_1, \dots, a_d$  sont non nuls, non inversibles et deux à deux premiers entre eux, alors :

$$\bar{\varphi} : x \bmod a_1 \dots a_d \mapsto (x \bmod a_1, \dots, x \bmod a_d)$$

est un isomorphisme d'anneaux de  $A/\langle a_1 \dots a_d \rangle$  dans  $A/\langle a_1 \rangle \times \dots \times A/\langle a_d \rangle$ .

Posons  $a = a_1 \dots a_d$  et pour  $j \in \llbracket 1, d \rrbracket$ ,  $b_j = \frac{a}{a_j}$ . Il existe  $(u_1, \dots, u_d) \in A^d$  tel que  $\sum_{i=1}^d u_i b_i = 1$ . La réciproque de  $\bar{\varphi}$  s'exprime alors :

$$\bar{\varphi}^{-1} : (x_1 \bmod a_1, \dots, x_d \bmod a_d) \mapsto \sum_{i=1}^d x_i a_i b_i \bmod a_1 \dots a_d$$

**Application 17** ([R] 291). Résolution d'un système de congruence.

**Exemple 18** (Interpolation de Lagrange). Soient  $x_1, \dots, x_n \in K$  deux à deux distincts et  $y_1, \dots, y_n \in K^n$ . Un polynôme interpolateur des  $x_i$  en  $y_i$  est une solution du système :

$$\{\forall i \in \llbracket 1, n \rrbracket, P \equiv y_i [X - x_i]\}$$

**Exemple 19.** Recherche de  $P \in (\mathbb{Z}/5\mathbb{Z})[X]$  tel que  $P(\bar{0}) = \bar{2}$ ,  $P(\bar{1}) = \bar{0}$ ,  $P(\bar{2}) = \bar{1}$  de degré minimal.

**Proposition 20** ([R] 298).  $\forall (n, m) \in \mathbb{N}_{\geq 2}^2$ ,  $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/n \wedge m\mathbb{Z} \times \mathbb{Z}/n \vee m\mathbb{Z}$

## II. Algorithmes de calcul dans un anneau euclidien

Dans cette section,  $A$  est supposé euclidien. Soit  $(a, b) \in A \times A \setminus \{0\}$ .

### A. Algorithmes d'Euclide

**Lemme 21** (d'Euclide - [R] 264). Si  $a = bq + r$  avec  $(q, r) \in A^2$ , alors  $a \wedge b = b \wedge r$ .

**Algorithme 22** (d'Euclide - [R] 264). Posons  $r_{-1} = a$  et  $r_0 = b$ , et pour  $n \geq 1$ ,  $r_n$  est un reste d'une division euclidienne de  $r_{n-2}$  par  $r_{n-1}$  si  $r_{n-1} \neq 0$ , et  $r_n = 0$  sinon.

Il existe  $N \in \mathbb{N}$  tel que  $\forall n \geq N + 1$ ,  $r_n = 0$  ; de plus,  $a \wedge b = r_n$ .



**Exemple 23.**  $M_n \wedge M_m = M_{n \wedge m}$ , où  $(n, m) \in \mathbb{N}^2$  et  $M_n = 2^n - 1$ .

$$(X^n - 1) \wedge (X^m - 1) = X^{n \wedge m} - 1.$$

**Algorithme 24** (d'Euclide étendu - [R] 265). Soit  $(q_n)_{n \geq 1}$  une suite de quotients dans l'algorithme d'Euclide, soit  $N$  le rang du dernier reste non nul. On peut trouver un couple de Bézout en "remontant" l'algorithme d'Euclide, i.e. en écrivant  $a \wedge b = r_N = r_{N-2} - q_N r_{N-1}$ , puis en y substituant  $r_{N-1} = r_{N-3} - q_{N-1} r_{N-2}$ , puis en y substituant  $r_{N-2} = r_{N-4} - q_{N-2} r_{N-3}$ , etc. jusqu'à exprimer  $a \wedge b$  sous la forme  $a \wedge b = af(q_1, \dots, q_N) + bg(q_1, \dots, q_N)$ .

**Application 25.** Calcul d'un inverse dans un corps de rupture : soit  $K = \mathbb{Q}[X]/\langle X^2 - X - 1 \rangle \cong \mathbb{Q}(\varphi)$ . Dans  $K$ ,  $(2\varphi + 1)^{-1} = 2\varphi - 3$ .

**Proposition 26.**  $GL_2(\mathbb{Z})$  agit sur  $\mathbb{Z}^2$  par  $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \alpha a + \beta b \\ \gamma a + \delta b \end{pmatrix}$ . Les orbites de cette action sont les  $E_d = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{Z}^2 \mid a \wedge b = d \right\}$ ,  $d \in \mathbb{N}$ .

**Corollaire 27.** D'après l'algorithme d'Euclide,  $\forall (a, b) \in \mathbb{Z}^2$ ,  $\exists P \in GL_2(\mathbb{Z}) : P \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \wedge b \\ 0 \end{pmatrix}$

**Application 28.** Soit  $a = (a_1, \dots, a_n)$  un vecteur de  $\mathbb{Z}^n$ . On peut compléter  $(a)$  en une  $\mathbb{Z}$ -base de  $\mathbb{Z}^n$  si, et seulement si,  $a_1 \wedge \dots \wedge a_n = 1$ .

## B. Du côté de $\mathbb{Z}$ et $K[X]$ , un point sur la complexité

Dans le cas de la division euclidienne dans  $\mathbb{Z}$ , on impose aux restes d'être positifs, ce qui rend les reste et quotient uniques.

**Théorème 29** (de LAMÉ - [D] 38). Supposons que  $a > b \geq 1$ . Soient  $(F_k)_k$  la suite de FIBONACCI débutant à 0, et  $k \in \mathbb{N}$  tel que  $b < F_{k+1}$ . L'algorithme d'EUCLIDE pour  $a$  et  $b$  termine en moins de  $k$  étapes.

**Remarque 30.** Cette majoration est optimale : considérer  $a = F_{k+1}$ ,  $b = F_k$ .

**Algorithme 31** (PGCD binaire - [D] 36). Supposons  $a \geq b \geq 0$ . La fonction suivante :

```
PGCD_binaire(a,b) :
  Si a = 0 : renvoyer b
  Si 2 | a et 2 | b : renvoyer 2×PGCD_binaire(a/2, b/2)
  Si 2 | a et non(2 | b) : renvoyer PGCD_binaire(a/2, b)
  Si non(2 | a) et 2 | b : renvoyer PGCD_binaire(a, b/2)
  Sinon : renvoyer PGCD_binaire((a - b)/2, b)
appliquée à (a, b) renvoie a ∧ b.
```

**Remarque 32.** Algorithme 31 se termine en au plus  $\lceil \log_2(a) \rceil$  récursions.

**Proposition 33.** Soit  $(P, Q) \in K[X]^2$  tel que  $n := \deg P \geq \deg Q \geq 1$ . L'algorithme d'EUCLIDE appliqué à  $P$  et  $Q$  termine en au plus  $n$  étapes.

## III. Applications en arithmétique et en théorie des groupes

### A. (Systèmes d') équations diophantiennes linéaires

**Définition 34** ([G] 163). Soit  $M \in \mathcal{M}_{n,m}(I\mathbb{Z})$ . On dit que  $M$  est sous forme normale d'HERMITE si elle est sous la forme :

$$\begin{pmatrix} 0 & \dots & 0 & p_1 & * & \dots & * & + & * & \dots & * & + \\ & & & & p_2 & * & \dots & * & + & * & \dots & * \\ & & & & & & & & p_3 & \dots & & \\ & & & & & & & & & & & \vdots \\ & & & & & & & & & \dots & + & * & \dots & * \\ & & & & & & & & & & p_r & * & \dots & * \\ & & & & & & & & & & & & 0 \\ & & & & & & & & & & & & \vdots \\ & & & & & & & & & & & & 0 \end{pmatrix}$$

où les pivots  $p_i$  (i.e. les premiers coefficients non-nuls sur chaque ligne) sont strictement positifs, et les coefficients au dessus de chaque pivot sont positifs et inférieurs au pivot.

