Algèbre linéaire MA122

Alexis Bouthier

Table des matières

Chapitre 1

Étude du groupe symétrique

1. Généralités sur les groupes

1.1. Groupes. Partant d'un ensemble, il s'agit de l'enrichir avec des structures supplémentaires, telles que des opérations.

Définition 1.1.1. Soit un ensemble E, une loi de composition interne (LCI) sur E est une fonction $* : E \times E \to E$. Cette loi est généralement notée entre deux éléments.

Exemple 1.1.2. Pour $(x, y) \in \mathbb{R}^2$, $(x, y) \mapsto x + y$ est une loi de composition interne. Si E est un ensemble non-vide et $\mathcal{P}(E)$ l'ensemble de ses parties, alors $(A, B) \mapsto A \cap B$ est une LCI sur $\mathcal{P}(E)$.

Définition 1.1.3. Soit $*$ une LCI sur E. On dit que $(E, *)$ est un monoïde si :

1. $\forall\ (x, y, z) \in E^3, (x * y) * z = x * (y * z)$ (Associativité).
2. $\exists\ e \in E, \forall\ x \in E, e * x = x * e = x$ (Existence d'un élément neutre).

Si pour toute paire $(x, y) \in E^2$, on a $x * y = y * x$, on dit que E est un monoïde commutatif ou abélien.

Remarque 1.1.4. L'utilité de l'associativité est qu'elle permet d'écrire $x * y * z$ sans se préoccuper du parenthésage. Toutes les lois de composition interne ne sont pas nécessairement associatives. La soustraction sur $\mathbb{R}$ est un exemple de loi non associative. $4 - (3 - 2) = 3 \neq (4 - 3) - 2 = -1$.

Exemple 1.1.5. $(\mathbb{N}, +)$ ou $(\mathbb{N}, \times)$ sont des monoïdes abéliens, $(M_n(\mathbb{R}), \times)$ est un monoïde non-commutatif.

Définition 1.1.6. Soit $*$ une LCI sur E. On dit que $(E, *)$ est un groupe si c'est un monoïde et qu'il vérifie :

$$\forall\ x \in E, \exists\ y \in E, xy = yx = e \text{(Existence d'un inverse).}$$

C'est un groupe abélien si de plus $(E, *)$ est un monoïde abélien.

Exemple 1.1.7. $(\mathbb{Z}, +)$ est un groupe abélien, $(GL_n(\mathbb{R}), \times)$ est un groupe non-commutatif.

Lemme 1.1.8. *Soit $(E, *)$ un ensemble avec une LCI, si elle admet un élément neutre, alors il est unique. De plus, si $(E, *)$ est un groupe, alors il y a unicité de l'inverse.*

Démonstration. En effet, si e et e' sont deux éléments neutres, on a $e * e' = e$ et $e * e' = e'$. Pour la deuxième assertion, soit $x \in E$, supposons qu'il admette deux inverses $y, y' \in E$. On a alors :

$$y = y(xy') = y'.$$

□

Ainsi, si $(E, *)$ est un groupe, pour tout $x \in E$, il résulte du lemme que l'on peut définir x^{-1}, l'inverse de x. On note immédiatement que pour toute paire $(x, y) \in E^2$:

$$(x * y)^{-1} = y^{-1} * x^{-1}$$

Dans la suite, on note la LCI de manière multiplicative, sauf mention explicite et l'élément neutre 1. Pour $n \in \mathbb{N}^*$, si l'on multiplie n fois x, on note x^n. Attention, en général :

$$(xy)^n \neq x^n y^n.$$

C'est vrai seulement si la loi est commutative (pensez aux matrices). En effet, on a :

$$x^2y^2 = xxyy \text{ et } (xy)^2 = xyxy.$$

1.2. Sous-groupes. On se donne dans la suite $(G, .)$ un groupe.

Définition 1.2.1. Une partie non-vide H de G est un sous- groupe si :

$$\forall\ (x, y) \in H^2, xy^{-1} \in H.$$

Remarques.

1.2.2. On remarque que comme H est non-vide, on a automatiquement $1 \in H$. En effet, il suffit de choisir $x \in H$ et par hypothèse, on a $1 = x.x^{-1} \in H$.

1.2.3. Dans les applications, pour montrer que quelque chose est un groupe, il est souvent plus commode de montrer que c'est un sous-groupe d'un groupe de « référence ».

Exemple 1.2.4. $(\mathbb{Q}^*, \times)$ est un sous-groupe de $(\mathbb{R}^*, \times)$, $\mathbb{U}_n := \{z \in \mathbb{C} \mid z^n = 1\}$ est un sous-groupe de $(\mathbb{C}^*, \times)$.

1.3. Morphismes de groupes. Soient $(A, .)$ et $(B, .)$ deux groupes.

Un morphisme de groupes est une fonction entre groupes $f : A \to B$ telle que :

$$f(1_A) = 1_B, f(xy) = f(x)f(y).$$

Remarque 1.3.1. On a automatiquement $f(x)f(x^{-1}) = f(xx^{-1}) = 1$ soit $f(x^{-1}) = f(x)^{-1}$.

Exemple 1.3.2. $z \mapsto |z|$ de $(\mathbb{C}^*, .) \to (\mathbb{R}^*, .)$ ou $x \mapsto e^x$ de $(\mathbb{R}, +)$ sur $(\mathbb{R}^*, .)$ sont des morphismes de groupes.

Vocabulaire usuel sur les morphismes :

Définition 1.3.3. Soit $f : G \to H$, un morphisme de groupes. On dit que :

1. f est un *endomorphisme* si $G = H$.
2. f est un *isomorphisme* si c'est un morphisme de groupes bijectif.
3. f est un *automorphisme* si c'est un endomorphisme bijectif.

Exemples.

1.3.4. $x \mapsto x^2$ est un endomorphisme de groupes de $(\mathbb{R}^*, \times)$.

1.3.5. $x \mapsto e^x$ est une bijection de $(\mathbb{R}, +)$ sur $(\mathbb{R}_+^*, \times)$. On dit que ces groupes sont isomorphes.

aut-int

Exemple 1.3.6. Pour un groupe G et $x \in G$, $\phi_x : G \to G$ donné par $y \mapsto xyx^{-1}$ est un automorphisme de G. On appelle un tel automorphisme, un automorphisme intérieur. Si $x = 1$, on obtient l'automorphisme identité Id_G donné par $y \mapsto y$.

Exemple 1.3.7. Soit G un groupe, alors l'ensemble $\mathrm{Aut}(G)$ des automorphismes de G avec la composition des applications comme LCI est un groupe.

Démonstration. La loi de composition est clairement associative et pour tout $\sigma \in \mathrm{Aut}(G)$, on a $\mathrm{Id}_G \circ \sigma = \sigma \circ \mathrm{Id}_G = \sigma$. De plus comme σ est bijective, soit σ^{-1} son inverse, alors on a bien $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{Id}$. Il suffit donc de vérifier que σ^{-1} est aussi un morphisme de groupes. On a $\sigma(1) = 1$ donc $\sigma^{-1}(1) = 1$. Soit $(x, y) \in G^2$, alors $\sigma(\sigma^{-1}(x)\sigma^{-1}(y)) = \sigma(\sigma^{-1}(x))\sigma(\sigma^{-1}(y)) = xy = \sigma(\sigma^{-1}(xy))$, soit $\sigma^{-1}(x)\sigma^{-1}(y) = \sigma^{-1}(xy)$ par injectivité de σ. □

1.4. Image et noyau d'un morphisme. Soit $\phi : G \to H$ un morphisme de groupes.

Lemme 1.4.1. *Soient $G' \subset G$, $H' \subset H$ des sous-groupes, alors $\phi(G')$ et $\phi^{-1}(H')$ sont aussi des sous-groupes.*

Démonstration. $e \in G'$ comme G' est un sous-groupe et $\phi(e) = e' \in \phi(G')$. De plus, $\phi(x)\phi(y)^{-1} = \phi(xy^{-1})$ et $xy^{-1} \in G'$ donc $\phi(G')$ est un sous-groupe. On a l'équivalence :

$$x \in \phi^{-1}(H') \iff \phi(x) \in H'.$$

Comme $\phi(1) = 1 \in H'$, $1 \in \phi^{-1}(H')$. Si $x, y \in \phi^{-1}(H')$, alors $\phi(x)\phi(y)^{-1} \in H'$. Or $\phi(x)\phi(y)^{-1} = \phi(xy^{-1})$, donc on obtient $xy^{-1} \in \phi^{-1}(H')$, ce qui conclut. □

Définition 1.4.2. **1.** On définit l'image de ϕ, notée $\operatorname{Im}\phi$ par le sous-groupe $\phi(G) \subset H$. On a $\operatorname{Im}\phi = H$ si et seulement si ϕ est surjective.

2. On définit le noyau de ϕ, noté $\operatorname{Ker}\phi$, par le sous-groupe $\phi^{-1}(\{e\}) \subset G$.

Exemple 1.4.3.

$\phi : \mathbb{C} \to \mathbb{R}$, donné par $z \mapsto \operatorname{Re}(z)$ est surjectif, donc $\operatorname{Im}\phi = \mathbb{R}$. De plus, $\operatorname{Ker}\phi = i\mathbb{R}$.

$\phi : (\mathbb{R}, +) \to (\mathbb{U}, \times)$, donné par $x \mapsto e^{ix}$ est surjectif de noyau $2\pi\mathbb{Z}$.

Proposition 1.4.6. *Soit $\phi : G \to H$ un morphisme de groupes. Alors, ϕ est injectif si et seulement si* $\operatorname{Ker}\phi = \{1\}$.

Démonstration. Sens direct : soit $x \in G$ tel que $\phi(x) = 1$ alors $\phi(x) = \phi(1)$ et $x = 1$.

Sens réciproque : Si pour $(x, x') \in G^2$, on a $\phi(x) = \phi(x')$, alors $\phi(x)\phi(x')^{-1} = 1$, d'où $\phi(xx'^{-1}) = 1$. Comme $\operatorname{Ker}\phi = \{1\}$, on obtient $xx'^{-1} = 1$ et $x = x'$. □

Proposition 1.4.7. *Soit $\phi : G \to H$ un morphisme de groupes finis de même cardinal, alors on a l'équivalence :*

$$\phi \text{ injective} \iff \phi \text{ surjective} \iff \phi \text{ bijective.}$$

Démonstration. On montre (1) $\implies$ (2) $\implies$ (3) $\implies$ (1). Si ϕ est injective, $\operatorname{card}(G) = \operatorname{card}(\phi(G)) = \operatorname{card}(H)$ donc $\phi(G) = H$ et ϕ est surjective. Si ϕ est surjective, alors $\phi(G) = H$ et si ϕ n'est pas injective, on aurait $\operatorname{card}(H) = \operatorname{card}\phi(G) < \operatorname{card} G$, donc ϕ est injective donc bijective. La dernière assertion est triviale. □

fin **Lemme 1.4.8.** *Soit G un groupe fini, alors pour tout $x \in G$, il existe $n \in \mathbb{N}^*$, $x^n = 1$.*

Démonstration. En effet si tel n'est pas le cas alors on obtiendrait un morphisme de groupes injectif :

$$\mathbb{Z} \to G$$

donné par $k \mapsto x^k$. Or, G est fini, contradiction. □

2. L'exemple du groupe symétrique

Proposition 2.0.1. *Soit un ensemble E, on note* $\operatorname{Bij}(E)$ *l'ensemble des bijections de E, alors* $(\operatorname{Bij}(E), \circ)$*, muni de la composition des fonctions est un groupe.*

Démonstration. On a clairement que Id_E est l'élément neutre, la loi est clairement associative et pour $\sigma \in \operatorname{Bij}(E)$, sa fonction réciproque σ^{-1} est l'inverse pour la composition. Ainsi, $\operatorname{Bij}(E)$ est bien un groupe. □

Soit $n \in \mathbb{N}^*$, on définit alors $S_n = \mathrm{Bij}(\llbracket 1, n \rrbracket)$ que l'on munit de la composition des fonctions et on l'appelle le groupe symétrique à n éléments.

Lemme 2.0.2. *Pour tout $n \in \mathbb{N}^*$, on a $\mathrm{card}(S_n) = n!$.*

Démonstration. Pour compter les éléments de S_n, il suffit de voir comment une telle permutation. Pour $\sigma(1)$, il y a n choix, $\sigma(2)$ (n-1) choix, comme σ doit être injective, jusqu'à $\sigma(n)$ où il ne reste plus qu'un seul élément, en faisant le produit, on obtient $\mathrm{card}(S_n) = n!$. □

Définition 2.0.3. Pour $1 \leqslant k \leqslant n$, on note $(a_1, \ldots, a_k) \in S_n$ la permutation σ donnée par $\sigma(a_i) = a_{i+1}$ pour $1 \leqslant i \leqslant k-1$, $\sigma(a_k) = a_1$ et qui fixe tout élément $y \notin \{a_1, \ldots, a_k\}$. On appelle une telle permutation un cycle de longeur k ou k-cycle et l'ensemble $\{a_1, \ldots, a_k\}$ est appelé le support du cycle. Si $k = 2$, on parle de transposition. On note que l'on a $\sigma^k = 1$.

commut **Lemme 2.0.4.** *Soient $\sigma, \sigma' \in S_n$ des cycles à supports disjoints, alors ils commutent.*

Démonstration. Soient $\sigma = (a_1, \ldots, a_k)$ et $\sigma' = (b_1, \ldots, b_r)$. Si $x \notin \{a_1, \ldots a_k\} \cup \{b_1, \ldots, b_r\}$, on a $\sigma(x) = \sigma'(x) = x$. Si $x \in \{a_1, \ldots a_k\}$, $\sigma'(x) = x$ et $\sigma(x) \in \{a_1, \ldots a_k\}$ donc $\sigma\sigma'(x) = \sigma'\sigma(x)$ et pareillement pour $x \in \{b_1, \ldots, b_r\}$. On obtient ainsi que $\sigma\sigma' = \sigma'\sigma$ comme souhaité. □

plog **Lemme 2.0.5.** *Soit un sous-ensemble non-vide $F \subset \llbracket 1, n \rrbracket$, alors on a un morphisme injectif canonique :*

$$\Phi : \mathrm{Bij}(F) \to S_n.$$

De plus, si $p = \mathrm{card}(F)$, alors on a $\mathrm{Bij}(F) \simeq S_p$.

Démonstration. Pour $\sigma \in \mathrm{Bij}(F)$, il suffit de poser $\Phi(\sigma)$ telle que $\Phi(\sigma)_{|F} = \sigma$ et $\Phi(\sigma)_{|\overline{F}} = \mathrm{Id}_{|F}$. On a immédiatement que $\Phi(\sigma) \in S_n$ et que Φ est injective. Enfin, on a bien :

$$\Phi(\sigma) \circ \Phi(\sigma') = \Phi(\sigma\sigma'),$$

puisqu'il suffit de vérifier l'égalité en restreignant respectivement à F et à $\overline{F}$, où l'égalité devient tautologique. □

Le premier théorème de structure sur les permutations est le suivant :

cycle **Théorème 2.0.6.** *Toute permutation $\sigma \in S_n$ est un produit $\sigma = \sigma_1 \ldots \sigma_r$ de cycles à supports disjoints. Si chaque σ_i est de longueur k_i, on parle de $k_1 \times \cdots \times k_r$-cycle.*

Démonstration. On procède par récurrence forte sur n. Si $n = 1$, c'est clair, supposons $n \geqslant 2$, supposons la propriété vraie pour tout $k \leqslant n-1$. Soit $\sigma \in S_n$, si $\sigma(1) = 1$, alors comme σ est bijective, on a $\sigma(\llbracket 2, n \rrbracket) = \llbracket 2, n \rrbracket$, de telle sorte que $\sigma_1 = \sigma_{|\llbracket 2,n \rrbracket}$ induit une

permutation de $\mathrm{Bij}(\llbracket 2, n\rrbracket) \simeq S_{n-1}$, on applique alors la récurrence à σ_1 et $\sigma = \sigma_1$ est bien produit de cycles à supports disjoints où l'on voit σ_1 comme une permutation de S_n via le plongement 2.0.5 :

$$S_{n-1} \to S_n.$$

Si $\sigma(1) \neq 1$, d'après 1.4.8, il existe $\ell \in \mathbb{N}^*$ tel que $\sigma^\ell = \mathrm{Id}$, en particulier, soit $i_1 \in \mathbb{N}^*$ le plus petit entier tel $\sigma^{i_1}(1) = 1$. On définit alors $\sigma_1 = (1, \sigma(1), \ldots, \sigma^{i_1-1}(1))$. Appelons F_1 le support de σ_1, on a alors une décomposition en somme disjointe :

$$\llbracket 1, n\rrbracket = F_1 \coprod \overline{F_1}.$$

de telle sorte que σ stabilise F_1 et son complémentaire [1]. Comme σ injective, on obtient donc que $\sigma' = \sigma_{|\overline{F_1}} \in \mathrm{Bij}(\overline{F_1})$ et on applique l'hypothèse de récurrence à σ' et on a alors $\sigma = \sigma_1\sigma'$ où l'on voit σ' comme un élément de S_n via 2.0.5.

