UFR MATHÉMATIQUES
Université Clermont Auvergne

Documents de synthèse sur quelques thèmes pour la préparation à l'Agrégation Interne

Ces 9 documents ont pour objet de regrouper sur quelques thèmes transversaux du progamme de l'Agrégation Interne les notions de bases et applications classiques relatives au sujet abordé. Ils ne visent pas à l'innovation dans le point de vue ni à l'originalité dans les applications évoquées, mais à l'efficacité pour les stagiaires préparant le concours en leur proposant une présentation organisée permettant une mise en ordre de leurs connaissances, complétée éventuellement par quelques ouvertures. En particulier, ils ne constituent nullement des plans de leçons pour les épreuves orales.

François DUMAS, juin 2023

Dualité en algèbre linéaire (cas de la dimension finie)

1. Notions de base sur les formes linéaires

Dans tout ce qui suit, on désigne par E un $\mathbb{K}$-espace vectoriel de dimension finie n.

1.1 - Espace dual

Définition. On appelle *forme linéaire* sur E toute application linéaire de E dans $\mathbb{K}$.

Exemples.
- L'application trace $A \mapsto \operatorname{Tr} A$ est une forme linéaire sur $\mathcal{M}_n(\mathbb{K})$,
- Si $f : \mathbb{R}^n \to \mathbb{R}$ est une application différentiable en un point a, alors la différentielle $d_a f$ est une forme linéaire sur $\mathbb{R}^n$.

Définition et proposition. On appelle *espace dual* de E, noté E^*, l'espace vectoriel des formes linéaires sur E. Il vérifie $\dim E^* = n$ et donc E^* est isomorphe à E.

Notation. Pour toute forme linéaire $\ell \in E^*$ et tout vecteur $v \in E$, on note :

$$\langle \ell, v \rangle = \ell(v) \in \mathbb{K}.$$

Le crochet ainsi défini est une forme bilinéaire $E^* \times E \to \mathbb{K}$, appelée *crochet de dualité*.

1.2 - Base duale

Proposition. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base de E.

(i) Pour tout $1 \leq i \leq n$, l'application $e_i^* : E \to \mathbb{K}$ qui, à tout vecteur $v = \sum_{i=1}^n x_i e_i$, associe le scalaire x_i est une forme linéaire ; elle est déterminée par :

$$\langle e_i^*, e_j \rangle = \delta_{i,j} \quad \text{pour tous } 1 \leq i, j \leq n.$$

(ii) La famille $\mathcal{B}^* = (e_1^*, \dots, e_n^*)$ est une base de E^*, *base duale* de $\mathcal{B}$, qui vérifie :

$$v = \sum_{i=1}^n \langle e_i^*, v \rangle e_i \quad \text{pour tout } v \in E, \quad \text{et} \quad \ell = \sum_{i=1}^n \langle \ell, e_i \rangle e_i^* \quad \text{pour tout } \ell \in E^*.$$

Preuve. Vérification directe des différents points. □

▶ *Remarques.*
1. L'application qui à tout vecteur $v = \sum_{i=1}^n x_i e_i$ de E associe la forme linéaire $\ell = \sum_{i=1}^n x_i e_i^*$ donne un isomorphisme explicite de E sur E^*.
2. Pour toute base $\mathcal{B}'$ de E^*, il existe une unique base $\mathcal{B}$ de E telle que $\mathcal{B}'$ soit la base duale de $\mathcal{B}$; on dit parfois que $\mathcal{B}$ est la base antéduale de $\mathcal{B}'$.