**Algorithme 35** (d'HERMITE - [G] 164). Soit  $M \in \mathcal{M}_{n,m}(\mathbb{Z}) \setminus \{0\}$ . On définit  $\delta_{i_0,j}(M) = \min \{|M_{i,j}| : i \geq i_0, M_{i,j} \neq 0\}$ . L'algorithme d'HERMITE :

Soit  $i_0 = 1$ . Tant que  $i_0 < n$  : soit  $j_0 = \min \{1 \leq j \leq m \mid \delta_{i_0,j}(M) \neq 0\}$

Si  $\forall i > i_0, M_{i,j_0} = 0$ , alors  $L_{i_0} \leftarrow sg(M_{i_0,j_0})L_{i_0}$ , et pour  $i$  allant de 1 à  $i_0 - 1$ ,  $L_i \leftarrow L_i - q_i L_{i_0}$  où  $q_i$  est le quotient de la division euclidienne de  $M_{i,j_0}$  par  $M_{i_0,j_0}$ . On remplace  $i_0$  par  $i_0 + 1$

Sinon, soit  $k \in \llbracket i_0, n \rrbracket$  tel que  $|M_{k,j_0}|$  soit non nul et minimal. On effectue  $L_i \longleftrightarrow L_{i_0}$  puis, pour  $i$  allant de  $i_0 + 1$  à  $n$ ,  $L_i \leftarrow L_i - q_i L_{i_0}$

transforme  $M$  sous une forme normale d'HERMITE  $M_H$ . En particulier, il existe  $P \in GL_n(\mathbb{Z})$  telle que  $M_H = PM$ .

**Application 36.** Résolution d'un système d'équations diophantiennes linéaires.

**Exemple 37.** Cas d'une seule équation linéaire

$$(E) : \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}^T \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = b \text{ avec } a_1 \wedge \dots \wedge a_n = 1.$$

D'après Cor 24, il existe  $P \in GL_n(\mathbb{Z})$  telle que

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}^T P = \begin{pmatrix} a_1 \wedge \dots \wedge a_n \\ 0 \\ \vdots \\ 0 \end{pmatrix}^T = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}^T$$

$$\text{De là, } (E) \iff \begin{pmatrix} 1 \\ \vdots \\ 0 \end{pmatrix}^T \begin{pmatrix} \tilde{x}_1 \\ \vdots \\ \tilde{x}_n \end{pmatrix} = b \iff \tilde{x}_1 = b \text{ où}$$

$$\begin{pmatrix} \tilde{x}_1 \\ \vdots \\ \tilde{x}_n \end{pmatrix} = P^{-1} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

$$\text{Donc } S(E) = \left\{ P \begin{pmatrix} 1 \\ x_1 \\ \vdots \\ x_n \end{pmatrix} \mid (x_2, \dots, x_n) \in \mathbb{Z}^{n-1} \right\}$$



## B. Un théorème de LIOUVILLE

**Théorème 38** (de LIOUVILLE - [FGN] 179, [R] 404). *L'équation  $P^n + Q^n + R^n = 0$  n'admet pas de solution non triviale (i.e.  $P, Q, R$  non associées) dans  $\mathbb{C}[X]$  dès lors que  $n \geq 3$ .*

## C. Quelques résultats en théorie des groupes

Soit  $G$  un groupe fini. On note  $\text{ord}(g)$  l'ordre de  $g \in G$ .

**Proposition 39** ([R] 9). *L'exposant de  $G$  ( $\max_{g \in G} \text{ord}(g)$ ) vaut  $\text{ppcm}(\{\text{ord}(g)\}_{g \in G})$ .*

**Lemme 40** ([R] 29). *Soit  $n \in \mathbb{N} \setminus \{0, 1\}$ , soit  $\bar{d} \in \mathbb{Z}/n\mathbb{Z}$ . On a  $\text{ord}(\bar{d}) = \frac{n^d}{n \wedge d}$ .*

**Théorème 41** (de structure des groupes abéliens finis - [R] 28). *Supposons  $G$  abélien, de cardinal au moins 2. Il existe  $(d_1, \dots, d_s) \in (\mathbb{N} \setminus \{0, 1\})^s$  tels que :*

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_s\mathbb{Z}, \quad d_1 \mid d_2 \mid \dots \mid d_s$$

*Les entiers  $d_1, \dots, d_s$  sont appelés facteurs invariants de  $G$ . Ils sont uniques et déterminent la classe d'isomorphisme de  $G$ .*

**Exemple 42.** *Soit  $p$  un nombre premier. Un groupe abélien d'ordre  $p^2$  est isomorphe à  $\mathbb{Z}/p^2\mathbb{Z}$  ou  $(\mathbb{Z}/p\mathbb{Z})^2$ .*

## Développements

- Développement 1 : Théorème des restes chinois 16 et Exemple de calcul 19.
- Développement 2 : Théorème de Liouville 38

## Références

- R *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition
- P *Cours d'algèbre*, Perrin
- D *Cours d'algèbre*, Michel Demazure
- FGN *Oraux X-ENS Algèbre 1*, Serge Francinou, Hervé Giannella, Serge Nicolas
- G *Algèbre I - Groupes, corps et théorie de Galois*, Daniel Guin, Thomas Hausberger

# 148 : Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

Dans toute cette leçon,  $E$  désigne espace vectoriel sur un corps  $K$ . On ne rappellera pas les éléments de la théorie des espaces vectoriels.

## I. Théorie de la dimension finie

### A. Familles libres, familles génératrices, bases

Soit  $\mathcal{F} \subseteq E$ .

**Définition 1** ([Gr] 11-11-10-13). On dit que  $\mathcal{F}$  est libre si :  $\forall (\vec{v}_1, \dots, \vec{v}_n) \in \mathcal{F}^n, \forall (\lambda_1, \dots, \lambda_n) \in K^n,$

$$\sum_{k=1}^n \lambda_k \vec{v}_k = \vec{0} \implies \lambda_1 = \dots = \lambda_n = 0$$

On dit que  $\mathcal{F}$  est liée si  $\mathcal{F}$  n'est pas libre.

On dit que  $\mathcal{F}$  est génératrice (de  $E$ ) si tout vecteur de  $E$  peut s'écrire comme combinaison linéaire finie de vecteurs de  $\mathcal{F}$ .

On dit que  $\mathcal{F}$  est une base de  $E$  si  $\mathcal{F}$  est à la fois libre et génératrice.

**Exemple 2.** — Dans  $\mathbb{R}^2$  :

- $\{(1, 1), (1, -1)\}$  est génératrice et libre ;
- $\{(0, 1), (1, 0), (2, 5)\}$  est génératrice et liée ;
- $\{(-4, 3)\}$  est non génératrice et libre ;
- $\{(1, 1), (2, 2)\}$  est non génératrice et liée ;

[Gr] 14 La famille  $\{(0, \dots, 1, \dots, 0)\}_{i \in \llbracket 1, n \rrbracket}$  est une base de  $K^n$ , appelée base canonique.

**Proposition 3** ([Gr] 13).  $\mathcal{F} = \{\}$  est une base de  $E$  si, et seulement si,  $\forall x \in E, \exists ! (\lambda_1, \dots, \lambda_n) \in K^n : x = \lambda_1 \vec{v}_1 + \dots + \lambda_n \vec{v}_n$

**Proposition 4** ([Gr] 14). —  $\{x\}$  est libre  $\iff x \neq 0$

- Toute sur-famille d'une famille génératrice (resp. liée) est génératrice (resp. liée)
- Toute sous-famille d'une famille libre est libre
- Une famille contenant le vecteur nul est liée

### B. Dimension d'un espace vectoriel

**Définition 5** ([Gr] 11). On dit que  $E$  est de dimension finie si  $E$  admet une famille génératrice finie.

**Exemple 6.** —  $K^n$  est un  $K$ -espace vectoriel de dimension finie, contrairement à  $K[X]$ .

- $\mathbb{R}$  est un  $\mathbb{Q}$ -espace vectoriel de dimension infinie.

**Lemme 7** (de STEINIZ - [Gr] 17). Si  $\mathcal{G} \subset E$  est finie et génératrice, alors toute famille de  $E$  contenant plus de  $\#\mathcal{G}$  éléments est liée.

**Théorème/Définition 8** ([Gr] 17). Si  $E$  est de dimension finie, alors toutes les bases de  $E$  ont le même cardinal (fini), que l'on appelle dimension de  $E$ , et que l'on note  $\dim_K(E)$  ou  $\dim(E)$  s'il n'y a pas d'ambiguïté sur  $K$ .

À partir de maintenant, on suppose  $E$  de dimension finie.

**Théorème 9** ([Gr] 18).  $\mathcal{B} \subseteq E$  est une base de  $E \iff \mathcal{B}$  est libre et  $\#\mathcal{B} = \dim(E) \iff \mathcal{B}$  est génératrice et  $\#\mathcal{B} = \dim(E)$ .

**Théorème 10** ([Gr] 19). Si  $F$  est un sous-espace vectoriel de  $E$ , alors  $F$  est de dimension finie, et  $\dim(F) \leq \dim(E)$  avec égalité si, et seulement si,  $E = F$ .