□

unik **Proposition 2.0.7.** *La décomposition est unique à permutation des facteurs près.*

Démonstration. On écrit deux telles compositions $\sigma = \sigma_1 \ldots \sigma_r = \sigma'_1 \ldots \sigma'_s$. Soit $i \in \mathrm{supp}(\sigma_1)$, alors $\sigma_1(i) \neq i$ et il existe t tel que $i \in \mathrm{supp}(\sigma'_t)$. Or comme les deux sont des cycles, on a $\mathrm{supp}(\sigma_1) = \{\sigma^k(i), k \in \mathbb{Z}\} = \mathrm{supp}(\sigma'_t)$ et $\sigma_1 = \sigma'_t$ que l'on peut donc simplifier des deux côtés en itérant, on trouve alors $r = s$ et $\sigma_i = \sigma'_i$ quitte à réordonner, d'où l'unicité. □

trans **Théorème 2.0.8.** *Le groupe S_n est engendré par les transpositions. De plus, il est même engendré par les transpositions $(1i)$ pour $i \in \llbracket 1, n\rrbracket$.*

Remarque 2.0.9. On prendra garde au fait que dans la décomposition en produit de transpositions, les transpositions ne commutent pas entre elles et il n'y a pas unicité de la décomposition à permutation des facteurs près.

Démonstration. D'après 2.0.6, il suffit donc de montrer qu'un cycle est un produit de transpositions et l'on vérifie immédiatement que :

$$(a_1, \ldots, a_k) = (a_1a_2)(a_2a_3)\ldots(a_{k-1}a_k). \tag{2.0.9.1}$$ {tprod}

Enfin, on a $(ij) = (1i)(1j)(1i)$ ce qui conclut. □

1. Si $x \notin F_1$ tel que $\sigma(x) \in F_1$, alors $\sigma(x) = \sigma^r(1)$ pour un $r \in \mathbb{N}$, soit $\sigma^{r-1}(1) = x$ et $x \in F_1$, absurde

2.1. Signature et groupe alterné. Soit $n \in \mathbb{N}^*$, pour $\sigma \in S_n$ et $f(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n]$, on fait agir S_n sur $\mathbb{Z}[X_1, \dots, X_n]$ par :

$$\sigma.P = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

.

Pour $\sigma, \tau \in S_n$, on a :

$$\sigma.(\tau.f) = \sigma.f(X_{\tau(1)}, \dots, X_{\tau(n)}) = f(X_{\sigma\circ\tau(1)}, \dots, X_{\sigma\circ\tau(n)}) = (\sigma\tau).f \qquad (2.1.0.2)$$

{scomp}

De plus pour $P, Q \in \mathbb{Z}[X_1, \dots, X_n]$ et $\lambda \in \mathbb{Z}$, on a immédiatement que l'action est linéaire :

$$\sigma.(P + \lambda Q) = \sigma.P + \lambda\sigma.Q$$

et compatible avec le produit [2] :

$$\sigma.(PQ) = (\sigma.P)(\sigma Q).$$

On considère alors la différente :

$$\Delta = \prod_{1 \leqslant i < j \leqslant n} (X_i - X_j)$$

sign

Théorème 2.1.1. *Pour tout $\sigma \in S_n$, on a $\sigma.\Delta = \epsilon(\sigma)\Delta$ avec $\epsilon(\sigma) \in \{\pm 1\}$. L'application $\epsilon : S_n \to \mathbb{Z}/2\mathbb{Z}$ est alors un morphisme de groupes, que l'on appelle la signature.*

Démonstration. On considère la transposition $\tau = (rs)$ avec $1 \leqslant r < s \leqslant n$. Calculons $\tau.\Delta$, on a :

$$\tau.\Delta = \prod_{1 \leqslant i < j \leqslant n} (X_{\tau(i)} - X_{\tau(j)}) = \prod_{1 \leqslant i < j \leqslant n} \tau.(X_i - X_j).$$

On a déjà que $\tau(X_r - X_s) = -(X_s - X_r)$. Si un facteur ne contient pas X_r ou X_s dedans, alors il est inchangé. Pour les autres facteurs, on les regroupe par paires :

$$(X_k - X_s)(X_k - X_r) \text{ si } k > s,$$
$$(X_k - X_s)(X_k - X_r) \text{ si } r < k < s,$$
$$(X_k - X_s)(X_k - X_r) \text{ si } k < r.$$

Chacun de ces facteurs sont inchangés lorsque l'on applique τ, on en déduit donc que :

$$\tau.\Delta = -\Delta.$$

Ainsi, comme S_n est engendré par les tranpositions d'après 2.0.8, on obtient que $\sigma.\Delta = \pm\Delta$ et on définit $\epsilon(\sigma) \in \{\pm 1\}$ tel que :

$$\sigma.\Delta = \epsilon(\sigma)\Delta.$$

On a immédiatement que $\epsilon(\mathrm{Id}) = 1$ et montrons que l'on obtient un morphisme de groupes, on a la suite d'égalités en utilisant (2.1.0.2) et la linéarité de l'action :

$$\epsilon(\sigma\sigma')\Delta = (\sigma\sigma'.\Delta) = \sigma.(\sigma'\Delta) = \sigma(\epsilon(\sigma')\Delta) = \epsilon(\sigma')\sigma.\Delta = \epsilon(\sigma)\epsilon(\sigma')\Delta.$$

2. $PQ(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)})Q(X_{\sigma(1)}, \dots, X_{\sigma(n)})$.

et on obtient un morphisme de groupes $\epsilon : S_n \to \mathbb{Z}/2\mathbb{Z}$. □

cal-sign **Corollaire 2.1.2.** *Pour toute transposition, on a $\epsilon(\tau) = -1$ et pour tout r-cycle σ, on a $\epsilon(\sigma) = (-1)^{r-1}$.*

DÉMONSTRATION. La preuve précédente donne déjà que $\epsilon(\tau) = -1$. Enfin, si $\sigma = (a_1, \ldots, a_k)$, d'après (2.0.9.1), c'est le produit de $r - 1$ transpositions. □

Chapitre 2

Déterminants

1. Rappels sur les espaces vectoriels

1.1. Anneaux.

Définition 1.1.1. Soit $(A, +, .)$ un ensemble muni de deux LCI, on dit que A est un anneau si :

1. $(A, +)$ est un groupe abélien.

2. $(A, .)$ est un monoïde.

3. $\forall\ (x, y, z) \in A^3$, on a $x.(y + z) = x.y + x.z$ et $(x + y).z = x.z + y.z$ (distributivité) .

Enfin, A est un anneau commutatif, si $(A, .)$ est un monoïde commutatif.

Exemple 1.1.2. $(\mathbb{Z}, +, \times)$, $(\mathbb{C}, +, \times)$ sont des anneaux commutatifs, $(M_n(\mathbb{R}), +, \times)$ est un anneau non-commutatif. Si A et A' sont deux anneaux alors le produit direct de $A \times A'$ est aussi un anneau en faisant les opérations composantes par composantes. Pour un anneau A, on a l'anneau des polynômes à coefficients dans A :

$$A[X] = \{\sum_{d=0}^{n} a_d X^d, n \in \mathbb{N}, a_i \in A\},$$

avec l'addition et la multiplication habituelle des polynômes. Plus généralement on dispose de l'anneau $A[X_1, \ldots, X_r]$ en r indéterminées, qui consiste en les expressions de la forme $\sum_{\underline{i} \in \mathbb{N}^r} a_{\underline{i}} X_1^{i_1} \ldots X_r^{i_r}$ avec les $a_{\underline{i}}$ presque tous nuls.

Définition 1.1.3. Un sous-anneau B de A vérifie :

— $(B, +)$ est un sous-groupe de $(A, +)$.

— $(B, \times)$ est un sous-monoïde de $(A, \times)$.

Un morphisme d'anneaux est une fonction entre anneaux $f : A \to B$ telle que :

— $f : (A, +) \to (B, +)$ est un morphisme de groupes.

— $f : (A, \times) \to (B, \times)$ est un morphisme de monoïdes.

Exemple 1.1.4. Le morphisme ev : $\mathcal{F}(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$ donné par $f \mapsto f(0)$ est un morphisme d'anneaux.

1.2. Groupes des inversibles et Corps. Soit un anneau $(A, +, \times)$. Tout élément $x \in A$ n'est pas nécessairement inversible.

inv-ring **Lemme 1.2.1.** *Soit $(A^\times, \times)$ l'ensemble des éléments inversibles pour $\times$, alors c'est un groupe. On l'appelle le groupe des inversibles.*

Démonstration. $(A^\times, \times)$ est un sous-monoïde de $(A, \times)$ et par définition tout élément est inversible. □

Exemple 1.2.2. $\mathbb{Z}^\times = \{\pm 1\}, \mathbb{Q}^\times = \mathbb{Q}^*$. Si p premier, alors $(\mathbb{Z}/p^m\mathbb{Z})^\times = \{x \in \mathbb{Z}/p\mathbb{Z} \mid x \neq 0[p]\}$.

Définition 1.2.3. Soit un anneau A, on dit que c'est un corps s'il est non-réduit à $\{0\}$ et si tout élément non-nul est inversible. Un sous-corps est un sous-anneau qui est un corps. Un morphisme de corps est un morphisme d'anneaux entre corps.

Remarque 1.2.4. Dans ce cours, on ne considèrera que des corps commutatifs, i.e. tels que A soit un anneau commutatif.

Exemple 1.2.5. Les ensembles $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ pour p premier, sont des corps. Si $\mathbb{K}$ est un corps, $\mathbb{K}(X)$ qui consiste en les fractions rationnelles à coefficients dans $\mathbb{K}$ est aussi un corps.

1.3. Espaces vectoriels. On rappelle la définition suivante.

Définition 1.3.1. Soit $\mathbb{K}$ un corps. On appelle $\mathbb{K}$-espace vectoriel un ensemble E, muni d'une LCI $+$ telle que :

(i) $(E, +)$ est un groupe abélien.

(ii) Il existe une application $. : \mathbb{K} \times E \to E$, appelée loi externe telle que :

(a) $\forall\ x \in E, 1.x = x$.

(b) $\forall\ (\lambda, \mu) \in \mathbb{K}^2, x \in E, (\lambda.\mu).x = \lambda.(\mu.x)$.

(c) $\forall\ (\lambda, \mu) \in \mathbb{K}^2, (x, y) \in E^2, (\lambda + \mu).(x + y) = \lambda.x + \mu.x + \lambda.y + \mu.y$.

Remarques.

1.3.2. Nous n'allons pas refaire toutes les définitions qui sont déjà connues. On a surtout rappelé celle-ci pour bien mettre l'accent que l'on travaille avec $\mathbb{K}$ un corps arbitraire et pas seulement $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

1.3.3. Ces données peuvent être rassemblées en une seule. Si l'on note $\mathrm{End}(E)$ l'anneau des endomorphismes de groupes abéliens de E, muni de l'adddition et de la composition des endomorphismes, alors la donnée d'une structure de $\mathbb{K}$-espace vectoriel revient à la donnée d'un morphisme d'anneaux $\phi : A \to \mathrm{End}(M)$, donné par $a \mapsto \phi_a$ où $\phi_a : E \to E$ est donnée par $x \mapsto a.x$.

On a ensuite les notions usuelles de sous-epaces vectoriels, morphisme d'espaces vectoriels, qui sont précisément les applications linéaires, et de noyau et d'image d'applications linéaires. On va juste introduire deux notions de base supplémentaires.

1.4. Adjoint d'un endomorphisme. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, soit $E^\vee = \mathrm{Hom}(E, \mathbb{K})$ son dual, on a $dim(E) = \dim(E^\vee)$, mais en général ces deux espaces vectoriels ne sont pas canoniquement isomorphes et il n'y a pas de flèche canonique $E \to E^\vee$. En revanche on a un accouplement canonique :

$$\forall\ x \in E, f \in E^\vee, \langle x, f\rangle = f(x).$$

On a également une flèche canonique :

$$\Phi : \mathrm{End}(E) \to \mathrm{End}(E^\vee)$$

donnée par $u \mapsto {}^t u : E^\vee \to E^\vee$ où ${}^t u(f) = f \circ u$. On appelle ${}^t u$ l'adjoint de u. Par construction, on a l'égalité suivante :

$$\forall\ x \in E, f \in E^\vee, \langle u(x), f\rangle = \left\langle x, {}^t u(f)\right\rangle.$$

Proposition 1.4.1. *La flèche Φ est un isomorphisme.*

Démonstration. Il suffit de montrer l'injectivité, puisque les espaces ont même dimension. Soit $u \in \mathrm{End}(E)$, tel que ${}^t u = 0$. Soit $B = (e_1, \ldots, e_n)$ une base de E, $(e_1^*, \ldots, e_n^*)$ la base duale, (u_{ij}) les coefficients de la matrice de u dans B, alors on a par hypothèse :

$$\forall\ i \in [\![1, n]\!], 0 = {}^t u(e_i^*) = e_i^* u = 0,$$

d'où l'on déduit pour tout $1 \leqslant i, k \leqslant n$, $e_i^* u(e_k) = u_{ik} = 0$ et $u = 0$. □

Si on prend $E = \mathbb{K}^n$, alors dans ce cas on a un isomorphisme canonique :

$$\psi : E \to E^\vee$$

qui à $x = (x_1, \ldots, x_n)$ associe la forme linéaire $\phi_x : \mathbb{K}^n \to \mathbb{K}$ donnée par $\phi_x(y) = \sum_{i=1}^{n} x_i y_i$. Ainsi, l'isomorphisme composé :

$$M_n(\mathbb{K}) \to \mathrm{End}(E) \xrightarrow{\Phi} \mathrm{End}(E^\vee) \xrightarrow{\psi} \mathrm{End}(E) = M_n(\mathbb{K})$$

n'est autre que la transposition des matrices $M \mapsto {}^t M$.

1.5. Orthogonal d'un espace vectoriel. Soit E un $\mathbb{K}$ espace vectoriel.

Définition 1.5.1. Des éléments $x \in E$, $\phi \in E^\vee$ sont dits orthogonaux si $\phi(x) = \langle x, \phi\rangle = 0$.

- Si $A \subset E$, on désigne par $A^\perp := \{\phi \in E^\vee, \forall\ x \in A, \phi(x) = 0\}$. L'ensemble $A^\perp$ est un sous-espace vectoriel de $E^\vee$, appelé l'orthogonal de A.
- Si $B \subset E^\vee$, on désigne par $B^\circ := \{x \in E, \forall\ \phi \in B, \phi(x) = 0\}$. L'ensemble B° est un sous-espace vectoriel de E, appelé l'orthogonal de B.

Remarque 1.5.2. Si $\phi \in E^\vee$, alors on a $\{\phi\}^\circ = \mathrm{Ker}(\phi)$.

On a les propriétés aisées suivantes, laissées en exercice :

Lemme 1.5.3. — *Si $A_1 \subset A_2 \subset E$, alors $A_2^\perp \subset A_1^\perp$.*

— *Si $B_1 \subset B_2 \subset E^\vee$, alors $B_2^\circ \subset B_1^\circ$.*

— *Si $A \subset E$, alors $A^\perp = (\mathrm{Vect}\, A)^\perp$.*

— *Si $B \subset E^\vee$, $B^\circ = (\mathrm{Vect}(B))^\circ$.*

Le théorème clé qui nous intéresse est le suivant :

perp1 **Théorème 1.5.4.** *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, $F \subset E$ et $H \subset E^\vee$ des sous-espaces vectoriels, alors on a :*

(i) $\dim(F) + \dim(F^\perp) = \dim(E)$ *et* $(F^\perp)^\circ = F$.

(ii) $\dim(H) + \dim(H^\circ) = \dim(E)$ *et* $(G^\circ)^\perp = G$.

Démonstration. (i) Soit $r = \dim(F)$ et $(e_1, \dots, e_r)$ une base de F complétée en une base $(e_1, \dots, e_n)$ de E. On a $F = \mathrm{Vect}(e_1, \dots, e_r)$ donc d'après la proposition précédente $F^\perp = \{e_1, \dots, e_r\}^\perp$. Soit $\phi \in E^\vee$, $\phi = \sum \lambda_i e_i^*$, alors :

$$\phi \in \{e_1, \dots, e_r\}^\perp \Longleftrightarrow \forall i \in [\![1, r]\!], 0 = \phi(e_i) = \lambda_i,$$

Ainsi $\phi \in F^\perp$ si et seulement si $\phi \in \mathrm{Vect}(e_{r+1}^*, \dots, e_n^*)$, d'où la première égalité et $F^\perp = \mathrm{Vect}(e_{r+1}^*, \dots, e_n^*)$. Maintenant, on a :

$$x = \sum a_i e_i \in (F^\perp)^\circ \Longleftrightarrow \forall i \in [\![r+1, n]\!], 0 = e_i^*(x) = a_i,$$

ce qui montre que $(F^\perp)^\circ = F$.