▶ *Exemples.*

1. Soit $E = \mathbb{K}^n$. Soit $\mathcal{B}$ une base de E. Les composantes des vecteurs de $\mathcal{B}$ par rapport à la base canonique de E sont données par les vecteurs colonnes d'une matrice carrée $n \times n$ inversible A. Alors les composantes des vecteurs de $\mathcal{B}^*$ par rapport à la base duale de la base canonique sont données par les vecteurs lignes de la matrice A^{-1}.
2. Polynômes d'interpolation de Lagrange. Soit $E = \mathbb{K}_n[X]$. Soient $a_0, a_1, \ldots, a_n$ une famille fixée d'éléments de $\mathbb{K}$ deux à deux distincts. On considère les formes linéaires $\ell_0, \ell_1, \ldots, \ell_n$ définies par $\ell_i(P) = P(a_i)$ pour tout $P \in E$ et tout $1 \leq i \leq n$. Alors la famille $(\ell_0, \ell_1, \ldots, \ell_n)$ est une base de E^* dont la base antéduale $(L_0, L_1, \ldots, L_n)$ est définie par : $L_i = \prod_{1 \leq j \leq n, j \neq i} \left(\frac{X - a_j}{a_i - a_j}\right)$. Tout polynôme $P \in E$ s'écrit donc $P(X) = \sum_{i=1}^n P(a_i) L_i(X)$.
3. Formule de Taylor. Soit $E = \mathbb{K}_n[X]$. Soient a un élément fixé de $\mathbb{K}$. On considère les formes linéaires $\ell_0, \ell_1, \ldots, \ell_n$ définies par $\ell_i(P) = P^{(i)}(a)$ pour tout $P \in E$ et tout $1 \leq i \leq n$. Alors la famille $(\ell_0, \ell_1, \ldots, \ell_n)$ est une base de E^* dont la base antéduale $(e_0, e_1, \ldots, e_n)$ est définie par : $e_i = \frac{(X-a)^i}{i!}$, ce qui traduit le fait que $\ell_k(e_j) = e_j^{(k)}(a)$ vaut 0 si $k \neq j$ et 1 si $k = j$. Tout polynôme $P \in E$ s'écrit donc $P(X) = \sum_{i=1}^n P^{(i)}(a) \frac{(X-a)^i}{i!}$.

1.3 - Bidual

Proposition.

(i) Pour tout $v \in E$, l'application $\varphi_v : E^* \to \mathbb{K}$ qui, à toute forme linéaire $\ell \in E^*$, associe le scalaire $\varphi_v(\ell) = \langle \ell, v \rangle$ est une forme linéaire sur E^* ;

(ii) L'application $\varphi : v \mapsto \varphi_v$ est un isomorphisme de l'espace vectoriel de E sur l'espace vectoriel bidual E^{**}.

Preuve. Le point (i) est évident. Pour (ii), il est clair que φ est linéaire et comme $\dim E = \dim E^* = \dim E^{**}$, il suffit de montrer que φ est injectif. Soit $v \in \operatorname{Ker} \varphi$. Il vérifie $\ell(v) = 0$ pour toute forme linéaire ℓ dans E^*. En particulier $e_i^*(v) = 0$ pour tout $1 \leq i \leq n$. Comme $e_i^*(v)$ n'est autre que la composante i-ième de v dans la base $\mathcal{B} = (e_1, \ldots, e_n)$, on conclut que $v = 0_E$. □

1.4 - Orthogonalité associée à la dualité

La bilinéarité du crochet de dualité défini en 1.1 permet d'introduire la notion suivante.

Proposition et définitions.

(i) Un vecteur $v \in E$ et une forme linéaire $\ell \in E^*$ sont dits *orthogonaux* lorsque $\langle \ell, v \rangle = 0$.

(ii) Pour toute partie A de E, on appelle *orthogonal de* A, noté $A^\perp$, le sous-espace vectoriel de E^* défini par $A^\perp = \{\ell \in E^* \,;\, \langle \ell, v \rangle = 0 \text{ pour tout } v \in A\}$.

(iii) Pour toute partie X de E^*, on appelle *orthogonal de* X, noté X°, le sous-espace vectoriel de E défini par $X^\circ = \{v \in E \,;\, \langle \ell, v \rangle = 0 \text{ pour tout } \ell \in X\}$.