**Théorème 11** (des bases extraites et incomplètes - [Gr] 19). Soient  $\mathcal{L} \subseteq E$  libre et  $\mathcal{G} \subseteq E$  génératrice telles que  $\mathcal{L} \subseteq \mathcal{G}$ . Alors il existe une base  $\mathcal{B}$  de  $E$  telle que  $\mathcal{L} \subseteq \mathcal{B} \subseteq \mathcal{G}$ .

**Corollaire 12.** Tout espace vectoriel de dimension finie admet une base.

**Proposition 13** ([Gr] 63). Soit  $F$  un espace vectoriel de dimension finie. Les espaces vectoriels  $E$  et  $F$  sont isomorphes si, et seulement si,  $\dim(E) = \dim(F)$ .

**Exemple 14.** Soit  $(a_0, \dots, a_{p-1}) \in \mathbb{C}^p$ . L'application  $y \mapsto (y(0), y'(0), \dots, y^{(p-1)}(0))$  est un isomorphisme entre  $S_{\mathbb{R}}(E) = \{y \in C^p(\mathbb{R}, \mathbb{C}) \mid y^{(p)} = a_{p-1}y^{(p-1)} + \dots + a_0y\}$  et  $\mathbb{C}^p$ . Par conséquent,  $\dim(S_{\mathbb{R}}(E)) = p$ .

**Proposition 15** ([Gr] 22). Soient  $E_1, \dots, E_p$  supplémentaires dans  $E$ . Si  $\mathcal{B}_1, \dots, \mathcal{B}_p$  sont des bases de  $E_1, \dots, E_p$ , alors  $\mathcal{B} = \mathcal{B}_1 \sqcup \dots \sqcup \mathcal{B}_p$  est une base de  $E$ , dite adaptée à la décomposition  $E = E_1 \oplus \dots \oplus E_p$ .

**Corollaire 16** ([Gr] 22).  $\dim(E \oplus F) = \dim(E) + \dim(F)$

**Proposition 17** ([Gr] 23).

$$\begin{aligned} E = E_1 \oplus E_2 &\iff \begin{cases} E = E_1 + E_2 \\ \dim(E) = \dim(E_1) + \dim(E_2) \end{cases} \\ &\iff \begin{cases} E_1 \cap E_2 = \{\vec{0}\} \\ \dim(E) = \dim(E_1) + \dim(E_2) \end{cases} \end{aligned}$$

## C. Calculs de dimensions

Dans ce paragraphe,  $F$  est un espace vectoriel de dimension finie.

**Théorème 18** (Formule de GRASSMANN - [Gr] 24).  $\dim(E + F) = \dim(E) + \dim(F) - \dim(E \cap F) < +\infty$

**Proposition 19** ([Gr] 18).  $\dim(E \times F) = \dim(E) + \dim(F) < +\infty$

**Proposition 20.**  $\dim(\mathcal{L}(E, F)) = \dim(E) \times \dim(F) < +\infty$

## D. Extensions de corps

Dans ce paragraphe,  $F/L/K$  est une tour d'extensions de corps.

**Définition 21** ([P] 65). On appelle degré de  $L/K$  l'entier  $[L : K] = \dim_K(L)$ .

**Théorème 22** (de la base télescopique - [P] 65). Supposons  $F/L$  et  $L/K$  de degrés finis : elles admettent alors des bases  $\{f_1, \dots, f_n\}$  et  $\{e_1, \dots, e_p\}$  respectivement.

La famille  $\{e_i f_j\}_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}}$  est une base de  $F/K$ , et donc  $[F : K] = [F : L] \cdot [L : K]$ .

**Définition 23** ([P] 66). On dit que  $\alpha \in L$  est algébrique sur  $K$  s'il existe  $P \in K[X] \setminus \{0\}$  tel que  $P(\alpha) = 0$ .

Le cas échéant, on définit le polynôme minimal de  $\alpha$  sur  $K$  comme étant l'unique générateur unitaire de l'idéal  $\{P \in K[X] \mid P(\alpha) = 0\}$ , appelé idéal annulateur de  $\alpha$ .

**Notation 24** ([P] 66). Soit  $\alpha \in L$ . On pose  $K[\alpha] = \{P(\alpha) \mid P \in K[X]\}$  et  $K(\alpha = \text{Frac}(K[\alpha]))$ .

**Théorème 25** ([P] 66). Soit  $\alpha \in L$ . Sont équivalentes :

1.  $\alpha$  est algébrique sur  $K$
2.  $K[\alpha] = K(\alpha)$
3.  $[K[\alpha] : K] < +\infty$

Le cas échéant,  $[K[\alpha] : K]$  est le degré du polynôme minimal de  $\alpha$  sur  $K$ .

## II. Rang d'une application linéaire, d'une matrice, d'une famille

### A. Définitions - formule du rang et conséquences

Dans ce paragraphe, on se donne  $F$  de dimension finie,  $u \in \mathcal{L}(E, F)$ , une base  $\mathcal{B} = (e_1, \dots, e_n)$  de  $E$ , et  $(x_1, \dots, x_r) \in E^r$ .

**Définition 26** ([Gr] 61,82). 1. Le rang de  $u$  est l'entier  $\text{rg}(u) = \dim(\text{Im}(u))$  ;  
2. Le rang de  $\{x_1, \dots, x_r\}$  est l'entier  $\text{rg}(x_1, \dots, x_r) = \dim(\text{Vect}(x_1, \dots, x_r))$ .

**Proposition 27** ([Gr] e82).  $\text{rg}(u) = \text{rg}(u(e_1), \dots, u(e_n))$

**Théorème 28** (du rang - [Gr] 64).  $\dim(E) = \dim(\text{Ker}(u)) + \text{rg}(u)$

**Théorème 29** ([Gr] 65). Si  $\dim(F) = \dim(E)$ , alors  $u$  bijective  $\iff u$  injective  $\iff u$  surjective  $\iff \exists v \in \mathcal{L}(F, E) : u \circ v = \text{id}_E \iff \exists v \in \mathcal{L}(E, F) : v \circ u = \text{id}_F$ .

**Exemple 30** ([Gr] 65). Ce n'est pas vrai en dimension infinie : dans  $K[X]$ ,  $P \mapsto P'$  est surjective mais pas injective.

**Proposition 31.** —  $\forall v \in GL(E), \text{rg}(u \circ v) = \text{rg}(u)$   
—  $\forall w \in GL(F), \text{rg}(w \circ u) = \text{rg}(u)$

**Corollaire 32.** Le rang est invariant par équivalence.

### B. Le cas particulier des matrices

Soit  $A \in \mathcal{M}_{n,p}(K)$ . Notons  $C_1, \dots, C_p$  ses colonnes et  $L_1, \dots, L_n$  ses lignes.

**Définition 33** ([Gr] 33). Le rang de  $A$  est l'entier  $\text{rg}(A) = \dim(\{AX \mid X \in \mathcal{M}_{n,1}(K)\}) = \text{rg}(C_1, \dots, C_p)$ .

**Proposition 34** ([Gr] 82). Le rang d'une application linéaire est le rang de sa matrice dans n'importe quel couple de bases.

**Théorème 35** ([Go] 128).  $\text{rg}(A) = r \implies A$  est équivalente à  $J_{n,p,r} := \begin{pmatrix} I_r & 0_{p-r} \\ 0_{n-r} & 0_* \end{pmatrix}$ .

**Corollaire 36** ([Go] 128). Deux matrices sont équivalentes si, et seulement si, elles ont le même rang.

**Remarque 37** ([Go] 128). Pour déterminer le rang de  $A$  en pratique, on utilise l'algorithme du pivot de GAUSS pour transformer  $A$  en  $J_{n,p,r}$ .

**Théorème 38** ([Gr] 83).  $\text{rg}(A) = \text{rg}(^t A)$

**Théorème 39** ([Go] 128). Le rang de  $A$  est la taille de sa plus grande sous-matrice inversible, donc l'ordre de son plus grand mineur non nul.

**Corollaire 40.** Si  $L/K$  est une extension de  $K$ , alors  $\text{rg}_K(A) = \text{rg}_L(A)$ .

## III. Applications

### A. Formes quadratiques réelles

**Théorème 41** (Loi d'inertie de SYLVESTER - [R] 476). Soient  $E$  un  $\mathbb{R}$ -espace vectoriel de dimension finie  $n > 0$ , et  $q$  est une forme quadratique sur  $E$ . Soit  $\mathcal{B} = \{e_1, \dots, e_n\}$  une base de  $E$  orthogonale pour  $q$ . Quitte à renuméroter  $\mathcal{B}$ , supposons que  $q(e_1) > 0, \dots, q(e_s) > 0, q(e_{s+1}) < 0, \dots, q(e_{s+t}) < 0, q(e_{s+t+1}) = \dots = q(e_n) = 0$ . Le couple  $(s, t)$  ne dépend alors pas du choix de la base orthogonale : on l'appelle signature de  $q$ .