(ii) Soit $r = \dim G$, $(f_1, \dots, f_r)$ une base de G complétée en une base $(f_1, \dots, f_n)$ de $E^\vee$. Soit $(e_1, \dots, e_n)$ une base antéduale de telle sorte que pour tout i, $f_i = e_i^*$, on a $G = \mathrm{Vect}(e_1^*, \dots, e_r^*)$ et en procédant comme ci-dessus, on trouve $G^\circ = \mathrm{Vect}(e_{r+1}, \dots, e_n)$ et $(G^\circ)^\perp = G$. □

Remarque 1.5.7. Si on est en dimension infinie, on a toujours $(F^\perp)^\circ = F$. En revanche, on n'a pas toujours en général $(G^\circ)^\perp = G$. Prenons $E = \mathbb{R}[X]$, B le sous-espace vectoriel de $E^\vee$ engendré par les formes linéaires $\phi_n : P \mapsto P^{(n)}(0)$. Si $P \in B^\circ$, alors pour tout $n \in \mathbb{N}$, on a $P^{(n)}(0) = 0$, donc $P = 0$. Ainsi $B^\circ = \{0\}$ et $(B^\circ)^\perp = E^\vee$ et $B \neq (B^\circ)^\perp$ (la forme linéaire $\phi : P \mapsto P(1)$ n'est pas dans B). En revanche, on atoujours l'inclusion $B \subset (B^\circ)^\perp$.

2. Formes n-linéaires alternées

Soit $\mathbb{K}$ un corps, $E_1, \dots, E_r$, F, $r+1$ $\mathbb{K}$-espaces vectoriels. Un *application r-linéaire* est une application $f : E_1 \times \cdots \times E_r \to F$, r-linéaire en chacun des arguments, autrement dit pour tout $1 \leqslant i \leqslant r$ et pour tout $(r-1)$-uplet $(a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n) \in E_1 \times E_{i-1} \times E_{i+1} \times \cdots \times E_r$, l'application partielle de E_i dans F :

$$x_i \mapsto (a_1, \dots, a_{i-1}, x_i, a_{i+1}, \dots, a_n)$$

est une application linéaire.

Une application r-linéaire de $E_1 \times \cdots \times E_r$ dans $\mathbb{K}$ est appelée une *forme r-linéaire.*

Considérons le cas où tous les E_i sont égaux une application r-linéaire $f : E^r \to F$ est dite *alternée* si $f(x_1, \dots, x_r) = 0$ s'il existe deux indices $i < j$ tels que $x_i = x_j$. On déduit aussitôt de cette définition que l'on a pour tout $(x_1, \dots, x_n) \in E^r$:

$$f(x_1, \dots, x_{i-1}, x_i + x_j, x_{i+1}, \dots, x_{j-1}, x_i + x_j, x_{j+1}, \dots, x_r) = 0,$$

soit :

$$f(x_1, \dots, x_i, \dots, x_j, \dots, x_r) + f(x_1, \dots, x_j, \dots, x_i, \dots, x_r) = 0.$$

Ainsi, quand on échange deux des arguments x_i dans f, la valeur de f change de signe. Comme toute permutation $\sigma \in S_n$ est un produit de transpositions, on obtient donc que :

$$f(x_{\sigma(1)}, \dots, x_{\sigma(r)}) = \epsilon(\sigma) f(x_1, \dots, x_r). \tag{2.0.0.1}$$ {permu}

i-alt **Proposition 2.0.1.** *Pour E un $\mathbb{K}$-espace vectoriel de dimension n, soit $i \in \mathbb{N}^*$, on note $\Lambda^i E^\vee$ l'espace vectoriel des i-formes alternées. Alors, on a $\dim \Lambda^i E^\vee = \binom{n}{i}$, en particulier $\dim \Lambda^n E^\vee = 1$.*

Démonstration. Soit $i \in \mathbb{N}^*$, $f \in \Lambda^i E^\vee$ et $(e_1, \dots, e_n)$ une base de E. Par i-linéarité, f est déterminée par son image sur les i-uplets $(e_{l_1}, \dots, e_{l_i})$.

Si $i > n$, alors obligatoirement, dans un tel i-uplet, on retrouve au moins deux fois le même vecteur, donc comme f est alternée, $f = 0$ sur tous ces i-uplets et alors $\Lambda^i E^\vee = \{0\}$.

Si $i \leqslant n$, alors à nouveau comme f est alternée, elle est déterminée par les $(e_{l_1}, \dots, e_{l_i})$ avec les l_k tous distincts. De plus, il résulte de (2.0.0.1) que f prend la même valeur à plus ou moins un près si l'on fait une permutation des vecteurs du i-uplet. Pour compter le nombre de tels i-uplets, cela revient donc à choisir i éléments parmi n, soit $\binom{n}{i}$. Ces mêmes uplets peuvent également être décrits comme les suites strictement croissantes de i-entiers $\underline{l} = (1 \leqslant l_1 < \cdots < l_i \leqslant n)$. Enfin, réciproquement si on se donne des valeurs $c_{\underline{l}} \in \mathbb{K}$ pour chaque choix de telle suite, alors il existe une unique forme i-linéaire alternée $u \in \Lambda^i E^\vee$ définie par $u(e_{\underline{l}}) = c_{\underline{l}}$. □

f-det **Remarque 2.0.2.** Il résulte donc de la proposition ci-dessus que si E est de dimension n, alors toute forme n-linéaire alternée est entièrement déterminée par sa valeur $f(b_1, \dots, b_n)$ pour une base $(b_1, \dots, b_n)$ de E. On utilise un tel résultat pour la définition suivante.

det **Définition 2.0.3.** Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$, alors il existe un unique élément, $\det(u) \in \mathbb{K}$ tel que pour tout $f \in \Lambda^n E^\vee$, on ait :

$$f \circ u = \det(u) f.$$

Remarque 2.0.4. On a immédiatement que $\det(Id_E) = 1$ et $\det(0_E) = 0$ pour 0_E l'endomorphisme nul.

Démonstration. Tout d'abord, comme $u \in \mathcal{L}(E)$, si $f \in \Lambda^n E^\vee$, $f \circ u \in \Lambda^n E^\vee$. Ainsi, comme $\dim(\Lambda^n E^\vee) = 1$, il existe $f_0 \in \Lambda^n E^\vee$ telle que pour toute n-forme linéaire alternée, on ait $f = \lambda f_0$ avec $\lambda \in \mathbb{K}$, il suffit donc de montrer l'énoncé pour f_0. Or dans ce cas f_0 et $f_0 \circ u$ sont toutes deux des n-formes linéaires alternées, donc sont proportionnelles, d'où l'existence de $\det(u)$. □

compo **Proposition 2.0.5.** *Soit E un $\mathbb{K}$-espace vectoriel de dimension n, $u, v \in \mathcal{L}(E)$, alors on a l'égalité :*

$$\det(u \circ v) = \det(u) \det(v).$$

Démonstration. Soit $f \in \Lambda^n E^\vee$ non-nulle, d'après det 2.0.3, on a :

$$f \circ (u \circ v) = \det(u \circ v) f.$$

Or on a aussi, comme $f \circ u \in \Lambda^n E^\vee$:

$$f \circ (u \circ v) = (f \circ u) \circ v = \det(v)(f \circ u) = \det(v) \det(u) f,$$

d'où l'égalité souhaitée comme f est non-nulle. □

comp2 **Corollaire 2.0.6.** *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$, alors* $\det(u) \in \mathbb{K}^\times$*, si et seulement si u bijectif. De plus, on a alors :*

$$\det(u^{-1}) = \det(u)^{-1}.$$

Remarque 2.0.7. Comme $\mathbb{K}$ est un corps, on a $\mathbb{K}^\times = \mathbb{K} - \{0\}$, mais si on travaillait sur un anneau A, alors ce ne serait plus le cas. En effet, on a par exemple $\mathbb{Z}^\times = \{\pm 1\}$, ce qui est plus restrictif qu'un entier non-nul.

Démonstration. Si u est bijectif, soit u^{-1} son inverse, alors $u \circ u^{-1} = \mathrm{Id}_E$, donc en prenant les déterminants de chaque côté et en appliquant compo 2.0.5, on a :

$$\det(u) \det(u^{-1}) = 1$$

donc $\det(u) \in \mathbb{K}^\times$ et on a $\det(u^{-1}) = (\det(u))^{-1}$. Si u n'est pas bijectif, soit $x \in Ker(u)$ non-nul, alors on le complète en une base $(x, b_2, \ldots, b_n)$ de E de telle sorte que si f est une n-forme linéaire alternée non-nulle :

$$f \circ u(x, b_2, \ldots, b_n) = f(u(x), u(b_2), \ldots, u(b_n)) = 0 = \det(u) f(x, b_2, \ldots, b_n),$$

et $f(x, b_2, \ldots, b_n) \neq 0$ d'après 2.0.2 et comme $f \neq 0$. □

Pour un $\mathbb{K}$-espace vectoriel E de dimension n, si $B = (b_i)_{1 \leqslant i \leqslant n}$, $u \in \mathcal{L}(E)$, on note $\mathrm{Mat}_B(u) = (u_{ij})$ la matrice de u dans la base B. On a alors la formule suivante :

calcul **Proposition 2.0.8.** *Avec les notations ci-dessus, on a dessus :*

$$\det(u) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} u_{\sigma(i)i}.$$

En particulier, le membre de droite ne dépend du choix de la base B.

Démonstration. On choisit f une n-forme linéaire alternée non-nulle et on calcule $f(u(b_1), \ldots, u(b_n))$, on a alors :

$$f(u(b_1), \ldots, u(b_n)) = f(\sum_{j=1}^{n} u_{j1} b_j, \ldots, \sum_{j=1}^{n} u_{jn} b_j).$$

En utilisant le caractère alterné, lorsque l'on développe cette expression par n-linéarité, ne subsistent que les n-uplets $(b_{\sigma(1)}, \ldots, b_{\sigma(n)})$ pour $\sigma \in S_n$, on a donc :

$$f(\sum_{j=1}^{n} u_{j1} b_j, \ldots, \sum_{j=1}^{n} u_{jn} b_j) = \sum_{\sigma \in S_n} \prod_{i=1}^{n} u_{\sigma(i)i} f(b_{\sigma(1)}, \ldots, b_{\sigma(n)}) = \det(u) f(b_1, \ldots, b_n).$$

Ainsi, comme $f(b_{\sigma(1)}, \ldots, b_{\sigma(r)}) = \epsilon(\sigma) f(b_1, \ldots, b_n)$ et que $f(b_1, \ldots, b_n) \neq 0$, il suffit d'identifier les deux membres de l'égalité. □

Le calcul précédent justifie la définition du déterminant matriciel et va nous permettre de travailler dans une situation plus générale que celle des corps.

3. Déterminant matriciel

3.1. Définitions et premières propriétés. Dans toute cette section, A désigne un anneau commutatif.

Définition 3.1.1. Pour $M = (m_{ij}) \in M_n(A)$, on définit alors :

$$\det(M) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} m_{\sigma(i)i}. \qquad (3.1.1.1)$$ {ddet}

Remarque 3.1.2. Il résulte de 2.0.8 que si $A = \mathbb{K}$ est un corps et si u est l'endomorphisme dont la matrice dans la base canonique est M, on a $\det(u_M) = \det(M)$.

Exemple 3.1.3. Dans le cas $n = 2$, si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, alors $\det(M) = ad - bc$.

Dans la section précédente, on a établi un certain nombre de propriétés dans le cas des corps, on va maintenant les obtenir dans le cas général.

fond-d **Théorème 3.1.4.** *Pour $M \in M_n(A)$, on a les propriétés suivantes :*

(i) $\det(M) = \prod_{i=1}^{n} m_{ii}$, *si M est triangulaire supérieure.*

(ii) *On a* $\det(M) = \det({}^tM)$, *donc on a en particulier l'égalité ci-dessus dans le cas triangulaire inférieur.*

(iii) *Pour tout* $M, M' \in M_n(A), \det(MM') = \det(M)\det(M')$.

Démonstration. (i) Si M est triangulaire supérieure, alors pour tout $\sigma \neq \mathrm{Id}$, on vérifie par récurrence qu'il existe i tel que $\sigma(i) > i$ de telle sorte que $m_{\sigma(i)i} = 0$ comme M est triangulaire supérieure. Donc il ne reste que la contribution pour l'identité dans (3.1.1.1) et donc on en déduit que :

$$\det(M) = \prod_{i=1}^{n} m_{ii}.$$

(ii) Par définition, on a :

$$\det({}^tM) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} ({}^tM)_{\sigma(i)i} = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} m_{i\sigma(i)}.$$

Fixons $\sigma \in S_n$ et posons $j = \sigma(i)$, on a l'égalité :

$$\prod_{i}^{n} m_{i,\sigma(i)} = \prod_{j=1}^{n} m_{\sigma^{-1}(j),j}$$

Maintenant l'application $\sigma \mapsto \sigma^{-1}$ est une bijection de S_n et $\epsilon(\sigma) = \epsilon(\sigma^{-1})$, il vient donc que :

$$\det({}^tM) = \sum_{\sigma \in S_n} \epsilon(\sigma^{-1}) \prod_{j=1}^{n} m_{\sigma^{-1}(j),j} = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} m_{\sigma(i)i} = \det(M).$$

(iii) Si $A = \mathbb{K}$ est un corps, cela se déduit de 2.0.5 puisque $\det(u_M) = \det(M)$ si u_M est l'endomorphisme associé à M et du fait que la composition des endomorphismes correspond à la multiplication des matrices. Pour le calcul général, l'idée est de voir l'égalité à montrer comme une identité polynomiale. On se place dans l'anneau universel $\mathbb{Z}[B_{ij}, C_{ij}]_{1 \leqslant i,j \leqslant n}$ et

on regarde les matrices universelles $B = (B_{ij})$ et $C = (C_{ij})$. On a une inclusion dans le corps des fractions rationnelles :

$$\mathbb{Z}[B_{ij}, C_{ij}] \hookrightarrow \mathbb{Q}(B_{ij}, C_{ij}),$$

Maintenant comme $\mathbb{Q}(B_{ij}, C_{ij})$ est un corps, on a l'identité :

$$\det(BC) = \det(B).\det(C), \tag{3.1.7.1}$$

{univ-eq}

et comme les deux membres sont dans $\mathbb{Z}[B_{ij}, C_{ij}]$, l'identité a lieu dans $\mathbb{Z}[B_{ij}, C_{ij}]$. On va obtenir maintenant l'identité par spécialisation. Si A est un anneau arbitraire, $M = (m_{ij})$ et $M' = (m'_{ij})$ dans $M_n(A)$, on a un morphisme d'anneaux :

$$\phi : M_n(\mathbb{Z}[B_{ij}, C_{ij}]) \to M_n(A)$$

qui envoie les B_{ij} sur les m_{ij} et les C_{ij} sur les m'_{ij}. On applique alors ϕ à l'égalité (3.1.7.1) dans $\mathbb{Z}[B_{ij}, C_{ij}]$ et on déduit :

$$\det(MM') = \det(M)\det(M') \in M_n(A).$$

□

Si on ne veut pas avoir recours au corps des fractions rationnelles $\mathbb{Q}(B_{ij}, C_{ij})$, on peut utiliser le lemme suivant qui nous ramène aux complexes.

C-sp

Proposition 3.1.8. *Soit $P \in \mathbb{Z}[X_1, \ldots, X_n]$, supposons que pour tout $(x_1, \ldots, x_n) \in \mathbb{C}^n$, $P(x_1, \ldots, x_n) = 0$ alors $P = 0$.*

Démonstration. On procède par récurrence sur $n \in \mathbb{N}^*$. Si $n = 1$, alors P admet une infinité de racines donc est nul. Passons de n à $n + 1$, dans P, si par l'absurde $P \neq 0$, on considère le monôme de plus haut degré en X_{n+1}, soit d son degré. Si $d = 0$, alors cela signifie que $P \in \mathbb{Z}[X_1, \ldots, X_n]$ et on applique l'hypothèse de récurrence pour obtenir une contradiction.

Si $d \neq 0$, le monôme est de la forme $a_d X_1^{i_1} \ldots X_n^{i_n} X_{n+1}^d$. On évalue alors en $x_2 = \cdots = x_n = 1$ et $x_1 = z \in \mathbb{C}$ avec z tel que $z^{i_1} = a_d^{-1}$. On obtient alors un polynôme $Q = P(z, 1, \ldots, 1, X) \in \mathbb{C}[X]$ unitaire de degré d avec une infinité de zéros, donc $Q = 0$ contradiction. □

3.2. Propriétés de multilinéarité. On pourrait formuler des propriétés de multilinéarité pour un anneau A commutatif, mais cela nécessite d'ajouter beaucoup de définitions, alors que cela vient gratuitement dans le cas des corps. On suppose donc que l'on travaille sur un corps $\mathbb{K}$ commutatif et on expliquera les modifications à faire en général.