Le fait que $A^\perp$ et X° sont des sous-espaces vectoriel est évident.

▶ *Exercice.* Pour toutes parties A et B de E, et toutes parties X et Y de E^*, on a :

$$\text{Si } A \subset B, \text{ alors } B^\perp \subset A^\perp, \qquad \text{Si } X \subset Y, \text{ alors } Y^\circ \subset X^\circ,$$
$$A \subset (A^\perp)^\circ \text{ et } A^\perp = (\operatorname{Vect} A)^\perp, \qquad X \subset (X^\circ)^\perp \text{ et } X^\circ = (\operatorname{Vect} X)^\circ,$$
$$\{0_E\}^\perp = E^* \text{ et } E^\perp = \{0_{E^*}\}. \qquad \{0_{E^*}\}^\circ = E \text{ et } (E^*)^\circ = \{0_E\}.$$

Si l'on suppose de plus que A et X sont des sous-espaces vectoriels de E et E^* respectivement, on a les résultats dimensionnels suivants.

Proposition. Soient F un sous-espace vectoriel de E et L un sous-espace vectoriel de E^*. On a :

$$\dim F + \dim F^\perp = n = \dim L + \dim L^\circ,$$

et par conséquent :

$$(F^\perp)^\circ = F \text{ et } (L^\circ)^\perp = L.$$

Preuve. La première égalité étant triviale lorsque $F = E$ ou $F = \{0_E\}$, on peut supposer que F est de dimension $1 \leq p \leq n-1$. D'après le théorème de la base incomplète, on peut considérer une base $\mathcal{B} = (e_i)_{1\leq i\leq n}$ de E dont les p premiers vecteurs forment une base $(e_i)_{1\leq i\leq p}$ de F. Parmi les vecteurs de la base duale $\mathcal{B}^* = (e_j^*)_{1\leq i\leq n}$ de E^*, considérons la famille $\mathcal{C} = (e_j^*)_{p+1\leq j\leq n}$. C'est évidemment une famille libre ; montrons qu'elle est génératrice de $F^\perp$. Il est clair que $e_j^* \in F^\perp$ pour tout $p+1 \leq j \leq n$ puisque $\langle e_j^*, e_i\rangle = 0$ pour tout $1 \leq i \leq p$ (par définition de la base duale). Tout élément ℓ de $F^\perp$ se décompose dans E^* sous la forme $\ell = \sum_{i=1}^n \langle \ell, e_j\rangle e_j^*$; mais $\langle \ell, e_i\rangle = 0$ lorsque $1 \leq i \leq p$, de sorte que ℓ est une combinaison linéaire des vecteurs de $\mathcal{C}$. On conclut que $\mathcal{C}$ est une base de $F^\perp$, et donc $\dim F^\perp = n - p$. Le seconde identité sur les dimensions se montre de même. Il est alors clair que, pour des raisons de dimensions, les inclusions $F \subset (F^\perp)^\circ$ et $L \subset (L^\circ)^\perp$ vues dans l'exercice précédent sont ici des égalités. □

Remarque : *cas des espaces vectoriels euclidiens.*

Supposons que E soit un espace vectoriel euclidien. Notons $u \cdot v$ le produit scalaires de deux vecteurs u et v dans E. Rappelons d'abord le résultat suivant, connu sous le nom de théorème de représentation des formes linéaires, ou théorème de représentation de Riesz.

(i) *Pour tout vecteur $a \in E$, l'application $\ell_a : E \to \mathbb{R}$ définie par $\ell_a(v) = a \cdot v$ pour tout $v \in E$ est une forme linéaire sur E.*
(ii) *Réciproquement, pour toute forme linéaire $\ell \in E^*$, il existe un unique vecteur $a \in E$ tel que $\ell = \ell_a$.*