**Théorème 42.** La classe de congruence d'une forme quadratique réelle ne dépend que du rang et de la signature.

### B. Réduction des endomorphismes

Dans ce paragraphe, on fixe  $u \in \mathcal{L}(E)$ .

**Proposition/Définition 43** ([R] 604).  $\{P \in K[X] \mid P(u) = 0_{\mathcal{L}(E)}\}$  est un idéal non nul : son unique générateur unitaire est appelé polynôme minimal de  $u$ . On le note  $\mu_u$ .

**Théorème 44** ([R] 683).  $u$  est diagonalisable  $\iff \mu_u$  est scindé à racines simples.

Dans le groupe suivant,  $E$  est un espace euclidien et  $u \in \mathcal{L}(E)$ .

**Définition 45** ([R] 743). On dit que  $u$  est normal si  $uu^* = u^*u$  où  $u^*$  est l'adjoint de  $u$ .

**Lemme 46** ([R] 745). Si  $u$  est normal,  $\exists P_1, \dots, P_r$  sont de dimension 1 ou 2, deux à deux orthogonaux et stables par  $u$  tels que  $E = P_1 \oplus \dots \oplus P_r$ .

**Théorème 47.** Si  $u$  est normal, alors il existe une base orthonormée  $\mathcal{B}$  de  $E$  telle que  $\text{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} D & & \\ & \ddots & \\ & & R_p \end{pmatrix}$  par blocs, avec  $D$  diagonale et les  $R_k$  de la forme  $\begin{pmatrix} a_k & -b_k \\ b_k & a_k \end{pmatrix}$ ,  $b_k \neq 0$ .

## Développements

- Développement 1 : Loi inertie Sylvester 41 et Th 42.
- Développement 2 : Lemme 46 et Théorème 47

## Références

- R *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition
- P *Cours d'algèbre*, Perrin
- Gr *Algèbre linéaire*, Joseph Grifone, 6e édition, 2e version
- Go *Les maths en tête - Algèbre et Probabilités*, Xavier Gourdon, 3e édition

# 149 : Déterminant. Exemples et applications.

Dans cette leçon,  $K$  désigne un corps,  $\mathbb{K}$  désigne  $\mathbb{R}$  ou  $\mathbb{C}$ , et  $E$  est un  $\mathbb{K}$ -espace vectoriel de dimension finie  $n \geq 1$ . On fixe une base  $\mathcal{B} = (e_1, \dots, e_n)$  de  $E$ .

## I. Les notions de déterminants

### A. Des formes multilinéaires au déterminant d'une famille de vecteurs

**Définition 1** ([Go] 140). Une forme  $k$ -linéaire sur  $E$  est une application  $\varphi : E^k \rightarrow \mathbb{K}$  telle que pour tout  $i \in \llbracket 1, k \rrbracket$ , pour tout  $(x_1, \dots, x_k) \in E^k$ ,  $\varphi(x_1, \dots, x_{i-1}, \cdot, x_{i+1}, \dots, x_k)$  est linéaire. On note  $\bigotimes^k E^*$  l'ensemble des formes  $k$ -linéaires sur  $E$ .

**Proposition 2.**  $(e_{i_1}^* \otimes \dots \otimes e_{i_k}^*)_{1 \leq i_1 \leq \dots \leq i_k \leq n}$  est une base de  $\bigotimes^k E^*$ , où pour  $(x_1, \dots, x_k) \in E^k$ ,  $e_{i_1}^* \otimes \dots \otimes e_{i_k}^*(x_1, \dots, x_k) = e_{i_1}^*(x_1) \dots e_{i_k}^*(x_k)$ .

**Définition 3** ([Go] 140-141). Une forme  $k$ -linéaire alternée est une forme  $k$ -linéaire  $\varphi \in \bigotimes^k E^*$  telle que  $\forall \sigma \in \mathfrak{S}_k$ ,  $\forall (x_1, \dots, x_k) \in E^k$ ,  $\varphi(x_{\sigma(1)}, \dots, x_{\sigma(k)}) = \varepsilon(\sigma) \varphi(x_1, \dots, x_k)$ .

On note  $\bigwedge^k E^*$  l'espace des formes  $k$ -linéaires alternées sur  $E$ .

**Proposition 4.**  $(e_{i_1}^* \wedge \dots \wedge e_{i_k}^*)_{1 \leq i_1 < \dots < i_k \leq n}$  est une base de  $\bigwedge^k E^*$ , où pour  $(x_1, \dots, x_k) \in E^k$ ,  $e_{i_1}^* \wedge \dots \wedge e_{i_k}^*(x_1, \dots, x_k) = \sum_{\sigma \in \mathfrak{S}_k} \varepsilon(\sigma) e_{i_1}^*(x_{\sigma(1)}) \dots e_{i_k}^*(x_{\sigma(k)})$ .

**Corollaire 5.** On a  $\dim(\bigwedge^k E^*) = \binom{n}{k}$ .

**Définition 6** ([Go] 141). On appelle déterminant dans la base  $\mathcal{B}$  l'unique forme  $n$ -linéaire alternée  $\det_{\mathcal{B}}$  sur  $E$  vérifiant  $\det_{\mathcal{B}}(\mathcal{B}) = 1$ . (La famille  $(\det_{\mathcal{B}})$  est une base de  $\bigwedge^n E^*$ .)

**Proposition 7** ([Go] 141).  $\forall (x_1, \dots, x_n) \in E^n$ ,  $\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) e_1^*(x_{\sigma(1)}) \dots e_n^*(x_{\sigma(n)})$ .

**Corollaire 8** ([Go] 141). Soient  $\varphi \in \bigwedge^n E^*$  et  $\mathcal{B}'$  une autre base de  $E$ . On a  $\varphi = \varphi(\mathcal{B}) \det_{\mathcal{B}}$ , en particulier on a donc  $\det_{\mathcal{B}'} = \det_{\mathcal{B}'}(\mathcal{B}) \det_{\mathcal{B}}$ .

**Proposition 9** ([Go] 141-142). Soit  $(x_1, \dots, x_n) \in E^n$ . Sont équivalentes :

1.  $(x_1, \dots, x_n)$  est liée ;
2. Pour toute base  $\mathcal{B}$  de  $E$ ,  $\det_{\mathcal{B}}(x_1, \dots, x_n) = 0$  ;
3. Il existe une base  $\mathcal{B}$  de  $E$  telle que  $\det_{\mathcal{B}}(x_1, \dots, x_n) = 0$ .

### B. Déterminant d'une matrice carrée, d'un endomorphisme

Soient  $u \in \mathcal{L}(E)$  et  $A = (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{R})$ .

**Définition 10** ([Go] 142). Si  $C_1, \dots, C_n$  sont les colonnes de  $A$ , alors :

$$\det(A) := \det_{\mathcal{E}}(C_1, \dots, C_n) = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) a_{1,\sigma(1)} \dots a_{n,\sigma(n)}$$

où  $\mathcal{E}$  désigne la base canonique de  $K^n$ .

**Proposition 11** ([Go] 142). Soient  $\lambda \in K$  et  $B \in \mathcal{M}_n(K)$ .

1.  $\det(A)$  ne change pas si on ajoute à une colonne une combinaison linéaire des autres colonnes ;
2.  $\det(A^T) = \det(A)$
3.  $\det(\lambda A) = \lambda^n \det(A)$
4.  $\det(AB) = \det(A) \det(B)$
5.  $A \in GL_n(K) \iff \det(A) \neq 0$  (auquel cas,  $\det(A^{-1}) = \det(A)^{-1}$ )

**Définition 12** ([Go] 142). Le déterminant de  $u$ , défini par :  $\det(u) = \det_{\mathcal{B}}(u(e_1), \dots, u(e_n)) = \det(\text{Mat}_{\mathcal{B}}(u))$  ne dépend pas du choix de  $\mathcal{B}$ .

### C. Propriétés analytiques

**Proposition 13** ([Rv] 83).  $A \mapsto \det A$  est polynomiale en les coefficients de  $A$  (relativement à la base canonique de  $\mathcal{M}_n(K)$ ), donc lisse.

**Corollaire 14.**  $GL_n(\mathbb{K})$  est ouvert dans  $\mathcal{M}_n(\mathbb{K})$ , et  $SL_n(\mathbb{R})$  est fermé.