On peut considérer le déterminant comme une application $\phi_C : \mathbb{K}^n \times \ldots \mathbb{K}^n \to \mathbb{K}$ sur les colonnes donnée par $(C_1, \ldots, C_n) \mapsto \det(C_1, \ldots, C_n)$, où $\det(C_1, \ldots, C_n)$ désigne le déterminant de la matrice de colonnes $(C_1, \ldots, C_n)$. De même, on peut le voir comme une application $\phi_L : \mathbb{K}^n \times \ldots \mathbb{K}^n \to \mathbb{K}$ sur les lignes de la matrice. Il s'agit d'obtenir une

description de ϕ_C. On dispose de la base canonique $(e_1, \dots, e_n)$ de $\mathbb{K}^n$, on définit la forme n-linéaire alternée sur $f_{can} \in \Lambda^n \mathbb{K}^n$ par $f_{can}(e_1, \dots, e_n) = 1$.

lin **Théorème 3.2.1.** *On a une égalité $\phi_C = f_{can}$, en particulier ϕ_C est une forme n-linéaire alternée. De même, $\phi_L = f_{can} \circ \mathrm{tr}$ où ${}^t() : M_n(\mathbb{K}) \to M_n(\mathbb{K})$ est la transposition.*

Démonstration. Soit $(C_1, \dots, C_n)$ un n-uplet de colonnes, M la matrice associée d'endormorphisme u_M. D'après calcul 2.0.8, on a :

$$f_{can}(C_1, \dots, C_n) = f_{can} \circ u_M(e_1, \dots, e_n) \tag{3.2.1.1}$$
$$= \det(M) f_{can}(e_1, \dots, e_n) = \det(M) \tag{3.2.1.2}$$
$$= \phi_C(C_1, \dots, C_n). \tag{3.2.1.3}$$

La description avec les lignes vient alors de l'égalité $\det(M) = \det({}^t M)$. □

Agen **Remarque 3.2.2.** Dans le cas d'un anneau commutatif, on dispose de la même manière de la forme f_{can} mais cette fois, elle est n-A-linéaire et alternée. Ici, n-A-linéaire signifie A-linéaire en chacune des variables et une application $u : A^n \to A^m$ est A-linéaire si $u(x + \lambda y) = u(x) + \lambda u(y)$, avec $\lambda \in A$ et $(x, y) \in A^n \times A^n$. La proposition calcul 2.0.8 s'étend telle quelle dans le cas d'un anneau A commutatif en se plaçant sur un anneau de polynômes universel et en utilisant C-sp 3.1.8.

pivot **Corollaire 3.2.3.** *Soit un anneau commutatif A, une opération sur les colonnes du type $C_i \leftarrow C_i + \sum_{j \neq i} \lambda_j C_j$ (resp. du même type sur les lignes) ne changent le déterminant.*

Remarque 3.2.4. Ce sont les opérations que l'on fait quand on effectue le pivot de Gauss.

Démonstration. C'est immédiat par linéarité et ensuite comme on a une forme alternée. □

Dans le cas des corps, on a l'implication réciproque :

Proposition 3.2.5. *Soit $\mathbb{K}$ un corps, $M \in M_n(\mathbb{K})$, les assertions suivantes sont équivalentes :*

(i) *Il existe $X \in \mathbb{K}^n$, tel que $AX = 0$.*

(ii) *Les colonnes $C_1 \dots, C_n$ de M sont liées.*

(iii) *On a $\det(M) = 0$.*

Démonstration. Les deux premières assertions sont clairement équivalentes ; en effet si les $C_1 \dots, C_n$ de M sont liées, c'est équivalent à :

$$\exists (\lambda_1, \dots, \lambda_n) \in \mathbb{K}^n - \{0\}, \sum_{i=1}^{n} \lambda_i C_i = 0 \Leftrightarrow MX = 0,$$

avec $X = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$. Enfin pour montrer l'équivalence entre (i) et (iii), d'après comp2 2.0.6, $\det(M) \neq 0$ si et seulement si M est bijective. □

Exemple 3.2.6. Sur un anneau général, ce n'est plus vrai. On peut avoir $Mx = 0$ pour un vecteur non-nul $x \in A^n$ sans avoir $\det(M) = 0$. Il suffit de prendre $A = \mathbb{Z}/6\mathbb{Z}$, $M = \mathrm{diag}(3, 3) \in M_2(A)$ et $x = (2, 2)$. On a alors $Mx = 0$ et pourtant $\det(M) = 9 \neq 0$. Le bon énoncé (que nous ne montrerons pas) est le suivant :

$$\exists\, x \neq 0, Mx = 0 \Longleftrightarrow \det(M) \text{ est un diviseur de zéro,}$$

où dans un anneau A, un élement $y \in A$ est un diviseur de zéro s'il existe $x \neq 0$ tel que $yx = 0$. Ainsi, dans le contre-exemple précédent, on avait $\det(M) = 9$ et $9.2 = 0$ [6], donc $\det(M)$ est bien un diviseur de zéro.

Voyons sur un exemple comment on calcule un déterminant en travaillant sur les lignes et colonnes :

Exemple 3.2.7 (déterminant de Van der Monde)**.** Montrons que :

$$V(x_1, \ldots, x_n) = \begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & \ldots & x_n \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_1^{n-1} & x_2^{n-1} & & \ldots & x_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant j < i \leqslant n} (x_j - x_i).$$

Démonstration. On effectue des opérations sur les lignes $L_i \to L_i - x_1 L_{i-1}$ pour $i \geqslant 2$, on trouve alors :

$$V(x_1, \ldots, x_n) = \begin{vmatrix} 1 & 1 & 1 & \ldots & 1 \\ 0 & x_2 - x_1 & \ldots & \ldots & x_n - x_1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & x_2^{n-1} - x_1 x_2^{n-2} & & \ldots & x_n^{n-1} - x_1 x_n^{n-2} \end{vmatrix}$$

soit :

$$V(x_1, \ldots, x_n) = \begin{vmatrix} 1 & 1 & \ldots & 1 & \\ x_2 - x_1 & \ldots & \ldots & x_n - x_1 & \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_2^{n-2}(x_2 - x_1) & & \ldots & x_n^{n-2}(x_{n-1} - x_1) & \end{vmatrix}$$

d'où l'on déduit :

$$V(x_1, \ldots, x_n) = \prod_{j=2}^{n} (x_j - x_1) V(x_2, \ldots, x_n),$$

ainsi, par récurrence, on déduit :

$$V(x_1,\dots,x_n)=\prod_{j=2}^{n}(x_j-x_1)\prod_{2\leqslant j<i\leqslant n}(x_j-x_i)=\prod_{1\leqslant j<i\leqslant n}(x_j-x_i).$$

□

3.3. Pivot de Gauss. Pour λ, on appelle matrices de transvections, les matrices de la forme $I_n+\lambda E_{ij}\in GL_n(A)$ avec $i\neq j$ et E_{ij} les matrices élémentaires, nulles partout sauf en l'indice (i,j) où elle vaut 1. On a $(I_n+\lambda E_{ij})^{-1}=I_n-\lambda E_{ij}$.

On appelle matrice de dilatation, les matrices de la forme $\mathrm{diag}(1,\dots,1,\lambda)$ avec $\lambda\in A^\times$. Etant donnée une matrice $M\in M_n(A)$, on rappelle que si l'on multiplie à gauche (resp. à droite) par $I_n+\lambda E_{ij}$ revient à faire la transformation élémentaire sur les colonnes $C_i\to C_i+\lambda C_j$ (resp. sur les lignes $L_i\to L_i+\lambda L_j$.)

Théorème 3.3.1 (Pivot de Gauss)**.** *Soit $\mathbb{K}$ un corps, alors $GL_n(\mathbb{K})$ est engendré par les transvections et dilatations.*

Démonstration. On procède par récurrence sur $n\in\mathbb{N}^*$, si $n=1$, il n'y a rien à montrer, passons de n à $n+1$. Soit $M\in GL_n(\mathbb{K})$, $\lambda=\det(M)\in\mathbb{K}^*$, en multipliant par $\mathrm{diag}(1,\dots,1,\lambda^{-1})$, on se ramène à une matrice de déterminant un. On regarde la première ligne, comme elle ne peut être entièrement nulle puisque la matrice est inversible, soit i_0 le plus petit entier tel que $a_{i_0}\in\mathbb{K}^\times$. Si $i_0=1$, on ne fait rien, si $i_0\geqslant 2$, alors on remplace $C_1\to C_1+C_{i_0}$ et on se ramène au cas où $a_{11}\neq 0$. Pour tout $i\geqslant 2$, on remplace la colonne C_i par $C_i-\frac{a_{1i}}{a_{11}}C_1$ et on se ramène à $L_1=(1,0,\dots,0)$. Ensuite, pour $i\geqslant 2$, on remplace la ligne L_i par $L_i-\frac{a_{i1}}{a_{11}}L_1$. On s'est donc ramené à une matrice de la forme :

$$M'=\left(\begin{array}{c|c}1&0\\\hline 0&M'\end{array}\right),$$

avec $\det(M'')=\det(M)$ [1], donc $M''\in GL_{n-1}(\mathbb{K})$. et on applique l'hypothèse de récurrence à GL_{n-1} via le plongement $GL_{n-1}\hookrightarrow GL_n$:

$$K\mapsto\left(\begin{array}{c|c}1&0\\\hline 0&K\end{array}\right).$$

□

Remarque 3.3.2. Il est crucial ici de travailler avec un corps, le résultat est faux déjà dans le cas de $GL_2(\mathbb{C}[X,Y])$ et c'est un problème délicat de répondre à cette question dans le

1. Dans 3.1.1.1, seules les permutations $\sigma\in S_n$ telles que $\sigma(1)=1$ contribuent et ce groupe s'identifie à S_{n-1}.

cas général. On peut montrer que la matrice de déterminant un :

$$M = \begin{pmatrix} 1+XY & X^2 \\ -Y^2 & 1-XY \end{pmatrix}$$

n'est pas un produit de transvections. On remarque aussi que dans cette matrice, il n'y aucun coefficient $a_{ij} \in A^\times$. Le résultat est revanche vrai pour les matrices inversibles de $M_n(\mathbb{Z})$ ou $M_n(\mathbb{K}[X])$ pour $\mathbb{K}$ un corps, car ce sont des anneaux euclidiens, i.e. qui disposent d'une division euclidienne.

4. Comatrice

4.1. Développement par rapport à une ligne ou colonne. Soit $M \in M_n(A)$, on note M_{ij} le déterminant de la matrice extraite en enlevant la i-ème ligne et la j-ième colonne, multiplié par $(-1)^{i+j}$. On appelle cela le cofacteur d'indice (i,j). On note $\mathrm{Com}(M)$ la matrice des cofacteurs.

De l'égalité pour toute matrice $B \in M_n(A)$, $\det(B) = \det({}^tB)$ et du fait que la transposition échange lignes en colonnes, on déduit que :

$$\mathrm{Com}({}^tM) = {}^t\,\mathrm{Com}(M). \qquad (4.1.0.1)$$ {t-com}

col-dvlp **Théorème 4.1.1.** *On a :*

$$\forall\ j \in [\![1,n]\!], \det(M) = \sum_{i=1}^{n} m_{ij} M_{ij}\ \textit{(développement par rapport à la } j\textit{-ième colonne)}.$$

$$\forall\ i \in [\![1,n]\!], \det(M) = \sum_{j=1}^{n} m_{ij} M_{ij}\ \textit{(développement par rapport à la } i\textit{-ème ligne)}.$$

Démonstration. Soient $(C_1, \ldots, C_n)$ les colonnes de $M = (m_{ij})$. Fixons $k \in [\![1,n]\!]$, on note $(E_1, \ldots E_n)$ les vecteurs de la base canonique de A^n. On a donc $C_k = \sum_{i=1}^{n} m_{ik} E_i$. En utilisant la n-linéarité du déterminant (lin 3.2.1 pour un corps et Agen 3.2.2 dans le cas général). On a :

$$\det(C_1, \ldots, C_n) = \sum_{i=1}^{n} m_{ik} \det(C_1, \ldots, C_{k-1}, E_i, C_{k+1} C_n).$$

On considère alors la permutation $\sigma = (1 \ldots k)$ de signature $\epsilon(\sigma) = (-1)^{k-1}$ et on a donc :

$$\det(C_1, \ldots, C_{k-1}, E_i, C_{k+1} C_n) = (-1)^{k-1} \det(E_i, C_1, C_2, \ldots, C_{k-1}, C_{k+1}, \ldots, C_n).$$

On a une égalité de matrices :

$$(E_i, C_1, C_2, \dots, C_{k-1}, C_{k+1}, \dots, C_n) = \begin{pmatrix} 0 & L_1 \\ \vdots & L_2 \\ 1 & L_i \\ 0 & \vdots \\ 0 & L_n \end{pmatrix}$$

et on permute maintenant la i-ème ligne à l'aide de $\sigma' = (12 \dots i)$ de signature $(-1)^{i-1}$, soit :

$$\det(C_1, \dots, C_{k-1}, E_i, C_{k+1}C_n) = (-1)^{k-1}(-1)^{i-1} \det(\begin{pmatrix} 1 & L_i \\ 0 & L_1 \\ \vdots & \vdots \\ 0 & L_{i-1} \\ 0 & L_{i+1} \\ \vdots & \vdots \\ 0 & L_n \end{pmatrix}),$$

et le membre de gauche est alors égal au déterminant :

$$\det \begin{pmatrix} L_1 \\ \vdots \\ L_{i-1} \\ L_{i+1} \\ L_n \end{pmatrix}$$

qui est précisément la matrice extraite où l'on a retiré la i-ème ligne et la j-ième colonne.

□

com **Théorème 4.1.2.** *Soit $M \in M_n(A)$, alors on a :*

$$M.{}^t\operatorname{Com}(M) = {}^t\operatorname{Com}(M)M = \det(M)I_n.$$

Démonstration. Soit $i \in [\![1, n]\!]$, calculons $(M.{}^t\operatorname{Com}(M))_{ii}$, on a alors :

$$(M.{}^t\operatorname{Com}(M))_{ii} = \sum_{j=1}^{n} m_{ij}({}^t\operatorname{Com}(M))_{ji} = \sum_{j=1}^{n} m_{ij}\operatorname{Com}(M)_{ij} = \det(M)$$

où la dernière égalité vient de col-dvlp 4.1.1. Regardons les coefficients non-diagonaux, fixons $i \neq j$, on a :

$$(M.{}^t\operatorname{Com}(M))_{ij} = \sum_{k=1}^{n} m_{ik}M_{jk}.$$

Notons $L_1, \dots, L_n$ les lignes de M. Soit $\tilde{M}$ la matrice où l'on remplace la j-ième ligne de A par L_i. On a immédiatement $\det(\tilde{A}) = 0$ par alternance. De plus, les lignes d'indices

différent de j de A et $\tilde{A}$ sont les mêmes, de telle sorte que les cofacteurs de A et $\tilde{A}$ sont les mêmes sur la ligne j. Ainsi, on a :

$$\sum_{k=1}^{n} m_{ik}M_{jk} = \sum_{k=1}^{n} m_{ik}\tilde{M}_{jk} = \det(\tilde{A}) = 0.$$

Ainsi, on obtient l'égalité :

$$M.{}^t\operatorname{Com}(M) = \det(M).I_n, \tag{4.1.2.1}$$ {1-eq}

comme souhaité. Pour montrer que ${}^t\operatorname{Com}(M).M = \det(M).I_n$, on applique la transposition ainsi que l'égalité (4.1.0.1) d'où l'on trouve :

$${}^t({}^t\operatorname{Com}(M).M) = {}^tM\operatorname{Com}(M) = \det({}^tM)I_n,$$

où la dernière égalité se déduit de (4.1.2.1) appliquée à ${}^tM$. Or, $\det(M) = \det({}^tM)$, ainsi on obtient :

$${}^t({}^t\operatorname{Com}(M).M) = \det(M).I_n,$$

et on applique à nouveau la transposition et on déduit la deuxième égalité. □

4.2. Applications de la comatrice.

4.2.1. *Groupe linéaire.* Pour un anneau commutatif A, on appelle groupe linéaire sur A, l'ensemble :

$$GL_n(A) = \{M \in M_n(A), \exists B \in M_n(A), MB = I_n\}.$$

On remarque que dans la définition, on ne demande que l'existence d'un inverse à droite, on va voir que cela force d'être aussi un inverse à gauche.

inv **Théorème 4.2.2.** *On a $GL_n(A) = \{M \in M_n(A), \det(M) \in A^\times\}$. En particulier, pour tout $M \in GL_n(A)$, on a :*

$$M^{-1} = \frac{1}{\det(M)}{}^t\operatorname{Com}(M),$$

et l'inverse à droite est aussi un inverse à gauche. Enfin, $GL_n(A)$ est un groupe.