Preuve. Le point (i) est clair par bilinéarité du produit scalaire. Pour (ii), considérons l'application $\Phi : E \to E^*$ définie par $\Phi(a) = \ell_a$ pour tout $a \in E$. Il est immédiat de vérifier qu'elle est linéaire. Son noyau est le sous-espace des vecteurs a tels que $\ell_a = 0_{E^*}$, ce qui équivaut à $a \cdot v = 0$ pour tout $v \in E$, et donc $a = 0_E$ par définition d'un produit scalaire. Ainsi $\operatorname{Ker}\Phi = \{0_E\}$, l'application $\Phi : E \to E^*$ est injective, donc bijective puisque $\dim E = \dim E^*$. Finalement, pour tout $\ell \in E^*$, il existe un unique $a \in E$ telle que $\ell = \Phi(a)$. □

Ainsi, via la correspondance bijective Φ, le crochet de dualité sur E (au sens de 1.1) coïncide avec le produit scalaire, au sens où :

pour tous $\ell \in E^*$ et $v \in E$, $\langle \ell, v\rangle = a \cdot v$, où a est l'unique vecteur de E tel que $\ell = \ell_a$.

Tous les résultats donnés ici dans le cadre de la dualité sur l'orthogonalité ou sur la transposition (ci-dessous) s'appliquent donc en particulier aux espaces euclidiens.

▶ *Exercice.* Pour tous sous-espaces vectoriels F_1 et F_2 de E, et L_1 et L_2 de E^*, on a :

$$(F_1 + F_2)^\perp = F_1^\perp \cap F_2^\perp \quad \text{et} \quad (F_1 \cap F_2)^\perp = F_1^\perp + F_2^\perp$$
$$(L_1 + L_2)^\circ = L_1^\circ \cap L_2^\circ \quad \text{et} \quad (L_1 \cap L_2)^\circ = L_1^\circ + L_2^\circ$$

1.5 - Transposition

On considère ici deux espaces vectoriels E et F de dimensions finies respectives n et m.

Définition et proposition. Pour tout application linéaire f de E dans F, l'application ${}^t f$ de F^* dans E^* définie par :

$${}^t f(\ell) = \ell \circ f \quad \text{pour tout } \ell \in F^*$$

est une application linéaire de F^* dans E^*. On l'appelle l'application *transposée* de f.

Preuve. Evident. □

Théorème. L'application $t : f \mapsto {}^t f$ est un isomorphisme d'espaces vectoriels de $\mathcal{L}(E, F)$ sur $\mathcal{L}(F^*, E^*)$.

Preuve. La linéarité de t est évidente. Soit $f \in \operatorname{Ker} t$. Pour tout $\ell \in F^*$ et tout $v \in E$, on a $\langle \ell, f(v) \rangle = \ell(f(v)) = {}^t f(\ell)(v) = 0$. Donc $f(v) \in (F^*)^\circ$ pour tout $v \in E$. Comme $(F^*)^\circ = \{0_E\}$, on conclut que f est l'application nulle dans $\mathcal{L}(E, F)$. Ceci montre que t est injective, et donc bijective puisque $\dim \mathcal{L}(E, F) = \dim \mathcal{L}(F^*, E^*) = nm$. □

▶ *Exercice.*

$\operatorname{Ker} {}^t f = (\operatorname{Im} f)^\perp$ et $\operatorname{Im} {}^t f = (\operatorname{Ker} f)^\perp$.

$\operatorname{rg} {}^t f = \operatorname{rg} f$, et si f est un isomorphisme, alors $({}^t f)^{-1} = {}^t f^{-1}$.

${}^t(g \circ f) = {}^t f \circ {}^t g$, avec G un espace vectoriel de dimension finie et $g \in \mathcal{L}(F, G)$.

1.6. - Hyperplans [1]

Soit $\ell : E \to \mathbb{K}$ une forme linéaire sur E. D'après la formule du rang, le rang de ℓ ne peut valoir que 1 ou 0. Ce rang est nul si et seulement ℓ est identiquement nulle. Ce rang vaut 1 si et seulement si ℓ est surjective ; son noyau est alors de dimension $n - 1$.