**Proposition 15** ([Rv] 83).  $\forall x \in \mathcal{M}_n(\mathbb{R})$ ,  $\forall H \in \mathcal{M}_n(\mathbb{R})$ ,  $d(\det)(X)(H) = \text{tr}(\text{Com}(X)^T H)$ , où  $\text{Com}(X)$  est appelée dans le paragraphe II.B.

## II. Calcul pratique d'un déterminant

### A. Cas simples, pivot de GAUSS

**Notation 16** ([Go] 142). On note  $|A|$  le déterminant d'une matrice carrée  $A$ .

**Proposition 17** ([Go] 106).  $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc$

$\begin{vmatrix} a & b & c \\ d & e & f \\ i & j & k \end{vmatrix} = aek + bfi + djc - cei - fja - bdk$  (règle de SARRUS)

**Lemme 18** ([Go] 142). Si  $A = (a_{i,j})_{1 \leq i,j \leq 1}$  est triangulaire, alors  $\det(A) = a_{1,1} a_{2,2} \dots a_{n,n}$ .

**Algorithme 19** (pivot de GAUSS). Pour calculer le déterminant d'une matrice, on peut la transformer en une matrice triangulaire par des opérations élémentaires sur les lignes et les colonnes :

- la transvection  $(C_i \rightarrow C_i + \lambda C_j)$  ne change pas le déterminant ;
- la permutation  $(C_i \leftrightarrow C_j)$  change le signe du déterminant ;
- la dilatation  $(C_i \Rightarrow \alpha C_i)$  change le déterminant d'un facteur  $\alpha$ .

**Exemple 20.**

$$\begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ -1 & -1 & 0 \end{vmatrix} = \begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{vmatrix} = 1$$

**Théorème 21** ([Go] 142). Le déterminant d'une matrice triangulaire par blocs est égal au produit des déterminants des blocs diagonaux.

## B. Mineurs, cofacteurs et développements

Soient  $A = (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(K)$ .

**Définition 22** ([Go] 142). Soit  $(i, j) \in \llbracket 1, n \rrbracket^2$ . On appelle mineur d'indice  $(i, j)$  de  $A$  le déterminant de la matrice extraite de  $A$  en supprimant sa  $i$ -ième ligne et sa  $j$ -ième colonne. On note  $\Delta_{i,j}$  ce mineur.

On appelle cofacteur d'indice  $(i, j)$  de  $A$  la quantité  $A_{i,j} = (-1)^{i+j} \Delta_{i,j}$ .

On appelle comatrice de  $A$  la matrice  $\text{Com}(A) = (A_{i,j})_{1 \leq i,j \leq n}$ .

**Théorème 23** (Formules de développement d'un déterminant

Par rapport à la  $i$ -ième ligne :  $\det A = \sum_{j=1}^n a_{i,j} A_{i,j}$

— Par rapport à la  $j$ -ième colonne :  $\det A = \sum_{i=1}^n a_{i,j} A_{i,j}$

**Exemple 24.**  $\begin{vmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ -1 & -1 & 0 \end{vmatrix} = 1 \cdot \begin{vmatrix} 1 & 1 \\ -1 & 0 \end{vmatrix} - 0 \cdot \begin{vmatrix} 1 & 1 \\ -1 & 0 \end{vmatrix} + (-1) \cdot \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix}$

$$\begin{vmatrix} 1 & 1 \\ 1 & 1 \end{vmatrix} = 1 - 0 + 0 = 1$$

**Théorème 25** (Formule de la comatrice - [Go] 143).  $A \text{Com}(A)^T = \text{Com}(A)^T A = \det(A) I_n$

## C. Déterminants remarquables

**Exemple 26** (déterminant circulant - [Go] 143; [IP] 388). Pour tout  $(a_1, \dots, a_n) \in \mathbb{C}^n$ ,

$$\begin{vmatrix} a_1 & a_2 & a_3 & \cdots & a_n \\ a_n & a_1 & a_2 & \cdots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \cdots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{vmatrix} = \prod_{k=1}^n P(\omega^k)$$

où  $\omega = e^{\frac{2i\pi}{n}}$  et  $P = \sum_{i=0}^{n-1} a_{i+1} X^i$ .

**Application 27** (FIG 1 - [IP] 388). Soient  $z_1, \dots, z_n$  des complexes qui sont les affixes des points  $M_1, \dots, M_n$ . On définit une suite de polygones du plan comme suivant :

- $P_0 = M_1 \dots M_n$
- Pour  $n \geq 1$ ,  $P_n$  est le polygone dont les sommets sont les milieux des arêtes de  $P_{n-1}$ . Alors  $(P_n)_n$  converge vers l'isobarycentre de  $P_0$ .

**Exemple 28** (déterminant de VANDERMONDE - [Go] 143). Pour tout  $(a_1, \dots, a_n) \in K^n$ ,

$$\begin{vmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{vmatrix} = \prod_{1 \leq i, j \leq n} a_i - a_j$$

## III. Applications des déterminants...

### A. ...en algèbre linéaire

**Remarque 29** ([BMP] 181). On étend la formule explicite du déterminant au cas des matrices à coefficients dans un anneau intègre  $A$ . Si  $M \in \mathcal{M}_n(A)$ , alors  $\det(M) \in A$ , et par plongement de  $A$  dans  $\text{Frac}(A)$ , les propriétés déjà vues restent vraies.

**Définition 30** ([Go] 172). Le polynôme caractéristique de  $A \in \mathcal{M}_n(K)$  est  $\chi_A = \det(XI_n - A)$ .

Le polynôme caractéristique d'un endomorphisme est celui de sa matrice dans n'importe quelle base.

**Proposition 31** ([Go] 159; [C] 47). —  $\forall A \in \mathcal{M}_n(K)$ ,  $\text{Sp}(A) = \chi_A^{-1}(\{0\})$

—  $\forall (A, B) \in \mathcal{M}_n(\mathbb{C})$ ,  $\chi_{AB} = \chi_{BA}$

**Théorème 32** (de CAYLEY-HAMILTON - [M2] 81).  $\forall A \in \mathcal{M}_n(\mathbb{K})$ ,  $\chi_A(A) = 0$ .

**Théorème 33** (Systèmes de CRAMER - [Gr] 145). Soient  $A \in \mathcal{M}_n(K)$  et  $B \in K^n$ . On note  $A_1, \dots, A_n$  les colonnes de  $A$ . La solution de  $AX = B$  est donnée par  $X = (x_1, \dots, x_n)$  où

$$\forall i \in \llbracket 1, n \rrbracket, \quad x_i = \frac{\det(A_1, \dots, A_{i-1}, B, A_{i+1}, \dots, A_n)}{\det(A)}$$

### B. ...en calcul intégral

**Théorème 34** (de changement de variable - ADMIS - [BP] 255-256). Soient  $U$  et  $V$  deux ouverts de  $\mathbb{R}^n$ , et  $\varphi : U \rightarrow V$  un  $C^1$ -difféomorphisme. Pour tout fonction  $f : V \rightarrow \mathbb{R}^+$  borélienne,

$$\int_U f \circ \varphi(u) \cdot |\det(d\varphi(u))| du = \int_V f(v) dv$$

**Application 35.**  $\forall \alpha > 0$ ,  $\int_{\mathbb{R}} e^{-\alpha x^2} dx = \sqrt{\frac{\pi}{\alpha}}$

**Théorème 36** ([BMP] 184). Notons  $\lambda$  la mesure de LEBESGUE sur  $\mathbb{R}^n$ . Pour tous  $X \subseteq \mathbb{R}^n$  mesurable et  $u \in \mathcal{L}(\mathbb{R}^n)$ ,  $\lambda(u(X)) = |\det(u)| \cdot \lambda(X)$

**Corollaire 37** (FIG. 3 - [BMP] 184). Soit  $(v_1, \dots, v_n) \in \mathbb{R}^n$ , notons  $\mathcal{P}(v_1, \dots, v_n) = \{\sum_{i=1}^n \lambda_i v_i \mid 0 \leq \lambda_i \leq 1\}$  le parallélotope engendré par  $v_1, \dots, v_n$ . On a  $\lambda(\mathcal{P}(v_1, \dots, v_n)) = |\det(v_1, \dots, v_n)|$ .

### C. ...en géométrie

Dans ce paragraphe,  $(E, \langle \cdot | \cdot \rangle)$  est un  $\mathbb{K}$ -espace préhilbertien.