Démonstration. Soit $M \in GL_n(A)$ alors il existe B tel que $MB = I_n$ d'où en appliquant le déterminant et par 3.1.4, on obtient :

$$\det(M)\det(B) = 1 \tag{4.2.2.1}$$ {invD}

et $\det(M) \in A^\times$. Réciproquement, pour $M \in M_n(A)$ tel que $\det(M) \in A^\times$, soit $B = \frac{1}{\det(M)}{}^t\operatorname{Com}(M) \in M_n(A)$, il résulte de 4.1.2 que $MB = I_n$ et $M \in GL_n(A)$. On obtient donc ainsi la formule pour l'inverse. Le fait que B est un inverse à gauche vient alors du fait que :

$$M.{}^t\operatorname{Com}(M) = {}^t\operatorname{Com}(M)M = \det(M)I_n$$

Enfin, $GL_n(A)$ est bien un groupe car $\det : M_n(A) \to A$ est un morphisme de monoïdes et comme $A^\times$ est un groupe $GL_n(A) = \det^{-1}(A^\times)$ en est un aussi. □

Exemple 4.2.3. Si A est un corps $\mathbb{K}$, alors $\mathbb{K}^\times = \mathbb{K} - \{0\}$ et on retrouve la condition habituelle que :

$$M \in GL_n(\mathbb{K}) \iff \det(M) \neq 0.$$

En revanche, ce n'est plus le cas pour un anneau général. Si $A = \mathbb{Z}$, on a :

$$M \in GL_n(\mathbb{Z}) \iff \det(M) \in \mathbb{Z}^\times = \{1, -1\}.$$

Enfin si $A = \mathbb{K}[X]$, avec $\mathbb{K}$ un corps, alors on a $\mathbb{K}[X]^\times = \mathbb{K}^\times$ et donc les matrices inversibles de $M_n(\mathbb{K}[X])$ sont celles de déterminant dans $\mathbb{K}^\times$.

Corollaire 4.2.4. *Pour tout $P \in GL_n(A)$, on a $\det(P^{-1}) = \det(P)^{-1}$. Ainsi si M et Q sont semblables dans $M_n(A)$, on a $\det(M) = \det(Q)$.*

Démonstration. La première assertion se déduit de (4.2.2.1). Pour la deuxième, on écrit $M = PQP^{-1}$ et on applique le déterminant, 3.1.4 ainsi que la première assertion. □

Définition 4.2.5. Pour un anneau commutatif A, on définit le groupe spécial linéaire $SL_n(A) = \{M \in GL_n(A), \det(M)\} = \mathrm{Ker}(\det : GL_n(A) \to A^\times)$.

4.2.6. *Formules de Cramer.* On considère un système linéaire :

$$MX = B$$

avec $M \in GL_n(A)$, $X, B \in A^n$ des vecteurs colonnes. On écrit :

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Proposition 4.2.7 (Formules de Cramer)**.** *Sous les hypothèses ci-dessus. Pour tout $k \in [\![1, n]\!]$, on a les formules suivantes :*

$$x_k = \frac{\det(C_1, \ldots, C_{k-1}, B, C_{k+1}, \ldots, C_n)}{\det(M)}.$$

Démonstration. On a $X = M^{-1}B$, et on utilise la formule d'inversion de 4.2.2 pour déduire :

$$x_k = \sum_{i=1}^{n} (M^{-1})_{ki} B_i = \frac{1}{\det(M)} \sum_{i=1}^{n} ({}^t \mathrm{Com}(M))_{ki} B_i = \frac{1}{\det(M)} \sum_{i=1}^{n} (\mathrm{Com}(M))_{ik} B_i$$

et la dernière égalité est exactement le développement de $\det(C_1, \ldots, C_{k-1}, B, C_{k+1}, \ldots, C_n)$ par rapport à la k-ième colonne. □

5. Mineurs

Soit $M \in M_n(A)$, soit $r \in [\![1, n]\!]$, on se donnes des indices $1 \leqslant i_1 < \cdots < i_r \leqslant n$ et $1 \leqslant j_1 < \cdots < j_r \leqslant n$, on appelle mineur d'ordre r de A le nombre :

$$\det((A_{i_k j_l})_{1 \leqslant k \leqslant r, 1 \leqslant l \leqslant r}).$$

Il y a $\binom{n}{r}^2$ mineurs d'ordre r, puisqu'il s'agit de choisir deux fois r entiers parmi n.

min **Théorème 5.0.1.** *Soit $\mathbb{K}$ un corps, $M \in M_n(\mathbb{K})$, $r \in [\![1, n]\!]$, alors $\mathrm{rg}(M) \geqslant r$ si et seulement si il existe un mineur d'ordre r non-nul.*

Remarque 5.0.2. Il est indispensable ici de travailler sur un corps, en général il n'y a pas de notion de rang.

Démonstration. Soient $C_1, \ldots, C_n$ les colonnes de M, comme $\mathrm{rg}(M) \geqslant r$, il existe $j_1 < \cdots < j_r$ tels que $\mathrm{rg}(B := [C_{j_1}, \ldots, C_{j_r}]) = r$. Comme $\mathrm{rg}(B) = \mathrm{rg}({}^tB) = r$, il existe $i_1 < \cdots < i_r$ tels que $\mathrm{rg}(L_{i_1}, \ldots L_{i_r}) = r$ où les L_i sont les lignes de B. On considère alors :

$$D = \begin{pmatrix} L_{i_1} \\ \vdots \\ L_{i_r} \end{pmatrix} \in M_r(\mathbb{K}),$$

comme $\mathrm{rg}(D) = r$, on a donc que D est inversible et $\det(D) \neq 0$. Réciproquement s'il existe un mineur d'ordre r tel que $\det((M_{i_k j_l})_{1 \leqslant k \leqslant r, 1 \leqslant l \leqslant r}) \neq 0$, notons $M_{(r)}$ la matrice extraite qui est donc de $\mathrm{rg}(r)$, en particulier ses colonnes forment un système libre. Or les colonnes $C_{j_1}, \ldots, C_{j_r}$ de M sont envoyés linéairement sur les colonnes de $M_{(r)}$ qui forment une base de $M_r(\mathbb{K})$, donc les colonnes $C_{j_1}, \ldots, C_{j_r}$ forment un système libre et on a $\mathrm{rg}(M) \geqslant r$. □

6. Déterminants par blocs

On se donne une matrice de $M_n(A)$ donnée par blocs :

$$M = \begin{pmatrix} B & C \\ 0 & Q \end{pmatrix}$$

avec $B \in M_p(A)$, $Q \in M_r(A)$ et $C \in M_{p,r}(A)$.

Proposition 6.0.1. *On a l'égalité :*

$$\det(M) = \det(B) \det(Q).$$

Démonstration. On commence par traiter le cas d'un corps $\mathbb{K}$. Si U n'est pas inversible, alors les p premières colonnes de M sont liées, donc $\det(U) \det(W) = 0 = \det(A)$. Si U inversible, on a :

$$\begin{pmatrix} B & C \\ 0 & Q \end{pmatrix} = \begin{pmatrix} B & 0 \\ 0 & I_r \end{pmatrix} \begin{pmatrix} I_p & B^{-1}C \\ 0 & Q \end{pmatrix}$$

A nouveau, si Q non inversible, on a le résultat en raisonnant sur les lignes. Et si Q inversible, on a :

$$\begin{pmatrix} B & C \\ 0 & Q \end{pmatrix} = \begin{pmatrix} B & 0 \\ 0 & I_r \end{pmatrix} \begin{pmatrix} I_p & B^{-1}CQ^{-1} \\ 0 & I_n \end{pmatrix} \begin{pmatrix} I_p & \\ 0 & Q \end{pmatrix},$$

d'où l'on déduit bien $\det(M) = \det(B)\det(Q)$.

Dans le cas général, on voit l'égalité

$$\det(M) = \det(B)\det(Q),$$

comme une identité polynomiale dans $\mathbb{Z}[B_{ij}, Q_{ij}, C_{ij}]$, que l'on plonge dans le corps $\mathbb{Q}(B_{ij}, Q_{ij}, C_{ij})$. Ainsi le cas des corps nous donne que l'identité est vrai dans $\mathbb{Z}[B_{ij}, Q_{ij}, C_{ij}]$. Il ne nous reste ensuite plus qu'à spécialiser dans un anneau A commutatif arbitraire. □

Corollaire 6.0.2. *En particulier, on obtient immédiatemment par récurrence que si M est triangulaire par blocs, de blocs $M_1, \ldots, M_p$, on a :*

$$det(M) = \prod_{i=1}^{p} \det(M_i).$$

7. Polynôme caractéristique

Soit $M \in M_n(A)$, on considère alors la matrice $XI_n - M \in M_n(A[X])$ et on définit le polynôme caractéristique de M par :

$$\chi_M(X) = \det(XI_n - M) \in A[X].$$

car-cal **Proposition 7.0.1.** *Soit $M \in M_n(A)$, alors χ_M est unitaire de degré n et :*

$$\chi_M(X) = X^n - \mathrm{Tr}(M)X^{n-1} + \cdots + (-1)^n \det(A).$$

Démonstration. La formule du déterminant donne :

$$\chi_M(X) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} (\delta_{\sigma(i)i} X - M_{\sigma(i)i})$$

avec $\delta_{\sigma(i)i} = 1$ si $\sigma(i) = i$ et 0 sinon. En particulier, dans le membre de droite, on a au plus n termes de degré un, ainsi, on a $\deg(\chi_M) \leqslant n$. Pour $\sigma \in S_n$, notons $Q_\sigma := \prod_{i=1}^{n} (M_{\sigma(i)i} - \delta_{\sigma(i)i} X)$. Si $\sigma \neq \mathrm{Id}$ alors, alors σ a au plus $n-2$ points fixes, donc $\deg Q_\sigma \leqslant n-2$. Si $\sigma = \mathrm{Id}$, le coefficient de X^n est $(-1)^n$.

Pour obtenir le coefficient en X^{n-1}, la seule contribution vient de $\sigma = \mathrm{Id}$ et dans ce cas, on obtient $-(\sum_{i=1}^{n} M_{ii}) = -\mathrm{Tr}(M)$. Pour déterminer le terme constant, il suffit de calculer $\chi_M(0)$, et on obtient alors :

$$\chi_M(0) = (-1)^n \det(M).$$

□

Une des raisons pour lesquelles le polynôme caractéristique est utile est la proposition suivante :

sp1 **Proposition 7.0.2.** *Soit $\mathbb{K}$ un corps, $M \in M_n(\mathbb{K})$ alors $\lambda \in \mathbb{K}$ est une valeur propre de M si et seulment si λ est une racine de χ_M. En particulier, M admet au plus n valeurs propres.*

Démonstration. Si $\lambda \in \mathbb{K}$ est une valeur propre, il existe $x \in \mathbb{K}^n$ tel que $Mx = \lambda x$, donc $(M - \lambda I_n).x = 0$, ainsi $M - \lambda I_n$ est non-inversible, donc $\chi_M(\lambda) = \det(M - \lambda I_n) = 0$. Réciproquement, soit λ une racine de χ_M, alors $\chi_M(\lambda) = \det(M - \lambda I_n) = 0$, donc $M - \lambda I_n$ n'est pas inversible et donc $\mathrm{Ker}(M - \lambda I_n) \neq \{0\}$. Comme $\deg \chi_M = n$, il admet au plus n racines, donc M admet au plus n valeurs propres. □

sim **Lemme 7.0.3.** *Deux matrices semblables M et Q de $M_n(A)$ ont même polynôme caractéristique.*

Démonstration. Soit $P \in GL_n(A)$ tel que $M = PQP^{-1}$, on a alors $XI_n - M = P(XI_n - Q)P^{-1}$ et on applique le déterminant. □

dens **Exemple 7.0.4.** Soit $\mathbb{K}$ un sous-corps de $\mathbb{C}$, alors $GL_n(\mathbb{K})$ est dense dans $M_n(\mathbb{K})$. Soit $M \in M_n(\mathbb{K})$, on définit la suite $M_r = (M - \frac{1}{r}I_n)_{r \geqslant 1}$. La suite (M_r) converge clairement vers M. Il suffit de voir que pour r assez grand $M_r \in GL_n(\mathbb{K})$. Or χ_M a un nombre fini de racines, de telle sorte que pour r assez grand, $\frac{1}{r}$ n'est pas une valeur propre. Ainsi, M_r est inversible, ce qui conclut.

Une application de la densité est l'énoncé suivant :

inv-det **Théorème 7.0.5.** *Soit $B, C \in M_n(A)$, alors $\chi_{BC} = \chi_{CB}$.*

Remarque 7.0.6. Ce qui est intéressant dans cet énoncé, c'est que même si l'on se restreint au cas où A est un corps, la preuve « naturelle » marche pour $\mathbb{K} = \mathbb{C}$. Si l'on veut le résultat pour $\mathbb{F}_p$, on a besoin d'utiliser la spécialisation.

Démonstration. On commence par montrer l'énoncé dans le cas $A = \mathbb{C}$. Supposons que B est inversible, alors on a $BCBB^{-1} = BC$, ainsi CB et BC sont semblables donc ont même polynôme caractéristique d'après 7.0.3. Si B n'est pas inversible, par densité 7.0.4 soit (B_n) une suite de matrices inversibles qui converge vers B. Alors pour tout $n \in \mathbb{N}$, on a $\chi_{CB_n} = \chi_{B_nC}$ et comme les coefficients du polynôme caractéristique sont polynomiaux en les coefficients de la matrice, par continuité, on en déduit que $\chi_{CB} = \chi_{BC}$.

On considère maintenant l'anneau universel $\mathbb{Z}[B_{ij}, C_{ij}]$, pour chaque $k \in [\![1, n]\!]$, considérons le polynôme $Q_k = c_k(CB) - c_k(BC) \in \mathbb{Z}[B_{ij}, C_{ij}]$, où $c_k(-)$ est le coefficient devant X^k du polynôme caractéristique. Le cas des complexes nous donne que pour toute évaluation de

Q_k en un uplet $(b_{ij}, c_{ij}) \in \mathbb{C}^{2n^2}$ est nulle, donc $Q_k = 0$ d'après C-sp 3.1.8. Il ne nous reste plus qu'à spécialiser la situation de $\mathbb{Z}[B_{ij}, C_{ij}]$ à un anneau A général et on a le résultat. □

Il y a une deuxième preuve plus algébrique, mais plus astucieuse dans le cas des corps :

On se place dans $M_n(\mathbb{K}(Y))$ et on considère la matrice $B - YI_n$. Comme $(-1)^n\chi_B = \det(B - YI_n) \in \mathbb{K}[Y]$ est un polynôme de degré n en Y, on en déduit qu'il est inversible dans $\mathbb{K}(Y)$, ainsi $B - YI_n \in GL_n(\mathbb{K}(Y))$, on en déduit alors que :

$$\chi_{C(B-YI_n)} = \chi_{(B-YI_n)C},$$

et il suffit de prendre $Y = 0$.

7.1. Théorème de Cayley-Hamilton. Soit un anneau commutatif A et $M \in M_n(A)$ alors pour tout $P = \sum_{k=0}^{d} a_k X^k \in A[X]$, on peut évaluer P en M, soit :

$$P(M) = \sum_{k=0}^{d} a_k M^k \in M_n(A).$$

CH **Théorème 7.1.1.** *[Cayley-Hamilton] Soit $M \in M_n(A)$, alors on a $\chi_M(M) = 0$.*

Avant de montrer ce théorème, voyons pourquoi il n'est pas si trivial. Une « preuve » (fausse) consiste à dire que

$$\det(M - XI_n)(M) = \det(M - M) = 0.$$

Expliquons pourquoi c'est faux. Ici, on va bien voir l'utilité d'avoir travaillé depuis le début avec des anneaux. Toute la subtilité est dans la notion d'évaluation. Dans la suite, supposons $A = \mathbb{Z}$, c'est suffisant pour l'explication. La matrice $M - XI_n$ est dans $M_n(\mathbb{Z}[X])$. Si on veut évaluer X en une certaine matrice $K \in M_n(\mathbb{Z})$, cela revient à considérer un morphisme d'anneaux

$$\phi_K : \mathbb{Z}[X] \to M_n(\mathbb{Z})$$

Or, on a une matrice dans $M_n(\mathbb{Z}[X])$, donc évaluer X en K revient à considérer alors un morphisme d'anneaux :

$$\tilde{\phi}_K : M_n(\mathbb{Z}[X]) \to M_n(M_n(\mathbb{Z})).$$

Sauf que maintenant, comme $M_n(\mathbb{Z})$ est un anneau non-commutatif, si l'on considère $M_n(M_n(\mathbb{Z}))$, il n'y a pas de théorie du déterminant qui soit multiplicatif et qui serait un morphisme de monoïdes $M_n(M_n(\mathbb{Z})) \to M_n(\mathbb{Z})$. En particulier, bien que l'on puisse évaluer $M - XI_n$ en M, prendre le déterminant n'a pas de sens et donc l'argument ci-dessus ne marche pas. Passons maintenant à la preuve.