Définition et proposition. On appelle *hyperplan* de E tout sous-espace vectoriel de E de dimension $n - 1$.

(i) Un sous-espace vectoriel H de E est un hyperplan si et seulement s'il existe une forme linéaire $\ell \in E^*$ non-nulle telle que $H = \operatorname{Ker} \ell$.

(ii) Dans ce cas une forme linéaire $\ell' \in E^*$ vérifie $H = \operatorname{Ker} \ell'$ si et seulement s'il existe un scalaire non-nul λ tel que $\ell' = \lambda \ell$.

1. On privilégie ici la définition historique et élémentaire d'hyperplan par la dimension, mais en vue d'une notion valide en toute dimension, on peut prendre comme une définition plus générale le fait d'être le noyau d'une forme linéaire non-nulle. Les deux notions coïncident bien sûr en dimension finie ; en dimension infinie un des problèmes principaux est de distinguer le cas des formes linéaires continues.

Preuve. Soit H un hyperplan. D'après le théorème de la base incomplète, on peut considérer une base $\mathcal{B} = (e_1, \dots, e_n)$ de E telle que $(e_1, \dots, e_{n-1})$ soit une base de H. Notons $\ell = e_n^*$. Tout vecteur $v \in E$ se décompose sous la forme $v = \sum_{i=1}^n \langle e_i^*, v\rangle e_i$, et $v \in H$ si et seulement si $\langle e_n^*, v\rangle = 0$, c'est-à-dire si et seulement si $v \in \operatorname{Ker} \ell$, ce qui montre (i). Pour montrer (ii), considérons une forme linéaire non-nulle ℓ' telle que $H = \operatorname{Ker} \ell'$. Pour tout $v \in E$, on a $\ell'(v) = \langle e_n^*, v\rangle \ell'(e_n)$ et $\ell(v) = \langle e_n^*, v\rangle \ell(e_n)$. Comme $\ell(e_n)$ et $\ell'(e_n)$ sont non-nuls, on déduit que $\ell'(v) = \lambda \ell(v)$ pour $\lambda = \ell'(e_n)\ell(e_n)^{-1}$. La réciproque est évidente. □

Corollaire. Soit $\mathcal{B}$ une base de E.

(i) Quels que soient des scalaires $a_1, a_2, \dots, a_n$ non tous nuls dans $\mathbb{K}$, l'ensemble des vecteurs de E dont les composantes $(x_1, x_2, \dots, x_n)$ dans la base $\mathcal{B}$ vérifient la relation $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$ est un hyperplan H de E.

(ii) Réciproquement, quel que soit un hyperplan H de E, il existe des scalaires $a_1, a_2, \dots, a_n$ non tous nuls dans $\mathbb{K}$ tel que H soit l'ensemble des vecteurs de E dont les composantes $(x_1, x_2, \dots, x_n)$ dans la base $\mathcal{B}$ vérifient la relation $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$.

On dit alors que la relation $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$ est une *équation de H dans la base $\mathcal{B}$*. Une relation de la forme $b_1x_1 + b_2x_2 + \cdots + b_nx_n = 0$ est une autre équation de H dans $\mathcal{B}$ si et seulement s'il existe $\lambda \in \mathbb{K}$ non-nul tel que $b_i = \lambda a_i$ pour tout $1 \leq i \leq n$.

▶ *Application : systèmes d'équations d'un sous-espace vectoriel.*

Tout sous-espace vectoriel F de dimension $1 \leq p \leq n$ est l'ensemble des vecteurs de E dont les composantes dans la base $\mathcal{B}$ vérifie un système de $n - p$ équations d'hyperplans, qui sont les noyaux de $n - p$ formes linéaires indépendantes.