**Définition 38** ([Go] 274). Soit  $(x_1, \dots, x_n) \in E^n$ . On appelle matrice de GRAM de  $x_1, \dots, x_n$  la matrice  $M_G(x_1, \dots, x_n) = (\langle x_i | x_j \rangle)_{1 \leq i, j \leq n}$ , et déterminant de GRAM de  $x_1, \dots, x_n$  sont déterminant  $G(x_1, \dots, x_n)$ .

**Théorème 39** ([Go] 275). Soient  $F$  un sous-espace vectoriel de  $E$ , et  $\mathcal{B} = (e_1, \dots, e_n)$  une base de  $F$ . Alors,  $\forall x \in E$ ,  $d(x, F)^2 = \frac{G(e_1, \dots, e_n, x)}{G(e_1, \dots, e_n)}$ .

**Théorème 40** (inégalités de HADAMARD - [Go] 275). On a :

1.  $\forall (x_1, \dots, x_n) \in E^n$ ,  $G(x_1, \dots, x_n) \leq \|x_1\|^2 \dots \|x_n\|^2$
2.  $\forall (x_1, \dots, x_n) \in (\mathbb{C}^n)^n$ ,  $|\det(x_1, \dots, x_n)| \leq \|x_1\|_2 \dots \|x_n\|_2$

De plus, dans les deux points, il y a égalité si, et seulement si,  $(x_1, \dots, x_n)$  est orthogonale.

### Développements

- Développement 1 : Exemple 26 et Application 27.
- Développement 2 : Théorèmes 39 et 40



## Références

Rv *Petit guide du calcul différentiel*, François Rouvière, 4e édition

IP *L'oral à l'agrégation de mathématiques*, Lucas Issenmann, Timothée Pecatte

M2 *Algèbre linéaire. Réduction des endomorphismes*, Roger Mansuy, Rached Mneimné, 3e édition

Gr *Algèbre linéaire*, Joseph Grifone, 6e édition, 2e version

Go *Les maths en tête - Algèbre et Probabilités*, Xavier Gourdon, 3e édition

BMP *Objectif Agrégation*, Vincent Beck, Jérôme Malick, Gabriel Peyré, 2e édition

BP *Théorie de l'intégration*, Marc Briane, Gilles Pagès, 7e édition

C *Carnet de voyage en Algèbre*, Philippe Caldero, Marie Peronnier

FIGURE 1: Règle de SARRUS

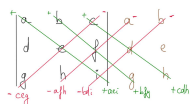
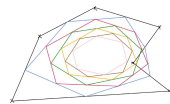


FIGURE 2: Suite de polygones



### RÉFÉRENCES

- [Go]: Les maths en tête - Algèbre et Probabilités (Xavier Gourdon) [3<sup>e</sup> édition]
- [Gr]: Algèbre linéaire (Joseph Grifone) [6<sup>e</sup> édition, 2<sup>e</sup> version]
- [Rv]: Petit guide du calcul différentiel (François Rouvière) [4<sup>e</sup> édition]
- [IP]: L'oral à l'agrégation de mathématiques (Lucas Issenmann, Timothée Pecatte)
- [M2]: Algèbre linéaire (Réduction des endomorphismes) (Roger Mansuy, Rached Mneimné) [3<sup>e</sup> édition]
- [C]: Carnet de voyage en Algèbre (Philippe Caldero, Marie Peronnier)
- [BMP]: Objectif Agrégation [2<sup>e</sup> édition] (Vincent Beck, Jérôme Malick, Gabriel Peyré)
- [BP]: Théorie de l'intégration (Marc Briane, Gilles Pagès) [7<sup>e</sup> édition]

FIGURE 3: Lien entre volume et déterminant

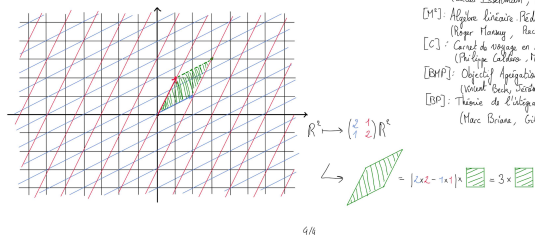


FIGURE 1.4 – s

# 151 : Sous-espaces stables par un endomorphisme ou une famille d'endomorphismes d'un espace vectoriel de dimension finie. Applications.

Soient  $K$  un corps commutatif,  $E$  un  $K$ -espace vectoriel de dimension  $n \geq 1$  et  $u \in \mathcal{L}(E)$ . Soit  $F$  un sous-espace vectoriel de  $E$ .

## I. Stabilité d'un sous-espace par un endomorphisme

### A. Introduction

**Définition 1** ([M2] 17). On dit que  $F$  est stable par  $u$  (ou  $u$ -stable) si  $u(F) \subseteq F$ .

**Exemple 2** ([M2] 17). On a :

- $\{0\}$ ,  $\text{Ker}(u)$ ,  $\text{Im}(u)$  et  $E$  sont stables par  $u$ .
- $\forall P \in K[X]$ ,  $\text{Ker}(P(u))$  et  $\text{Im}(P(u))$  sont stables par  $u$ .

**Proposition 3** ([M2] 17). Soit  $v \in \mathcal{L}(E)$ . Si  $v$  commute avec  $u$ , alors pour tout  $P \in K[X]$ ,  $\text{Ker}(P(u))$  et  $\text{Im}(P(u))$  sont stables par  $u$ .

**Remarque 4.** En particulier,  $\forall \lambda \in K$ ,  $E_\lambda(u) := \text{Ker}(u - \lambda \text{id}_E)$  est stable par  $u$ , et par tout endomorphisme qui commute avec  $u$ .

**Proposition 5** ([M2] e17). Soit  $E = F \oplus G$  une décomposition de  $E$ , soit  $\mathcal{B}$  une base de  $E$  adaptée à cette décomposition, notation  $\text{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$  par blocs. Alors  $F$  (resp.  $G$ ) est stable par  $u$  si, et seulement si,  $C = 0$  (resp.  $B = 0$ ).

**Corollaire 6** ([M2] e120).  $F$  est stable par  $u$  si, et seulement si,  $F^\perp$  est stable par  ${}^t u$ . (NB :  $\text{Mat}_{\mathcal{B}^*}({}^t u) = {}^t \text{Mat}_{\mathcal{B}}(u)$ ).

### B. Notion d'endomorphisme induit

**Définition 7** ([M2] 17). Si  $F$  est stable par  $u$ , alors on dispose de l'endomorphisme induit par  $u$  sur  $F : u_F : F \rightarrow F, x \mapsto u(x)$ .

**Proposition 8** ([M2] 55, 18). Si  $F$  est stable par  $u$ , alors  $\chi_{u_F} \mid \chi_u$  et  $\pi_{u_F} \mid \pi_u$ .

**Corollaire 9** ([M2] 93). Si  $F$  est stable par  $u$  et si  $u$  est diagonalisable (resp. trigonalisable, resp. nilpotent), alors  $u_F$  aussi.

**Proposition 10** ([M2] 55, 18). Si  $E = F_1 \oplus \dots \oplus F_p$  est une décomposition de  $E$  en somme de sous-espaces stables, alors :  $\chi_u = \chi_{u_{F_1}} \dots \chi_{u_{F_p}}$  et  $\pi_u = \pi_{u_{F_1}} \vee \dots \vee \pi_{u_{F_p}}$ .

## II. Application à la réduction des endomorphismes

**Lemme 11** (des noyaux - [M2] 43).  $\forall (P, Q) \in K[X]^2, P \wedge Q = 1 \implies \text{Ker}((PQ)(u)) = \text{Ker}(P(u)) \oplus \text{Ker}(Q(u))$

### A. Diagonalisation, trigonalisation

**Théorème 12** (de CAYLEY-HAMILTON - [M2] 82).  $\chi_u(u) = 0_{\mathcal{L}(E)}$

**Corollaire 13.**  $E = \bigoplus_{\lambda \in \text{Sp}(u)} \text{Ker}((u - \lambda \text{id}_E)^{\mu_{\lambda}(u)})$  est une décomposition de  $E$  en somme de sous-espaces stables.

**Proposition 14** ([M2] 84). Écrivons  $\chi_u = \prod_{\lambda \in \text{Sp}(u)} (X - \lambda)^{m(\lambda)}$  et posons  $E_\lambda(u) = \text{Ker}(\lambda \text{id}_E - u)$ . Pour tout  $\lambda \in \text{Sp}(u)$ ,  $1 \leq \dim(E_\lambda(u)) \leq m(\lambda)$ .

**Théorème 15** ([R] 683 ; [M2] 90-93). On a :

- $u$  est diagonalisable  $\iff \pi_u$  est scindé à racines simples  $\iff$  il existe  $P$  annulateur de  $u$  scindé à racines simples  $\iff \chi_u$  est scindé et  $\forall \lambda \in \text{Sp}(u)$ ,  $\dim(E_\lambda(u)) = \mu_{\chi_u}(\lambda)$ .
- $u$  est trigonalisable  $\iff \chi_u$  est scindé  $\iff$  il existe un polynôme scindé qui annule  $u$ .