Démonstration. On part de l'identité venant de la comatrice com 4.1.2 et de la définition du polynôme caractéristique :

$$(XI_n - M).{}^t\operatorname{Com}(XI_n - M) = \chi_M(X).I_n.$$

Notons $\tilde{C} := {}^t\operatorname{Com}(XI_n - M)$. Comme la matrice des cofacteurs consiste en les mineurs d'ordre $n-1$, on écrit :

$$\tilde{C} = B_0 + B_1X + \cdots + B_{n-1}X^{n-1} \in M_n(A[X])$$

avec les $B_i \in \mathrm{M}_n(A)$. On a donc :

$$(XI_n - M)(B_0 + B_1X + \cdots + B_{n-1}X^{n-1}) = a_0I_n + \ldots a_nX^n.I_n = \chi_M(X).I_n$$

Il en résulte alors $MB_0 = -a_0I_n$, $B_0 - MB_1 = a_1I_n, \ldots, B_{n-2} - MB_{n-1} = a_{n-1}I_n, B_{n-1} = a_nI_n$. On multiplie alors la première égalité par I_n, la seconde par M,..., la dernière par M^n et on fait la somme, le membre de gauche est alors nul et le membre de droite donne :

$$0 = \chi_M(M),$$

ce qu'on voulait. □

Exemple 7.1.2. Dans le cas de $M_2(A)$, le théorème de Cayley-Hamilton dit que pour tout $M \in M_2(A)$:

$$M^2 - \operatorname{Tr}(M)M + \det(M)I_2 = 0.$$

Donnons d'ores et déjà une petite application.

pol **Proposition 7.1.3.** *Soit $M \in GL_n(A)$, alors M^{-1} est un polynôme en M.*

Démonstration. Par Cayley Hamilton, on a :

$$\chi_M(M) = M^n + a_{n-1}M^{n-1} + \cdots + a_0I_n = 0$$

D'après 7.0.1, on a $a_0 = (-1)^n \det(M)$ et d'après 4.2.2, $\det(M) \in A^\times$, donc $a_0 \in A^\times$ et on peut écrire :

$$M.(M^{n-1} + a_{n-1}M^{n-2} + \cdots + a_1I_n) = -a_0I_n$$

et on trouve :

$$M^{-1} = -\frac{1}{a_0}[M^{n-1} + a_{n-1}M^{n-2} + \cdots + a_1I_n.] \qquad (7.1.3.1)$$ {inv-pol}

□

En fait, on a même le résultat plus fort suivant valable pour toute matrice :

pol-com **Proposition 7.1.4.** *Soit $\mathbb{K}$ un corps, soit $M \in GL_n(\mathbb{K})$, posons $Q_M = \frac{\chi_M - \det(M)}{X} \in A[X]$, alors on a l'égalité :*

$$Q_M(M) = {}^t\operatorname{Com}(M).$$

Démonstration. Tout d'abord, si M est inversible, comme $M^{-1} = \frac{{}^t\operatorname{Com}(M)}{\det(M)}$, il résulte de (7.1.3.1) que $Q(M) = {}^t\operatorname{Com}(M)$ Dans le cas général, on reprend l'astuce de 7.0.5 et on se place dans $M_n(\mathbb{K}(Y))$, de telle sorte que la matrice $M - YI_n \in GL_n(\mathbb{K}(Y))$. Ainsi, on a :

$$Q_{M-YI_n}(M - YI_n) = {}^t\operatorname{Com}(M - YI_n),$$

Maintenant, on a $Q_{M-YI_n} \in \mathbb{K}[Y][X]$ par construction, il ne nous reste plus qu'à évaluer en $Y = 0$ et on a le résultat voulu. □

7.2. Matrices compagnons. Partant d'un polynôme $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in A[X]$, on se pose la question de savoir si c'est le polynôme caractéristique d'une matrice $M \in M_n(A)$. Il s'avère que c'est effectivement le cas. On considère alors la matrice, appelée matrice compagnon :

$$C_P = \begin{pmatrix} 0 & 0 & 0 & \cdots & -a_0 \\ 1 & 0 & 0 & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}$$

Si $(e_1, \dots, e_n)$ est la base canonique, alors l'endomorphisme correspondant u vérifie :

$$\forall\ 1 \leqslant i \leqslant n-1, u(e_i) = e_{i+1}, u(e_n) = -\sum_{k=0}^{n-1} a_k e_k.$$

comp **Théorème 7.2.1.** *On a $\chi_{C_P} = P$.*

Démonstration. On va utiliser la description de l'endomorphisme pour obtenir le calcul du polynôme caractéristique. Tout d'abord, il résulte de la description de u que $(e_1, u(e_1), \dots, u^{n-1}(e_1))$ s'identifie précisément à la base canonique et on a :

$$u^n(e_1) = -\sum_{k=1}^{n-1} a_k e_k = -\sum_{k=1}^{n-1} a_k u^k(e_1),$$

ainsi on obtient que $P(u)(e_1) = 0$. Montrons que $P = \chi_u$, les deux sont unitaires de degré n, on effectue la division euclidienne de P par χ_u et on a :

$$P = \chi_u + R$$

avec $\deg(R) < n$. Or, en évaluant en u puis en e_1, on a par Cayley-Hamilton :

$$0 = P(u)(e_1) = \chi_u(u)(e_1) + R(u)(e_1) = R(u)(e_1).$$

Or comme $\deg(R) < n$ et $R(u)(e_1) = 0$, cela force que $(e_1, u(e_1), \dots, u^{n-1}(e_1))$ soit liée, ce qui n'est pas donc $R = 0$ et $P = \chi_u$. □

Chapitre 3

Réduction des endomorphismes

Introduction

Le but de ce chapitre est de ramener une matrice quelconque à une forme plus simple pour laquelle, il est aisé de calculer un certain nombre d'invariants, déterminant, rang, polynômes d'endomorphismes, etc... Pour une telle théorie, il est en revanche indispensable de travailler sur un corps $\mathbb{K}$. Une des principales raisons pour cela est que la réduction des endomophismes utilise de façon cruciale l'anneau $\mathbb{K}[X]$ qui admet des propriétés particulières si $\mathbb{K}$ est un corps mais plus si A est un anneau commutatif arbitraire (même déjà $\mathbb{Z}$).

1. Polynômes d'endomorphismes

1.1. Lemme des noyaux. Soient $\mathbb{K}$ un corps et E un $\mathbb{K}$-espace vectoriel. Pour $u \in \mathcal{L}(E)$ et $k \in \mathbb{N}$ on définit u^k comme la composée k-fois $u \circ \cdots \circ u$ avec la convention que $u^0 = \mathrm{Id}_E$. Plus généralement, pour $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{K}[X]$, on définit alors :

$$P(u) = \sum_{k=0}^{n} a_k u^k \in \mathcal{L}(E).$$

En particulier, si $P = 1$, on a $1(u) = \mathrm{Id}_E$.

Lemme 1.1.1. *Soient $P, Q \in \mathbb{K}[X]$, $u \in \mathcal{L}(E)$, on a alors les propriétés suivantes :*

(i) $\forall\ \lambda \in \mathbb{K}, (P + \lambda Q)(u) = P(u) + \lambda Q(u)$.

(ii) $(PQ)(u) = (QP)(u) = P(u) \circ Q(u)$.

Démonstration. (i) est immédiat. Pour (ii), on a déjà clairement que $(PQ)(u) = (QP)(u)$ puisque que $\mathbb{K}[X]$ est commutatif, montrons que $(PQ)(u) = P(u) \circ Q(u)$. L'égalité est linéaire en P et en Q de telle sorte que l'on se ramène à $P = X^l$ et $Q = X^r$ et l'égalité se ramène à :

$$u^{l+r} = u^l \circ u^r,$$

qui est vraie par définition. □

Dans la suite, on note $\mathbb{K}[u] = \{P(u), P \in \mathbb{K}[X]\} \subset \mathrm{End}(E)$.

kern1 **Proposition 1.1.2.** *[Lemme des noyaux] Soient $P, Q \in \mathbb{K}[X]$, $P \wedge Q = 1$ et $u \in \mathcal{L}(E)$, alors on a :*

$$\mathrm{Ker}((PQ)(u)) = \mathrm{Ker}(P(u)) \oplus \mathrm{Ker}(Q(u)).$$

Démonstration. Soit $x \in \mathrm{Ker}(P(u)) \cap \mathrm{Ker}(Q(u))$, alors $P(u)(x) = Q(u)(x) = 0$. Comme $P \wedge Q = 1$, on écrit un relation de Bezout, il existe $(W, R) \in \mathbb{K}[X]^2$ tel que $PW + QR = 1$. Ainsi, en appliquant u puis en évaluant en x, on a :

$$PW(u)(x) + QR(u)(x) = x$$

et donc $x = 0$ et $\mathrm{Ker}(P(u)) \cap \mathrm{Ker}(Q(u)) = \{0\}$. De plus, on a $(PQ)(u) = (QP)(u)$ et donc $\mathrm{Ker}(P(u)) \subset \mathrm{Ker}(PQ(u))$ et de même $\mathrm{Ker}(Q(u)) \subset \mathrm{Ker}(PQ(u))$, d'où une inclusion :

$$\mathrm{Ker}(P(u)) + \mathrm{Ker}(Q(u)) \subset \mathrm{Ker}((PQ)(u)).$$

Montrons l'inclusion réciproque : Soit $x \in \mathrm{Ker}(PQ(u))$, on écrit :

$$x = PW(u)(x) + QR(u)(x),$$

Posons $y = PW(u)(x)$ et $z = QR(u)(x)$. Montrons que $y \in \mathrm{Ker}(Q(u))$. On a $Q(u)(y) = QPW(u)(x) = W(u) \circ PQ(u)(x) = 0$ et de même $z \in \mathrm{Ker}(P(u))$, ce qui conclut. □

Le lemme admet la généralisation suivante :

kern2 **Corollaire 1.1.3.** *Soient $P_1, \ldots, P_s \in \mathbb{K}[X]$ deux à deux premiers entre eux, $f \in \mathcal{L}(E)$, alors :*

$$\mathrm{Ker}((P_1 \ldots P_s)(f)) = \bigoplus_{i=1}^{s} \mathrm{Ker}(P_i(f)).$$

Si de plus $(P_1 \ldots P_s)(f) = 0$, alors pour tout $i \in [\![1, s]\!]$, les projections $\pi_i : \mathrm{Ker}((P_1 \ldots P_s)(f)) \to \mathrm{Ker}(P_i(f))$ sont des polynômes en f.

Démonstration. On procède par récurrence sur s. Si $s = 1, 2$, c'est le lemme précédent. Si $s \geqslant 2$, alors comme les P_i sont deux à deux premiers entre eux, P_s est premier avec $P_1 \ldots P_{s-1}$, donc le cas $s = 2$, donne :

$$\mathrm{Ker}((P_1 \ldots P_s)(f)) = \bigoplus_{i=1}^{s} \mathrm{Ker}(P_i(f)),$$

et on applique l'hyothèse de récurrence à $P_1 \ldots P_{s-1}$ pour obtenir :

$$\mathrm{Ker}((P_1 \ldots P_s)(f)) = \bigoplus_{i=1}^{s} \mathrm{Ker}(P_i(f)),$$

comme souhaité. Pour l'assertion sur les projecteurs, fixons $i \in [\![1, s]\!]$, soit $R_i = \prod_{j \neq i} P_j$, alors R et P_i sont premiers entre eux, on écrit donc une relation de Bezout,

$$1 = UR_i + HP_i$$

Soit $\pi_i := (UR_i)(f)$, c'est bien un polynôme en f. Soit $x \in E$, alors $P_i(\pi_i(f)(x)) = UP_iR_i(f)(x) = 0$ donc $\mathrm{Im}(\pi_i) \subset \mathrm{Ker}(P_i(f))$. De plus, on a aussi $\pi_i(HP_i(f)(x)) = 0$, donc comme :

$$x = \pi_i(x) + HP_i(f)(x), \tag{1.1.3.1}$$ {ker3}

en appliquant à nouveau π_i, on trouve :

$$\forall\ x \in E, \pi_i(x) = \pi_i^2(x),$$

et π_i est un projecteur. Enfin, on a exactement $\mathrm{Im}\,\pi_i = \mathrm{Ker}(P_i(f))$, puisque si $x \in \mathrm{Ker}(P_i(f))$ dans (ker3 1.1.3.1), on trouve $x = \pi_i(x)$. □

1.2. Valeurs propres et vecteurs propres. Soit E un $\mathbb{K}$ espace vectoriel et $u \in \mathcal{L}(E)$.

Définition 1.2.1. Soit $\lambda \in \mathbb{K}$, on dit que λ est une valeur propre de u s'il existe $x \in E - \{0\}$ tel que $u(x) = \lambda x$. On dit alors que x est un vecteur propre. En particulier, si λ est une valeur propre, $u - \lambda\,\mathrm{Id}$ n'est pas injectif. Pour $\lambda \in \mathbb{K}$, on appelle sous-espace propre de u associé à λ, l'espace vectoriel $\mathrm{Ker}(u - \lambda\,\mathrm{Id}_E)$. On note $\mathrm{Sp}(u)$, l'ensemble des valeurs propres de u, on l'appelle le spectre de u.

vp1 **Remarque 1.2.2.** Si $\lambda_1, \ldots, \lambda_s \in \mathbb{K}$ sont deux à deux distincts, alors les $X - \lambda_i$ sont deux à deux premiers entre eux, d'où par le lemme des noyaux (kern2 1.1.3) :

$$\mathrm{Ker}(\prod_{i=1}^{s}(f - \lambda_i\,\mathrm{Id}_E)) = \bigoplus_{i=1}^{s}\mathrm{Ker}(u - \lambda_i\,\mathrm{Id}_E).$$

Ainsi, comme $\mathrm{Ker}(\prod_{i=1}^{s}(f - \lambda_i\,\mathrm{Id}_E)) \subset E$, on en déduit que si E est de dimension n, u admet au plus n valeurs propres.

1.3. Cas des matrices. Soit $n \in \mathbb{N}$, sur $\mathcal{L}(\mathbb{K}^n)$, on a une structure d'anneau, donnée par l'addition et la composition des endomorphismes. De même, $M_n(\mathbb{K})$, on a une structure d'anneau non-commutatif donnée par l'addition et la multiplication de matrices. On a un isomorphisme canonique de $\mathbb{K}$-espaces vectoriels :

$$\Phi : \mathcal{L}(\mathbb{K}^n) \to M_n(\mathbb{K}), \tag{1.3.0.1}$$ {endM}

qui envoie u sur $\mathrm{Mat}_B(u)$ où B est la base canonique. De plus, cet isomorphisme est aussi un isomorphisme d'anneaux qui envoie la composition des endomorphismes sur la multiplication matricielle. Ainsi pour tout $P \in \mathbb{K}[X]$ et $u \in \mathcal{L}(E)$, on a :

$$\Phi(P(u)) = P(\Phi(u)).$$

Cet isomorphisme nous permettra de traduire les énoncés sur les endomorphismes en énoncés matriciels et vice versa.

Ainsi pour $M \in M_n(\mathbb{K})$, on dit que $X \in \mathbb{K}^n$ non-nul est un *vecteur propre* de *valeur propre* λ si $MX = \lambda X$. On a alors de même la notion de sous-espace propre donné par $\mathrm{Ker}(M - \lambda I_n)$.

2. Diagonalisation

2.1. Critère de diagonalisation.

Définition 2.1.1. Soit $\mathbb{K}$ un corps, E un $\mathbb{K}$-espace vectoriel de dimension finie.

1. Soit $u \in \mathcal{L}(E)$, il est dit diagonalisable s'il existe une base B de E tel que $\mathrm{Mat}_B(u)$ est diagonale.
2. Soit $M \in M_n(\mathbb{K})$, elle est diagonalisable s'il existe $P \in GL_n(\mathbb{K})$ tel que PMP^{-1} est diagonale.

Remarques.

2.1.2. Pour rappel deux matrices $A, B \in M_n(\mathbb{K})$ sont dites semblables ou conjuguées s'il existe $Q \in GL_n(\mathbb{K})$ tel que $A = QBQ^{-1}$.

2.1.3. Etant donné que le changement de base revient à la conjugaison par la matrice de passage, on obtient que les deux notions coïncident via l'isomorphisme (endM I.3.0.1) entre matrices et endomorphismes.

Un des avantages des matrices diagonales est qu'il est aisé de calculer des polynômes matriciels, en effet si on a :

$$D = \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{bmatrix},$$

alors pour tout $k \in \mathbb{N}$, on a :

$$D^k = \begin{bmatrix} d_1^k & & \\ & \ddots & \\ & & d_r^k \end{bmatrix},$$

et par linéarité, on obtient que pour tout $P \in \mathbb{K}[X]$, on a :

$$P(D) = \begin{bmatrix} P(d_1) & & \\ & \ddots & \\ & & P(d_r) \end{bmatrix}.$$

diag1 **Théorème 2.1.4.** *Soit E un $\mathbb{K}$-espace vectoriel de dimension n, $u \in \mathcal{L}(E)$, les assertions suivantes sont équivalentes :*

(i) *u est diagonalisable.*

(ii) *Il existe une base de vecteurs propres de E.*

(iii) *On a une décomposition en somme directe $E = \bigoplus_{\lambda \in \mathrm{Sp}(u)} E_\lambda$.*

(iv) *Le polynôme caractéristique χ_u est scindé et $\dim E_\lambda = m(\lambda)$, où $m(\lambda)$ est la multiplicité de λ dans χ_u.*

(v) *Il existe $P \in \mathbb{K}[X]$, scindé à racines simples, tel que $P(u) = 0$.*

DÉMONSTRATION. $(i) \iff (ii)$, si $B = (x_1, \ldots, x_n)$ la base dans laquelle $\mathrm{Mat}_B(u)$ est diagonale de coefficients diagonaux λ_i, alors $u(x_i) = \lambda_i x_i$ et les x_i sont des vecteurs propres, Réciproquement dans une base de vecteurs propres, la matrice de u est diagonale, donc u diagonalisable.