Preuve. Soit $(e_1, \dots, e_p)$ une base de F. Complétons-la en une base $\mathcal{B} = (e_1, \dots, e_p, e_{p+1}, \dots, e_n)$ de E. Considérons la base duale $\mathcal{B}^* = (e_1^*, \dots, e_p^*, e_{p+1}^*, \dots, e_n^*)$. La sous-famille $(e_{p+1}^*, \dots, e_n^*)$ est évidemment libre, de sorte que $e_{p+1}^*, \dots, e_n^*$ sont $n-p$ formes linéaires indépendantes dans E^*. Comme on l'a vu en 2.2, un vecteur quelconque $v \in E$ s'écrit toujours $v = \sum_{i=1}^n \langle e_i^*, v\rangle e_i$; dire que $v \in F$ signifie donc que $\langle e_i^*, v\rangle = 0$ pour tout $p + 1 \leq i \leq n$, ce qui prouve que $\operatorname{Ker} f = \bigcap_{i=p+1}^n \operatorname{Ker} e_i^*$. □

2. Exemples d'applications [2]

2.1. - Engendrement de certains groupes de la géométrie.

▶ *Engendrement du groupe orthogonal par les symétries hyperplanes*

Si H est un hyperplan d'un espace vectoriel euclidien E non-nul, la symétrie orthogonale par rapport à H est l'application $s : E \to E$ qui, à tout vecteur $v \in E$ décomposé de façon unique

2. On se limite ici à quelques applications simples. Plusieurs autres sont intéressantes, mais nécessitent des développements spécifiques hors du format de ce petit document. Citons par exemple parmi les thèmes classiques : (1) les versions géométriques du théorème de Hahn-Banach sur la séparation des convexes par des hyperplans affines dans un espace vectoriel normé ; (2) le rôle des bases duales dans la preuve du théorème de réduction de Frobenius sur les endomorphismes cycliques ; (3) certaines applications en géométrie différentielle (extrema liés par exemple). Observons enfin qu'en raison de l'interprétation du crochet de dualité dans le cas des espaces euclidiens (détaillée précédemment au paragraphe 1.4) plusieurs résultats centraux dans ce contexte (comme la diagonalisation des endomorphismes symétriques) relèvent de raisonnements de dualité.

sous la forme $v = u + w$ avec $u \in H$ et $v \in H^\perp$, associe le vecteur $s(v) = u - w$. Une telle symétrie est appelée simplement une *symétrie hyperplane*. Toute symétrie hyperplane est une isométrie vectorielle, c'est-à-dire un élément du groupe orthogonal $\mathrm{O}(E)$.

Proposition. Soit E un espace vectoriel euclidien de dimension $n \geq 1$. Le groupe orthogonal $\mathrm{O}(E)$ est engendré par les symétries hyperplanes de E.

Preuve. On se propose de montrer que, pour toute isométrie $f \in \mathrm{O}(E)$ disctincte de id_E, il existe des symétries hyperplanes $s_1, \ldots, s_p$, avec $p \leq n$, telles que $f = s_1 \circ s_2 \circ \cdots \circ s_p$ (sachant que id_E est quant à elle toujours égale à $s \circ s$ pour toute symétrie hyperplane). On raisonne par récurrence sur n. Le résultat est vrai si $n = 1$ car alors $\mathrm{O}(E) = \{\mathrm{id}_E, -\mathrm{id}_E\}$ et $-\mathrm{id}_E$ est la symétrie par rapport à l'hyperplan $\{0_E\}$. Supposons le résultat vrai pour tout espace euclidien de dimension n, et prenons dans un espace euclidien E de dimension $n + 1$ une isométrie vectorielle f. Distinguons deux cas.