**Théorème 16** (de réduction simultanée - [M2] 94,107). Soit  $(u_i)_{i \in I} \in \mathcal{L}(E)^I$  une famille d'endomorphismes qui commutent deux à deux. Si tous les  $u_i, i \in I$  sont diagonalisables (resp. trigonalisables), alors il existe une base de  $E$  qui diagonalise (resp. trigonalise) simultanément tous les  $u_i, i \in I$ .

**Lemme 17** ([R] 743). Il existe un sous-espace de  $E$  de dimension 1 ou 2 stable par  $u$ .

### B. Cas des endomorphismes normaux

Dans l'encadré suivant, on suppose  $u$  normal

**Lemme 18** ([R] 743). Si  $F$  est un sous-espace de  $E$  stable par  $u$ , alors  $F^\perp$  est stable par  $u$ .

**Lemme 19** ([R] 744). Il existe des sous-espaces  $P_1, \dots, P_r$  de  $E$  stables par  $u$ , de dimension 1 ou 2, deux à deux orthogonaux, tels que

$$E = P_1 \bigoplus \dots \bigoplus P_r$$

**Lemme 20** (PAS DEV - [R] 745). Si  $n = \dim E = 2$ , alors :

- Si  $u$  admet une valeur propre réelle, alors  $u$  est diagonalisable dans une base orthonormée,
- Sinon, pour toute base orthonormée  $\mathcal{B}$  de  $E$ , il existe  $(a, b) \in \mathbb{R}^2$  tel que  $b \neq 0$  et  $\text{Mat}_{\mathcal{B}}(u) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ .

**Théorème 21** (de réduction des endomorphismes normaux - [R] 745). Il existe une base orthonormée  $\mathcal{B}$  de  $E$  telle que, par blocs,  $\text{Mat}_{\mathcal{B}}(u) = \text{diag}(D_p, R_1, \dots, R_r)$ , où  $D_p \in \mathcal{M}_n(\mathbb{R})$  est diagonale,  $\forall i \in \llbracket 1, n \rrbracket, \exists (a_i, b_i) \in \mathbb{R}^2 : b_i \neq 0$  et  $R_i = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix}$  et  $p + 2r = n$ .

**Corollaire 22** (théorème spectral - [R] 746 (734)). Tout endomorphisme auto-adjoint se diagonalise dans une base orthonormée.

**Corollaire 23** ([R] 727). Si  $u$  est orthogonal, alors il existe une base de  $E$  dans laquelle la matrice de  $u$  est de la

$$\text{forme, par blocs : } \begin{pmatrix} I_p & & & \\ & -I_q & & \\ & & R_1 & \\ & & & \ddots \\ & & & & R_r \end{pmatrix}, \text{ où } R_k = \begin{pmatrix} \cos(\theta_k) & -\sin(\theta_k) \\ \sin(\theta_k) & \cos(\theta_k) \end{pmatrix}$$

**Proposition 24.** Si  $u$  est une rotation et que  $\dim(E)$  est impaire, alors  $\text{Ker}(u - \text{id}_E) \neq \{0\}$ .

## Références

- R *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition  
M2 *Algèbre linéaire. Réduction des endomorphismes*, Roger Mansuy, Rached Mneimné, 3e édition

## II. Application à la décomposition des endomorphismes

### A. Décomposition de JORDAN des endomorphismes nilpotents

**Définition 25** ([M2] 143). On appelle bloc de JORDAN de taille  $d$  la matrice :

$$J_d := \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 \\ 0 & \cdots & \cdots & 0 \end{pmatrix}$$

Pour  $\lambda = (\lambda_1, \dots, \lambda_r) \in \mathbb{N}^r$ , on pose  $J_\lambda = \text{diag}(J_{\lambda_1}, \dots, J_{\lambda_r})$ .

**Théorème 26** (décomposition de JORDAN des endomorphismes nilpotents - [M2] 144). Supposons  $u$  nilpotent d'indice  $\lambda_1$ . Il existe  $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_r$  telle que  $\lambda_1 + \dots + \lambda_r = n$ , et  $\mathcal{B}$  une base de  $E$  telle que  $\text{Mat}_{\mathcal{B}}(u) = J_{\lambda_1, \dots, \lambda_r}$ . Cette décomposition est unique.

### B. Décomposition de DUNFORD

**Théorème 27** (décomposition de DUNFORD - [M2] 141 ; [R] 613). Si  $u$  est trigonalisable, alors il existe un unique couple  $(d, n) \in \mathcal{L}(E)^2$  tel que  $u = d + n$ ,  $d \circ n = n \circ d$ ,  $d$  est diagonalisable et  $n$  est nilpotent.

**Corollaire 28** ([R] 634). Sur  $K = \mathbb{R}$  ou  $K = \mathbb{C}$ ,  $e^u$  est diagonalisable si, et seulement si,  $u$  l'est.

### C. Une application : le critère de diagonalisabilité de KLARÈS

**Théorème 29** (critère de KLARÈS - [M2] 154). Posons  $\text{ad}_u : v \in \mathcal{L}(E) \mapsto u \circ v - v \circ u$ . Si  $u$  est trigonalisable, alors :

$$u \text{ diagonalisable} \iff \text{Ker}(\text{ad}_u) = \text{Ker}(\text{ad}_u^2)$$

## Développements

- Développement 1 : Lemmes 17, 18, 19 et Théorème ??.
- Développement 2 : Théorème 29

# 155 : Exponentielle de matrices. Applications.

Dans cette leçon,  $\mathbb{K}$  désigne  $\mathbb{R}$  ou  $\mathbb{C}$ ,  $n \in \mathbb{N}^*$  et  $(A, B) \in \mathcal{M}_n(\mathbb{K})^2$ . On fixe une norme d'algèbre  $\|\cdot\|$  sur  $\mathcal{M}_n(\mathbb{K})$ . On suppose connu et maîtrisé le calcul matriciel élémentaire.

**Théorème/Définition 1** ([R] 761). La série  $\sum_{k \in \mathbb{N}} \frac{A^k}{k!}$  converge normalement sur tout compact. Sa somme est appelée exponentielle de  $A$ , et est notée  $\exp(A)$  ou  $e^A$ .

**Exemple 2** ([R] 761).  $\forall (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$ ,  $\exp(\text{diag}(\lambda_1, \dots, \lambda_n)) = \text{diag}(e^{\lambda_1}, \dots, e^{\lambda_n})$ . En particulier,  $\exp(0_n) = I_n$  et  $\exp(I_n) = e \cdot I_n$ .

**Exemple 3.**  $\forall \theta \in \mathbb{R}$ ,  $R(\theta) := \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} = \exp\left(\begin{pmatrix} 0 & -\theta \\ \theta & 0 \end{pmatrix}\right)$

## I. Propriétés algébriques de l'exponentielle matricielle

**Proposition 4.** Si  $A$  et  $B$  commutent, alors  $\exp(A+B) = \exp(A)\exp(B)$ . (NB : la réciproque est vraie !) et  $\exp(A)$  et  $\exp(B)$  commutent.

**Contre-exemple 5.**  $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  et  $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$  ne commutent pas, et  $e^A e^B = \begin{pmatrix} e & e \\ 0 & 1/e \end{pmatrix} \neq \begin{pmatrix} e & 1/e \\ 0 & 1/e \end{pmatrix} = e^B e^A$ .

**Corollaire 6.**  $\exp(\mathcal{M}_n(\mathbb{K})) \subseteq GL_n(\mathbb{K})$ , et  $\exp(A)^{-1} = \exp(-A)$ .

**Proposition 7** ([R] 761-762). On a les propriétés suivantes :

- $\forall P \in GL_n(\mathbb{K})$ ,  $P \exp(A) P^{-1} = \exp(PAP^{-1})$
- ${}^t \exp(A) = \exp({}^t A)$
- $\det(\exp(A)) = e^{\text{tr}(A)}$
- $\overline{\exp(A)} = \exp(\overline{A})$

**Corollaire 8.**  $\exp(\mathcal{A}_n(\mathbb{K})) \subseteq O_n(\mathbb{K})$ , avec  $\mathcal{A}_n(\mathbb{K}) = \{M \in \mathcal{M}_n(\mathbb{K}) \mid {}^t M = -M\}$ .