$(ii) \iff (iii)$ est clair, si $(x_1, \ldots, x_n)$ est une base de vecteurs propres, de valeurs propres distinctes $\lambda_1, \ldots, \lambda_s$. Pour chaque λ_i, soit $E_k = \mathrm{Vect}(x_{k_1}, \ldots, x_{k_i})$ où les x_{k_l} sont de valeur propre λ_i. On a alors $E = \bigoplus_{k=1}^{s} E_k \subset \bigoplus_{\lambda \in \mathrm{Sp}(u)} E_\lambda \subset E$, d'où l'égalité. En particulier, on a $E_k = E_{\lambda_k}$. Réciproquement, si $E = \bigoplus_{\lambda \in \mathrm{Sp}(u)} E_\lambda$, il suffit de prendre pour chaque $\lambda \in \mathrm{Sp}(u)$, une base B_λ de E_λ alors la base $\bigcup \lambda \in \mathrm{Sp}(u) B_\lambda$ est une base de vecteurs propres.

$(ii) \Longrightarrow (iv)$. Dans une base de vecteurs propres B dans laquelle $\mathrm{Mat}_B(u) = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, on obtient :

$$\chi_u = \prod_{i=1}^{n} (X - \lambda_i) = \prod_{i=1}^{s} (X - \lambda_i)^{m(\lambda_i)}$$

où les $\lambda_1, \ldots, \lambda_s$ sont deux à deux distincts dans le dernier produit et $m_{\lambda_i} = \dim(E_{\lambda_i})$.

$(iv) \Longrightarrow (v)$. Si χ_u est scindé, on l'écrit $\chi_u = \prod_{i=1}^{s} (X - \mu_i)^{m_i}$, avec les μ_i distincts. Comme $\deg \chi_u = n$, on a $\sum_{i=1}^{s} m_i = n$. Soit $P = \prod_{i=1}^{s} (X - \mu_i)$, alors il est scindé à racines simples. Il suffit de montrer que $P(u) = 0$, par le lemme des noyaux, on a :

$$\mathrm{Ker}(P(u)) = \bigoplus_{i=1}^{s} E_{\mu_i}.$$

Or par hypothèse, on a $\dim E_{\mu_i} = m_i$, soit $\dim(\mathrm{Ker}(P(u)) = \sum_{i=1}^{s} m_i = n$ et $\mathrm{Ker}(P(u)) = E$, donc $P(u) = 0$ comme souhaité.

$(v) \Longrightarrow (iii)$. Si P est annulateur à racines simples, on écrit $P = \prod_{i=1}^{s} (X - \mu_i)$, on a $P(u) = 0$, d'où $\mathrm{Ker}(P(u)) = 0$ et en appliquant le lemme des noyaux kern2 1.1.3, on trouve $E = \bigoplus E_{\mu_i}$. □

D-nilp **Corollaire 2.1.10.** *Soit $u \in \mathcal{L}(E)$, on suppose u diagonalisable et nilpotent (i.e. il existe $r \in \mathbb{N}, u^r = 0$), alors $u = 0$.*

DÉMONSTRATION. Si u est diagonalisable, il admet une base de vecteurs propres. Montrons que la seule valeur propre de u est 0 et alors, dans cette base (et donc dans toutes), la matrice de u sera la matrice nulle. Soit λ une valeur propre de u, alors si x est un vecteur propre non-nul, on a $u(x) = \lambda.x$, soit $u^r(x) = \lambda^r x = 0$ donc $\lambda = 0$ et $u = 0$. □

2.2. Espaces stables et codiagonalisation. Soit un $\mathbb{K}$ espace vectoriel E, $F \subset E$ un sous-espace vectoriel et $u \in \mathcal{L}(E)$, on dit que F est stable si $u(F) \subset F$. Dans ce cas, il induit alors un endomorphisme $u_{|F} \in \mathcal{L}(F)$, on parle d'*endomorphisme induit*.

res **Lemme 2.2.1.** *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$ diagonalisable, $F \subset E$ un sous-espace stable, alors $u_{|F}$ est diagonalisable. Si de plus $E = F \oplus G$ avec F, G stables par u alors u diagonalisable si et seulement si $u_{|F}$ et $u_{|G}$ le sont.*

Démonstration. D'après diag1 2.1.4, il existe un polynôme annulateur scindé à racines simples tel que $P(u) = 0_E$ et en particulier, comme F est stable par u, on a aussi $P(u_{|F}) = 0_F$ et donc $u_{|F}$ est diagonalisable d'après diag1 2.1.4. Pour la deuxième assertion, on a déjà montré le sens direct, pour la réciproque, il suffit de considérer $B_F \cup B_G$ l'union de deux bases de diagonalisation pour $u_{|F}$ et $u_{|G}$. □

stab1 **Lemme 2.2.2.** *Soient $u, v \in \mathcal{L}(E)$ tels que $u \circ v = v \circ u$, alors les sous-espaces propres de u sont stables par v.*

Démonstration. Soit $\lambda \in \mathbb{K}$ et $x \in E_\lambda$, on a $u(v(x)) = v(u(x)) = v(\lambda x) = \lambda v(x)$ et $v(x) \in E_\lambda$. □

On déduit de ce lemme l'énoncé suivant :

codiag **Théorème 2.2.3.** *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, soit $\mathcal{A}$ une partie de $\mathcal{L}(E)$ constituée d'éléments diagonalisables qui commutent deux à deux, alors ils sont codiagonalisables, i.e. diagonalisables dans la même base.*

Démonstration. On procède par récurrence forte sur $n = \dim E$. Si $n = 0, 1$, c'est clair, si $n \geqslant 1$, on considère deux cas. Si $\mathcal{A} = \mathbb{K}.\mathrm{Id}_E$, c'est évident, sinon si $\mathcal{A} \nsubseteq \mathbb{K}.\mathrm{Id}_E$, soit $f \in \mathcal{A}$ avec $f \neq \mathbb{K}\,\mathrm{Id}_E$. Soit $\lambda \in \mathbb{K}$ une valeur propre de f, comme f n'est pas une homothétie, on a $\dim(E_\lambda) < n$, on pose alors $G = \bigoplus_{\mu \in \mathrm{Sp}(f), \mu \neq \lambda} G_\mu$.
On a $E = E_\lambda \oplus G$ et il résulte de stab1 2.2.2 que tous les éléments de $\mathcal{A}$ stabilisent E_λ et G et sont codiagonalisables lorsque que l'on les restreint à ces sous-espaces d'après res 2.2.1. Il existe alors des bases B_{E_λ} et B_G de E_λ et G dans lesquelles tous les élements induits de $\mathcal{A}$ sont diagonalisables, il suffit alors de prendre la base $B = B_{E_\lambda} \cup B_G$ pour conclure. □

Voyons une application de cet énoncé :

Exemple 2.2.4. Soit $G \subset GL_n(\mathbb{C})$ un groupe commutatif d'exposant fini, i.e. il existe $N \in \mathbb{N}^*$ tel que pour tout $g \in G$, $g^N = I_n$, alors G est fini.

Démonstration. En effet, $X^N - 1$ est scindé à racines simples, donc comme G est d'exposant fini, on obtient que tout élément $g \in G$ est diagonalisable. Comme de plus, G est

commutatif, d'après codiag 2.2.3 les éléments sont codiagonalisables de valeurs propres des racines N-ièmes de l'unité, il y a donc au plus N^n possibilités et G est fini. □

Remarque 2.2.5. Le résultat reste vrai sans l'hypothèse que G est commutatif, c'est le théorème de Burnside.

3. Trigonalisation

Après les matrices diagonales, les matrices les plus agréables sont les matrices triangulaires et même par transposition, on peut se ramener à des matrices triangulaires supérieures, ce que l'on fera dans la suite. Ce qui est particulièrement agréable est que sur un corps algébriquement clos, toute matrice peut se mettre sous forme triangulaire supérieure. On commence la section par rappeler les propriétés de base des matrices triangulaires supérieures.

Dans toute, la section, on se donne E un $\mathbb{K}$-espace vectoriel de dimension finie.

3.1. Matrices triangulaires. Notons $T_n(\mathbb{K}) \subset M_n(\mathbb{K})$ le sous-espace vectoriel des matrices triangulaires supérieures. Il est de dimension $\frac{n(n+1)}{2}$.

T-alg **Proposition 3.1.1.** *Pour tout $B, C \in T_n(\mathbb{K})$, $BC \in T_n(\mathbb{K})$ et si $B \in GL_n(\mathbb{K}) \cap T_n(\mathbb{K})$, $B^{-1} \in T_n(\mathbb{K})$.*

Démonstration. Pour la première assertion, on peut le faire par calcul matriciel, il est cependant plus commode de prendre le point de vue des endomorphismes. Soit alors $(e_1, \dots, e_n)$ la base canonique et u et v les endomorphismes associés à B et C. Comme B et C sont triangulaires supérieures, on a donc que :

$$\forall\ i \in [\![1, n]\!], u(e_i), v(e_i) \in \mathrm{Vect}(e_k)_{1 \leqslant k \leqslant i}$$

On obtient donc immédiatement que :

$$\forall\ i \in [\![1, n]\!], u(v(e_i)) \subset u(\mathrm{Vect}(e_k)_{1 \leqslant k \leqslant i}) \subset \mathrm{Vect}(e_k)_{1 \leqslant k \leqslant i}.$$

Et $\mathrm{Mat}_B(u \circ v)$ est triangulaire supérieure. Pour la deuxième assertion, d'après pol 7.1.3, on sait que B^{-1} est un polynôme en B et donc comme $T_n(\mathbb{K})$ est un $\mathbb{K}$-espace vectoriel stable par multiplication, on a $\mathbb{K}[B] \subset T_n(\mathbb{K})$ et $B^{-1} \in T_n(\mathbb{K})$. □

Au moins pour les coefficients diagonaux, il est aisé de calculer des polynômes de matrices triangulaires supérieures. En effet si :

$$M = \begin{pmatrix} \lambda_1 & \cdots & \cdots & * \\ 0 & \lambda_2 & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$$

alors pour tout $P \in \mathbb{K}[X]$, on a :

$$P(M) = \begin{pmatrix} P(\lambda_1) & \cdots & \cdots & * \\ 0 & P(\lambda_2) & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & P(\lambda_n) \end{pmatrix}$$

nilp **Proposition 3.1.2.** *Soit $B \in T_n(\mathbb{K})$ une matrice dont les coefficients diagonaux sont nuls, alors B est nilpotente et $B^n = 0$.*

DÉMONSTRATION. On peut le vérifier par calcul matriciel, mais on peut le faire sans effort. Les valeurs propres de B sont ses coefficients diagonaux, comme ils sont nuls, on obtient d'après sp1 7.0.2 que $\chi_B = X^n$ et on applique Cayley-Hamilton. □

3.2. Endomorphismes trigonalisables.

Définition 3.2.1.

1. Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$, alors u est trigonalisable s'il existe une base B dans laquelle Mat_B est triangulaire supérieure.
2. Soit $M \in M_n(\mathbb{K})$, alors elle est dite trigonalisable si elle est semblable à une matrice triangulaire supérieure.

Remarque 3.2.2. A nouveau les deux notions sont compatibles, via l'isomorphisme $\mathrm{End}(\mathbb{K}^n) \xrightarrow{\sim} M_n(\mathbb{K})$.

inf1 **Lemme 3.2.3.** *Si $M \in M_n(\mathbb{K})$ est triangulaire inférieure, alors elle est semblable à une matrice triangulaire supérieure.*

DÉMONSTRATION. Notons $T_n^{(1)}(\mathbb{K})$ l'espace vectoriel des matrices triangulaires inférieures. Soit la matrice $D = \mathrm{antidiag}[1, \ldots, 1]$ qui correspond au changement de base $(e_1, \ldots, e_n) \to (e_n, \ldots, e_1)$, alors l'isomorphisme de $M_n(\mathbb{K})$ donné par $M \mapsto DMD^{-1}$ envoie $T_n(\mathbb{K})$ sur $T_n^{(1)}(bK)$. □

Définition 3.2.4. On appelle drapeau de E toute suite de sous-espaces vectoriels :

$$\{0\} = E_0 \subset E_1 \subset \cdots \subset E_n = E,$$

avec $\dim(E_i) = i$. On note $(E_\bullet)$ une telle suite.

Pour un drapeau $(E_\bullet)$ de E et $u \in \mathcal{L}(E)$, on dit que u stabilise $(E_\bullet)$ si pour tout i, $u(E_i) \subset E_i$.

drap **Lemme 3.2.5.** *Soit $u \in \mathcal{L}(E)$, alors u est trigonalisable si et seulement si u stabilise un drapeau $(E_\bullet)$.*

Démonstration. Si $B = (e_1, \dots, e_n)$ est une base qui trigonalise u, alors il suffit de prendre pour $i \in [\![1, n]\!]$, $E_i = \mathrm{Vect}(x_k)_{1 \leqslant k \leqslant i}$. Réciproquement, si u stabilise un drapeau $(E_\bullet)$, pour tout $i \in [\![1, n]\!]$, E_{i-1} est un hyperplan de E_i de telle sorte que l'on a :

$$E_i = E_{i-1} \oplus \mathbb{K} u_i$$

avec $u_i \neq 0$ et il suffit d'écrire u dans la base $B = (u_1, \dots, u_n)$. □

3.3. Critères de trigonalisation.

trig **Théorème 3.3.1.** *Pour E un $\mathbb{K}$-espace vectoriel de dimension finie, soit $u \in \mathcal{L}(E)$, les assertions suivantes sont équivalentes :*

(i) *u est trigonalisable.*

(ii) *χ_u est scindé.*

(iii) *Il existe $P \in \mathbb{K}[X]$ scindé tel que $P(u) = 0$.*

Démonstration. $(i) \Longrightarrow (ii)$ Si u est trigonalisable de valeurs propres λ_i, alors pour calculer son polynôme caractéristique, il suffit de le faire dans une base de trigonalisation et on a :

$$\chi_u = \prod_{i=1}^{n} (X - \lambda_i)$$

et χ_u scindé. On a clairement $(ii) \Longrightarrow (iii)$ par Cayley-Hamilton. Montrons $(iii) \Longrightarrow (i)$, soit P scindé tel que $P(u) = 0$.

hyp **Lemme 3.3.2.** *Il existe un hyperplan H de E stable par u.*

Démonstration. On a $P(u) = P({}^t u) = 0$, comme P est scindé, on l'écrit $P = \prod_{i=1}^{n} (X - \lambda_i)$, ainsi on a :

$$({}^t u - \lambda_1 \mathrm{Id}_E) \circ \cdots \circ ({}^t u - \lambda_n \mathrm{Id}_E) = 0.$$

Donc il existe i_0 tel que ${}^t u - \lambda_{i_0} \mathrm{Id}$ ne soit pas injective, donc λ_{i_0} est une valeur propre de ${}^t u$. Soit $f \in E^\vee$ un vecteur propre de ${}^t u$ associé à λ_{i_0}, alors on prend $H = (f)^\circ$, c'est bien un hyperplan d'après perp1 1.5.4, montrons qu'il est stable par x, on a par définition :

$$H = \{x \in E, \langle x, f \rangle = 0\}.$$

On a alors :

$$\langle u(x), f \rangle = \langle x, {}^t u(f) \rangle = \langle x, \lambda f \rangle = 0$$

et $u(x) \in H$. □

Terminons maintenant la preuve. On procède par récurrence sur $n = \dim(E)$. Si $n = 0, 1$, c'est clair. Passons de n à $n+1$. Soit H un hyperplan stable de f, alors $P(f_{|H}) = 0$ donc $f_{|H}$ est trigonalisable par hypothèse de récurrence, soit $(\epsilon_2, \ldots, \epsilon_n)$ une base de trigonalisation de H, soit ϵ_1 tel que :

$$E = \mathbb{K}\epsilon_1 \oplus H,$$

alors dans la base $(\epsilon_1, \ldots, \epsilon_n)$, la matrice est triangulaire inférieure donc f trigonalisable d'après 3.2.3. □

res2 **Corollaire 3.3.3.** *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, $u \in \mathcal{L}(E)$ trigonalisable, $F \subset E$ un sous-espace stable, alors $u_{|F}$ est trigonalisable. Si de plus $E = F \oplus G$ avec F, G stables par u alors u trigonalisable si et seulement si $u_{|F}$ et $u_{|G}$ le sont.*

Démonstration. Si u est trigonalisable, il annule un polynôme scindé P, donc $P(u) = 0_E$ et comme F est stable, on a $P(u_{|F}) = 0_F$ et $u_{|F}$ diagonalisable d'après 3.3.1.