• Supposons qu'il existe un vecteur $u \in E$ non-nul tel que $f(u) = u$. Introduisons la droite D de base u et l'hyperplan $H = D^\perp$. Il est facile de vérifier que, parce f est une isométrie et D est stable par f, alors H est aussi stable par f. En appliquant l'hypothèse de récurrence à la restriction f_0 de f à H, il existe des symétries $s_1, s_2, \ldots, s_p$ par rapport à des hyperplans $F_1, F_2, \ldots, F_p$ de H telles que $f = s_1 \circ s_2 \circ \cdots \circ s_p$, avec $p \leq n$. On pose $L_i = F_i \oplus D$ pour tout $1 \leq i \leq n$, qui est un hyperplan de E. L'orthogonal $L_i^\perp$ de L_i dans E est égal à l'orthogonal de F_i dans H, $s_i(w) = -w$ pour tout $w \in L_i^\perp$. On prolonge s_i de H à $E = H \oplus D$ en posant $t_i(u) = u$. Alors $t_i(v) = v$ pour tout $v \in L_i$. Ainsi t_i est la symétrie orthogonale de E par rapport à l'hyperplan L_i. D'une part, pour tout $v \in H$, on a $(t_1 \circ \cdots \circ t_p)(v) = (s_1 \circ \cdots\cdots \circ s_t)(v) = f_0(v) = f(v)$. D'autre part $(t_1 \circ \cdots \circ t_p)(u) = u = f(u)$. On conclut que $f = t_1 \circ \cdots \circ t_p$ avec $p \leq n$.

• Supposons que, pour tout vecteur $u \in E$ non-nul, on a $f(u) \neq u$. Choisissons un tel vecteur u. Le vecteur $u - f(u) \neq 0_E$ engendre une droite vectorielle D. Notons H l'hyperplan $D^\perp$. Comme $f \in \mathrm{O}(E)$, les vecteurs $u - f(u)$ et $u + f(u)$ sont orthogonaux. Ainsi $u + f(u) \in H = D^\perp$, alors que $u - f(u) \in D = H^\perp$. En notant s la symétrie hyperplane par rapport à H, on a $s(u + f(u)) = u + f(u)$ et $s(u - f(u)) = -u + f(u)$. En écrivant $u = \frac{1}{2}(u + f(u)) + \frac{1}{2}(u - f(u))$, on déduit que $s(u) = f(u)$, d'où $u = s(f(u))$. On peut donc appliquer le premier cas à l'isométrie $s \circ f$: celle-ci est produit d'un nombre $p \leq n$ de symétries hyperplanes, donc $f = s \circ s \circ f$ est produit de $p + 1 \leq n + 1$ symétries hyperplanes. □

► *Engendrement du groupe spécial linéaire par les transvections*

Rappelons qu'une *transvection* d'un $\mathbb{K}$-espace vectoriel E de dimension finie n est un endomorphisme f de E tel qu'il existe une forme linéaire $\ell \in E^*$ et un vecteur non-nul $e \in \mathrm{Ker}\, \ell$ tels que $f(v) = v + \ell(v)e$ pour tout $v \in E$. Il est clair qu'on a alors $f \in \mathrm{SL}(E)$.

Exercice. Montrer que si v et w sont deux vecteurs non-nuls et non colinéaires de E, il existe une transvection f de E tel que $f(v) = w$. En déduire que si v et w sont deux vecteurs colinéaires non-nuls de E, il existe deux transvections f et g que $f(g(v)) = w$.

Exercice. Soit H et L deux hyperplans de E. Soit v un vecteur non-nul de E n'appartenant ni à H ni à L. Alors il existe une transvection f de E qui fixe v et qui échange H et L.

Proposition. Soit E un espace vectoriel de dimension $n \geq 1$. Le groupe spécial linéaire $\mathrm{SL}(E)$ est engendré par les transvections de E.

Preuve. On raisonne par récurrence sur n. Le résultat est vrai si $n = 1$. Supposons le résultat vrai pour tout espace vectoriel de dimension n, et prenons dans un espace vectoriel E de dimension $n + 1$ un isomorphisme $f \in \mathrm{SL}(E)$. Considerons un vecteur quelconque non-nul v de E. Quitte à composer par une ou deux transvections, il résulte du premier execice ci-dessus que l'on peut supposer que $f(v) = v$.