**Remarque 9.** On peut montrer que  $\exp(\mathcal{A}_n(\mathbb{R})) = SO_n(\mathbb{R})$ .

**Proposition 10.** Si  $A$  est diagonalisable, alors  $\text{Sp}(\exp(A)) = \exp(\text{Sp}(A))$ .

**Théorème 11.** On a :

- $\exp(A) \in \mathbb{K}_{n-1}[A]$  et commute avec  $A$ .
- Si  $A$  est diagonalisable et  $\mathbb{K} = \mathbb{R}$ , alors  $A \in \mathbb{R}_{n-1}[\exp(A)]$ .

**Remarque 12.** Pour  $A = \begin{pmatrix} 0 & 0 \\ 0 & 2i\pi \end{pmatrix} \in \mathcal{M}_2(\mathbb{C})$ , on a  $\exp(A) = I_2$  donc pour tout  $P \in \mathbb{C}[X]$ ,  $P(\exp(A)) = P(1)I_2 \neq A$ .

## II. L'exponentielle d'une matrice en pratique

### A. Quelques méthodes de calcul

**Proposition 13.** Supposons  $A$  diagonalisable. Il existe  $(\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n$  et  $P \in O_n(\mathbb{K})$  tels

$$\text{que } A = P \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} P^{-1}; \text{ alors } \exp(A) = P \begin{pmatrix} e^{\lambda_1} & & \\ & \ddots & \\ & & e^{\lambda_n} \end{pmatrix} P^{-1}.$$

**Théorème 14** (décomposition de DUNFORD - [R] 613). Si  $A$  est trigonalisable, alors il existe un unique  $(D, N) \in \mathcal{M}_n(\mathbb{K})^2$  tel que  $D$  est diagonalisable,  $N$  est nilpotente,  $D$  et  $N$  commutent, et  $A = D + N$ . De plus,  $(D, N) \in K[A]^2$ .

**Proposition 15.** Si  $A$  est nilpotente d'indice  $r$ , alors  $\exp(A) = \sum_{k=0}^{r-1} \frac{A^k}{k!}$ .

**Proposition 16** ([R] 765). Si  $A$  est trigonalisable, et si  $A = D + N$  est la décomposition de DUNFORD de  $A$ , alors  $e^A = e^D + e^D(e^N - I_n)$ .

En particulier,  $e^D$  est diagonalisable et  $e^D(e^N - I_n)$  est nilpotente, et ce sont les éléments de la décomposition de DUNFORD de  $e^A$ .

**Proposition 17** ([R] 778).  $(I_n + \frac{A}{k})^k \rightarrow_{k \rightarrow +\infty} \exp(A)$

**Remarque 18.** Cela fournit une méthode pour approcher numériquement l'exponentielle d'une matrice, toutefois bien moins efficace qu'un calcul direct.

## B. Application : résolution d'EDO linéaires à coefficients constants

**Proposition 19** ([Gr] 378).  $t \mapsto e^{tA}$  est lisse sur  $\mathbb{R}$ , de dérivée  $t \mapsto Ae^{tA} = e^{tA}A$ .

**Proposition 20** ([Gr] e378). L'unique solution du problème de CAUCHY

$$\begin{cases} Y' = AY \\ Y(t_0) = Y_0 \end{cases}$$

pour  $t_0 \in \mathbb{R}$ ,  $Y \in \mathcal{M}_{n,1}(\mathbb{R})$ , est  $t \mapsto e^{(t-t_0)A}Y_0$ .

**Exemple 21.** Le problème de CAUCHY  $\begin{cases} Y' = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} Y, \quad Y(0) = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{cases}$  admet pour (unique) solution  $t \mapsto \exp\left(t \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right) \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e^t \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = e^t \begin{pmatrix} t \\ 1 \end{pmatrix}$ .

**Proposition 22** (formule de DUHAMEL). Soient  $B : \mathbb{R} \rightarrow \mathcal{M}_{n,1}\mathbb{R}$  continue,  $t_0 \in \mathbb{R}$  et  $Y_0 \in \mathcal{M}_{n,1}(\mathbb{R})$ . L'unique solution du problème de CAUCHY  $\begin{cases} Y' = AY + B; \quad Y(t_0) = Y_0 \end{cases}$  est

$$t \mapsto e^{(t-t_0)A}Y_0 + \int_{t_0}^t e^{(t-s)A}B(s)ds$$

## III. Propriétés analytiques de l'exponentielle matricielle

### A. Injectivité, surjectivité

**Théorème 23** ([R] 769). L'application  $\exp : \mathcal{M}_n(\mathbb{C}) \rightarrow GL_n(\mathbb{C})$  est surjective, non injective.

**Contre-exemple 24.**  $\forall k \in \mathbb{Z}, \exp(2i\pi k I_n) = I_n$

**Théorème 25.** *L'application  $\exp : \mathcal{M}_n(\mathbb{R}) \rightarrow GL_n(\mathbb{R})$  n'est ni surjective, ni injective. Plus précisément,*

- $\exp(\mathcal{M}_n(\mathbb{R})) = \{M^2 \mid M \in GL_n(\mathbb{R})\} \neq GL_n(\mathbb{R})$
- Exemple 3 justifie la non-injectivité

**Remarque 26.** Comme  $\det(\exp(A)) = e^{\text{tr}(A)} > 0$ , on a  $\det^{-1}(\mathbb{R}^+) \cap \exp(\mathcal{M}_n(\mathbb{R})) = \emptyset$ .

**Proposition 27** ([R] e768-777). Notons  $\mathcal{N}_n(\mathbb{R})$  l'ensemble des matrices nilpotentes de  $\mathcal{M}_n(\mathbb{R})$ . L'application  $\exp : \mathcal{N}_n(\mathbb{R}) \rightarrow GL_n(\mathbb{R})$  est injective.

Notons  $\Delta_n(\mathbb{R})$  l'ensemble des matrices diagonalisables de  $\mathcal{M}_n(\mathbb{R})$ . L'application  $\exp : \Delta_n(\mathbb{R}) \rightarrow GL_n(\mathbb{R})$  est injective.

**Application 28** ([R] 777).  $\exp(A)$  est diagonalisable si, et seulement si,  $A$  l'est.

**Théorème 29** ([C] 357). L'application  $\exp : S_n(\mathbb{R}) \rightarrow S_n^{++}(\mathbb{R})$  est un homéomorphisme.

**Théorème/Définition 30** ([R] 766-768). Si  $A \in \mathcal{B}(I_n, 1)$ , alors  $\sum_{n \geq 1} (-1)^{n-1} \frac{A^n}{n}$  converge normalement sur tout compact. Sa somme est notée  $\ln(I_n + A)$ , et est appelée logarithme de  $A$ .

**Remarque 31.** On a  $\ln(I_n) = 0_n$ .

**Théorème 32** (ADMIS). L'application  $\exp : \mathcal{N}_n(\mathbb{C}) \rightarrow I_n + \mathcal{N}_n(\mathbb{C})$  est une bijection de réciproque  $\ln$ .

## B. Régularité

**Théorème 33** (ADMIS - [Rv] 306).  $\exp$  est lisse sur  $\mathcal{M}_n(\mathbb{R})$ .

**Proposition 34.** La différentielle de  $\exp$  en  $X \in \mathcal{M}_n(\mathbb{R})$  est :

$$d(\exp)(X) : H \mapsto \left( \sum_{n=0}^{+\infty} \frac{[\cdot, X]^n}{(n+1)!} \right) (H)$$

où  $[\cdot, X] : H \mapsto [H, X] = HX - XH$ .

**Corollaire 35.**  $\exp$  induit un  $C^1$ -difféomorphisme local d'un voisinage de  $0_n$  sur un voisinage de  $I_n$ .

## Développements

- Développement 1 : Théorème 29
- Développement 2 : Proposition 34

## Références

- R *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition
- C *Nouvelles histoires hédonistes de groupes et géométries I*, P. Caldero, J. Germoni
- Gr *Algèbre linéaire*, Joseph Grifone, 6e édition, 2e version
- Rv *Petit guide du calcul différentiel*, François Rouvière, 4e édition



# 156 : Endomorphismes trigonalisables. Endomorphismes nilpotents.

## Développements

## Références

- Gr *Algèbre linéaire*, Joseph Grifone, 6e édition, 2e version
- M2 *Algèbre linéaire. Réduction des endomorphismes*, Roger Mansuy, Rached Mneimné, 3e édition
- R *Mathématiques pour l'agrégation - Algèbre et géométrie*, Jean-Étienne Rombaldi, 2e édition
- Go *Les maths en tête - Algèbre et probabilités*, Xavier Gourdon, 3e édition
- C *Carnet de voyage en Algèbre*, Philippe Caldero, Marie Peronnier