Pour la deuxième assertion, le sens direct vient d'être vu et pour le sens réciproque on prend l'union de deux bases de trigonalisation. □

Définition 3.3.4. Soit $u \in \mathcal{L}(E)$, il est dit nilpotent s'il existe $r \in \mathbb{N}$ tel que $u^r = 0$. On appelle indice de nilpotence, le plus petit entier r tel que $u^r = 0$.

nilp2 **Corollaire 3.3.5.** *Soit $u \in \mathcal{L}(E)$ un endomorphisme nilpotent, alors il est trigonalisable. De plus, dans une base de trigonalisation, la matrice a ses coefficients diagonaux nuls.*

Démonstration. On a par définition $u^r = 0$, donc u annule un polynôme scindé donc est trigonalisable d'après 3.3.1. Une fois mis sous forme triangulaire supérieure T_u, soit λ une valeur propre de u, alors si x est un vecteur propre non-nul, on a $u(x) = \lambda.x$, soit $u^r(x) = \lambda^r x = 0$ donc $\lambda = 0$ et donc les coefficients diagonaux de T_u sont nuls. □

Corollaire 3.3.6. *Soit $\mathbb{K}$ algébriquement clos, alors tout $u \in \mathcal{L}(E)$ est trigonalisable.*

Démonstration. Comme $\mathbb{K}$ est algébriquement clos, pour tout $u \in \mathcal{L}(E)$, χ_u est scindé, donc u trigonalisable d'après 3.3.1. □

Corollaire 3.3.7. *Soit $u \in \mathcal{L}(E)$, $\lambda_1, \ldots, \lambda_n$ les racines de χ_u sur une clôture algébrique, on a :*

$$\mathrm{Tr}(u) = \sum_{i=1}^{n} \lambda_i, \det(u) = \prod_{i=1}^{n} \lambda_i.$$

Plus généralement pour $i \in [\![1, n]\!]$, le coefficient $c_i(u)$ de X^{n-i} de χ_u est le i-ème polynôme symétrique en les λ_k :

$$c_i(u) = (-1)^i \sum_{1 \leqslant k_1 < \cdots < k_i \leqslant n} \lambda_{k_1} \ldots \lambda_{k_i}.$$

DÉMONSTRATION. En effet, on se place sur une clôture algébrique $\overline{\mathbb{K}}$ de $\mathbb{K}$. Dans ce cas, u est trigonalisable de coefficients diagonaux ses valeurs propres $\lambda_1, \ldots, \lambda_n$ et $\chi_u = \prod_{j=1}^{n}(X-\lambda_j)$ et il suffit de développer le polynôme. □

Remarque 3.3.8. On rappelle que χ_u est invariant par conjugaison (7.0.5) de telle sorte que ses coefficients le sont aussi. Dans le cas de la trace et du déterminant, cela vient du fait que $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$ et $\det(AB) = \det(A)\det(B)$. En rechanche, pour les $c_i(u)$ avec $i \neq 1, n$, il n'est pas évident que la formule donnée en fonction des valeurs propres soit invariante.

cotrig **Théorème 3.3.9.** *Soit E un $\mathbb{K}$-espace vectoriel de dimension finie, soit $\mathcal{A}$ une partie de $\mathcal{L}(E)$ constituée d'éléments trigonalisables qui commutent deux à deux, alors ils sont cotrigonalisables, i.e. trigonalisables dans la même base.*

DÉMONSTRATION. C'est exactement la même preuve que dans le cas diagonalisable. □

Une autre application de 3.3.1 le théorème suivant :

DZ **Théorème 3.3.10.** *Les matrices diagonalisables sont denses dans $M_n(\mathbb{C})$.*

DÉMONSTRATION. Soit A une matrice de $M_n(\mathbb{C})$, quitte à la trigonaliser, on peut supposer qu'elle est triangulaire supérieure de valeurs propres $\lambda_1, \ldots, \lambda_s$. qui apparaîssent avec des multiplicités $m_1, \ldots, m_s$. Soit $\mu = \min\{|\lambda_i - \lambda_j|, i \neq j\}$. On prend alors la matrice A_n dont les coefficients diagonaux sont les $\lambda_i + \frac{\mu}{ip}$ et où les autres coefficients sont les mêmes que A. On a clairement $A_p \to A$ quand $p \to +\infty$ et A_p est diagonalisable d'après 2.1.4, car ses valeurs propres sont distinctes, donc χ_{A_p} est scindé à racines simples. □

4. Polynôme minimal

On a toujours E un $\mathbb{K}$-espace vectoriel de dimension finie.

4.1. Idéaux de $\mathbb{K}[X]$.

Définition 4.1.1. Soit A un anneau commutatif, on dit que $I \subset A$ est un idéal si $(I, +)$ est un sous-groupe et si :

$$\forall\ a \in A, a.I = \{ax, x \in I\} \subset I.$$

Remarques.

4.1.2. Si I est un idéal et $1 \in I$, alors $I = A$, puisque pour tout $a \in A$, $a = a.1 \in I$.

4.1.3. En particulier, pour tout $a \in A$, $aA = \{ax, a \in A\}$ est un idéal de A, on le note (a) et on dit que cet idéal est principal.

4.1.3. Plus généralement, si $(a_1, \dots, A_r) \in A^r$, on note $(a_1, \dots, a_r)$ l'idéal engendré par ces éléments, il consiste en les combinaisons $\sum_{i=1}^{r} a_i x_i$ avec les x_i dans A.

princ **Proposition 4.1.4.** *Soit $\mathbb{K}$ un corps, alors tout idéal de $\mathbb{K}[X]$ est principal et admet un unique générateur unitaire.*

Remarque 4.1.5. C'est une des propriétés principales auxquelles on faisait allusion qui ne marche pas en général, si on prend $\mathbb{Z}[X]$, alors l'idéal (p, X) n'est plus principal.

Démonstration. Soit $I \subset \mathbb{K}[X]$ un idéal non-nul, soit $P \in I$ non-nul de degré minimal d. Si $d = 0$, alors P est une constante inversible et $I = A$, sinon, montrons que $I = (P)$. Soit $Q \in I$, on effectue la division euclidienne de Q par P, soit $Q = PB + R$ avec $\deg(R) < d$. Si $R \neq 0$, alors $Q - PB \in I$, donc $R \in I$ et est de degré strictement inférieur à d, ce qui contredit sa minimalité et $I = (P)$. Enfin, la preuve donne que tous les générateurs de I sont de même degré, donc diffèrent d'une constante, ainsi I admet un unique générateur unitaire. □

rac **Lemme 4.1.6.** *Soit $u \in \mathcal{L}(E)$, λ une valeur propre de u, pour $P \in \mathbb{K}[X]$ tel que $P(u) = 0$, on a $P(\lambda) = 0$.*

Démonstration. Soit x un vecteur propre non-nul, alors $u(x) = \lambda x$, et $P(u)(x) = P(\lambda)x = 0$, d'où $P(\lambda) = 0$, comme x non-nul. □

ex-min **Proposition 4.1.7.** *Soient $u \in \mathcal{L}(E)$ et $x \in E$, alors les ensembles $I_u = \{P \in \mathbb{K}[X], P(u) = 0\}$ et $I_u(x) = \{P \in \mathbb{K}[X], P(u)(x) = 0\}$ sont des idéaux de $\mathbb{K}[X]$, en particulier, il sont principaux. Soient μ_u et $\mu_{u,x}$ les générateurs unitaires, on les appelle polynôme minimal et polynôme minimal ponctuel de u. On a $\mu_{u,x}|\mu_u|\chi_u$.*

Remarque 4.1.8. On appelle I_u l'ensemble des polynômes annulateurs de u.

Démonstration. Les ensembles I_u et $I_u(x)$ sont clairement des sous-groupes et pour $P \in I_u$ (resp. $P \in I_u(x)$) et $Q \in \mathbb{K}[X]$, alors $QP(u) = Q(u) \circ P(u) = 0$ (resp. $QP(u)(x) = Q(u) \circ P(u)(x) = 0$, donc $QP \in I_u$ (resp. $QP \in I_u(x)$), donc I_u et $I_u(x)$ sont des idéaux, donc sont principaux d'après princ 4.1.4. Enfin, par Cayley Hamilton, $\chi_u \in I_u$ donc $\mu_u|\chi_u$ et comme $\mu_u(u)(x) = 0$, on a aussi $\mu_{u,x}|\mu_u$. On sait déjà que les racines de χ_u sont les valeurs propres de u, le lemme rac 4.1.6 nous dit que ce sont exactement les racines de μ_u. □

Exemple 4.1.9. Soit u nilpotent dans $\mathcal{L}(E)$, alors si $n = \dim(E)$, on a $\chi_u = X^n$ et si r est l'indice de nilpotence de u, on a $\mu_u = X^r$. De même si u est diagonalisable de valeurs propres λ_i avec $m_i = \dim(E_{\lambda_i})$, alors $\mu_u = \prod(X - \lambda_i)$ et $\chi_u = \prod(X - \lambda_i)^{m_i}$.

Exemple 4.1.10. Si $P \in \mathbb{K}[X]$ est unitaire de degré n, soit $C_P \in M_n(\mathbb{K})$ sa matrice compagnon, alors d'après 7.2.1, $(e_1, C_P e_1, \ldots, C_P^{n-1} e_1)$ est une base de $\mathbb{K}^n$ et on trouve alors que $\mu_{C_P,e_1} = \mu_{C_P} = \chi_{C_P}$, puisqu'ils sont tous unitaires de degré n et se divisent successivement.

deg **Lemme 4.1.11.** *Soit $M \in M_n(\mathbb{K})$, alors on a $\deg(\mu_M) = \mathrm{rg}((A^k)_{k\in\mathbb{N}})$.*

Démonstration. La minimalité du polynôme minimal implique que son degré est précisément le plus petit entier $r \in \mathbb{N}$ tel que $(I_n, A, \ldots, A^r)$ est liée, ainsi $(I_n, A, \ldots, A^{r-1})$ est libre et on a $r = \mathrm{rg}((A^k)_{k\in\mathbb{N}}$. □

4.2. Invariance par extension de corps. On se donne une extension de corps $\mathbb{K} \subset \mathbb{L}$, a priori si $M \in M_n(\mathbb{K})$, le polynôme minimal peut changer suivant que l'on considère l'idéal I_u dans $\mathbb{K}[X]$ ou $\mathbb{L}[X]$, on va voir qu'il n'en n'est rien. On commence par un lemme.

Lemme 4.2.1. *Soient $X_1, \ldots, X_s$ des vecteurs de $\mathbb{K}^n$ alors, on a $\mathrm{rg}_{\mathbb{K}}[X_1, \ldots, X_s] = \mathrm{rg}_{\mathbb{L}}[X_1, \ldots, X_s]$.*

Démonstration. En effet, si on note $M \in M_{n,s}(\mathbb{K})$ la matrice de colonnes $X_1, \ldots, X_s$, si $r = \mathrm{rg}_{\mathbb{K}}[X_1, \ldots, X_s]$, alors par le théorème du rang, il existe $P, Q \in GL_n(\mathbb{K})$ telles que $M = PJ_rQ$ avec $J_r = \mathrm{diag}[1, \ldots, 1, 0, \ldots, 0]$ avec r fois un. Comme $GL_n(\mathbb{K}) \subset GL_n(\mathbb{L})$, on a $\mathrm{rg}_{\mathbb{L}}[X_1, \ldots, X_s] = r$. □

Théorème 4.2.2. *Soit $M \in M_n(\mathbb{K})$, alors on a $\mu_M^{\mathbb{K}} = \mu_M^{\mathbb{L}}$.*

Démonstration. On a déjà une inclusion d'idéaux annulateurs $I_M^{\mathbb{K}} \subset I_M^{\mathbb{L}} = \{P \in \mathbb{L}[X], P(M) = 0\}$, ce qui donne une relation de divisibilité $\mu_M^{\mathbb{L}} | \mu_M^{\mathbb{K}}$. Maintenant, on a d'après deg 4.1.11, $\deg(\mu_M^{\mathbb{L}}) = \mathrm{rg}_{\mathbb{L}}(A^k)_{k\in\mathbb{N}}$ qui d'après le lemme précédent est égal à $\mathrm{rg}_{\mathbb{K}}(A^k)_{k\in\mathbb{N}} = \deg(\mu_M^{\mathbb{K}})$. Ainsi, $\mu_M^{\mathbb{K}}$ et $\mu_M^{\mathbb{L}}$ sont de même degré et unitaires et comme $\mu_M^{\mathbb{L}} | \mu_M^{\mathbb{K}}$, on trouve $\mu_M^{\mathbb{K}} = \mu_M^{\mathbb{L}}$. □

5. Décomposition de Dunford

5.1. L'énoncé de réduction. Soit E un $\mathbb{K}$ espace vectoriel de dimension finie. Soit $u \in \mathcal{L}(E)$, on suppose χ_u scindé, il s'écrit alors :

$$\chi_u = \prod_{i=1}^{s} (X - \lambda_i)^{m_i}.$$

avec les λ_i deux à deux non-nuls.

On appelle *sous-espaces caractéristiques* les espaces vectoriels $F_i = \mathrm{Ker}((u - \lambda_i \mathrm{Id}_E)^{m_i})$. D'après Cayley-Hamilton et le lemme des noyaux, on a alors une décomposition canonique :

$$E = \bigoplus_{i=1}^{s} \mathrm{Ker}((u - \lambda_i \mathrm{Id}_E)^{m_i}).$$

dun **Théorème 5.1.1.** *[Décomposition de Dunford] Soit $u \in \mathcal{L}(E)$, on suppose χ_u scindé, alors u s'écrit de manière unique sous la forme $u = d + n$ où d est diagonalisable et n nilpotent avec $dn = nd$. Enfin, d et n sont des polynômes en u.*

Démonstration. On commence par montrer l'existence. On a :

$$E = \bigoplus_{i=1}^{s} \mathrm{Ker}((u - \lambda_i \mathrm{Id}_E)^{m_i}) = \bigoplus_{k=1}^{s} F_k.$$

Chaque F_k est stable par u et on a :

$$u_{|F_k} = \lambda_k \mathrm{Id}_{F_k} + (u - \lambda_k \mathrm{Id}_E)_{|F_k},$$

avec par définition $(u - \lambda_k \mathrm{Id}_{F_k})^{m_k}_{|F_k} = 0$, d'où une décomposition en diagonalisable plus nilpotent qui commutent. On définit alors d et n par :

$$\forall\ k \in [\![1, s]\!], d_k := d_{|F_k} = \lambda_k \mathrm{Id}_{F_k}, n_k = n_{|F_k} = u_{|F_k} - \lambda_k \mathrm{Id}_{F_k}\,.$$

Sur chaque F_k, d_k et n_k commutent, donc d et n commutent sur $E = \bigoplus_{i=1}^{s} F_k$; d est diagonalisable d'après res 2.2.1 puisqu'elle l'est sur chaque F_k et n nilpotent comme il l'est sur chaque F_k. Enfin, d'après kern2 1.1.3 les projections sur les espaces caractéristiques sont des polynômes en u, on obtient que d est un polynôme en u et donc n aussi, comme $u = d + n$.

Montrons l'unicité, supposons que l'on a $d + n = d' + n'$, alors $d - d' = n - n'$. Comme $f = d' + n'$ et que d' et n' commutent, d' et n' commutent avec f donc avec d et n comme ce sont des polynômes en f. Ainsi, d et d' sont codiagonalisables d'après codiag 2.2.3 et n et n' sont cotrigonalisables d'après milp2 3.3.5 et cotrig 3.3.9. Ainsi, $n - n' = d - d'$ est nilpotent et diagonalisable, donc nul d'après D-milp 2.1.10. Ainsi $n = n'$ et $d = d'$. □

En particulier, dans chaque espace caractéristique F_i, la matrice de u est donnée par :

$$M_i = \begin{pmatrix} \lambda_i & \cdots & \cdots & * \\ 0 & \lambda_i & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_i \end{pmatrix}$$

et ainsi en choisissant des bases dans chaque espace caractéristique, la matrice de u est alors diagonale par blocs :

$$\begin{bmatrix} M_1 & & \\ & \ddots & \\ & & M_s \end{bmatrix}.$$

Corollaire 5.1.2. *Si $\mathbb{K}$ est algébriquement clos, alors tout endomorphisme $u \in \mathcal{L}(E)$ admet une décomposition de Dunford.*

DÉMONSTRATION. En effet, comme $\mathbb{K}$ est algébriquement clos, χ_u est scindé. □

On a la version multiplicative, dite de Jordan-Chevalley :

Corollaire 5.1.3. *Soit $\gamma \in GL(E)$ sur un corps $\mathbb{K}$ algébriquement clos, alors on a une décomposition unique $\gamma = \gamma_s\gamma_u$, en diagonalisable et unipotent qui commutent.*

DÉMONSTRATION. On fait la décomposition de Dunford $\gamma = s + n$, comme γ inversible, on a que $s = \gamma - n$ est somme d'un inversible et d'un nilpotent qui commutent donc s est inversible. Posons alors $\gamma_u = Id + s^{-1}n$, alors γ_u est bien unipotent comme s et n commutent et il commute à s, en posant $\gamma_s = s$, on obtient donc que $\gamma = \gamma_u\gamma_s$.

Pour l'unicité, c'est analogue à la preuve de Dunford en utilisant qu'une matrice diagonalisable et unipotente est l'identité, ainsi que le fait que γ_u est aussi un polynôme en γ, puisque s^{-1} est un polynôme en s et que s. □