Prenons un hyperplan H de E qui ne contient pas v, de sorte que $v = f(v)$ n'appartient pas non plus à l'hyperplan $f(H)$. Donc d'après le second exercice ci-dessus, quitte à composer par une autre transvection, on peut supposer que $f(H) = H$. On applique l'hypothèse de récurrence à la restriction f_0 de f à H : il existe des transvections $g_1, \dots, g_p$ de H telles que $f = g_1 \circ \cdots \circ g_p$. Chacune des g_i se prolonge en une transvection f_i de E en fixant v, et l'on obtient $f = f_1 \circ \cdots \circ f_p$. □

2.2. - Formes linéaires sur l'espace vectoriel des matrices carrées.

► On fixe dans ce paragraphe un entier $n \geq 2$. La proposition suivante donne une description explicite des formes linéaires sur l'espace vectoriel $\mathcal{M}_n(\mathbb{K})$.

Proposition.
(i) Pour toute matrice $A \in \mathcal{M}_n(\mathbb{K})$, l'application $\varphi_A : \mathcal{M}_n(\mathbb{K}) \to \mathbb{K}$ définie par $\varphi_A(M) = \operatorname{tr}(AM)$ pour toute $M \in \mathcal{M}_n(\mathbb{K})$ est une forme linéaire sur $\mathcal{M}_n(\mathbb{K})$.
(ii) L'application $A \mapsto \varphi_A$ est un isomorphisme de l'espace vectoriel $\mathcal{M}_n(\mathbb{K})$ sur son dual $\mathcal{M}_n(\mathbb{K})^*$.

Preuve. Le point (i) est clair, de même que la linéarité de l'application $\Phi : A \mapsto \varphi_A$. Comme $\mathcal{M}_n(\mathbb{K})$ et son dual $\mathcal{M}_n(\mathbb{K})^*$ sont de même dimension, il suffit de montrer l'injectivité de Φ. Soit donc $A \in \operatorname{Ker}\Phi$. On a $\operatorname{tr}(AM) = \varphi_A(M) = O$ pour tout $M \in \mathcal{M}_n(\mathbb{K})$. En particulier, pour $M = E_{k,\ell}$ un vecteur fixé quelconque de la base canonique de $\mathcal{M}_n(\mathbb{K})$, on a en notant $A = (a_{ij})_{1 \leq i,j \leq n}$:

$$\begin{aligned} 0 = \operatorname{tr}(AE_{k,\ell}) = \operatorname{tr}\Big(\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}E_{i,j}E_{k,\ell}\Big) &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\operatorname{tr}(E_{i,j}E_{k,\ell}) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\operatorname{tr}(\delta_{k,j}E_{i,\ell}) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}\delta_{k,j}\delta_{i,\ell} = a_{\ell,k}. \end{aligned}$$

Ceci étant pour tous $1 \leq k, \ell \leq n$, on conclut que A est la matrice nulle, ce qui achève la preuve. □

► C'est une propriété bien connue de la trace que $\operatorname{tr}(MN) = \operatorname{tr}(NM)$ quelles que soient $M, N \in \mathcal{M}_n(\mathbb{K})$. On peut déduire de la proposition précédente que cette propriété caractérise la trace parmi les formes linéaires sur $\mathcal{M}_n(\mathbb{K})$ "à une constante près" :

Corollaire. L'ensemble des formes linéaires φ sur $\mathcal{M}_n(\mathbb{K})$ qui vérifient $\varphi(MN) = \varphi(NM)$ pour toutes $M, N \in \mathcal{M}_n(\mathbb{K})$ est un sous-espace vectoriel de dimension 1 du dual $\mathcal{M}_n(\mathbb{K})^*$, engendré par la trace.

Preuve. Soit $\varphi \in \mathcal{M}_n(\mathbb{K})^*$ vérifiant la condition $\varphi(MN) = \varphi(NM)$ pour toutes $M, N \in \mathcal{M}_n(\mathbb{K})$. D'après la proposition précédente, il existe une unique matrice $A \in \mathcal{M}_n(\mathbb{K})$ telle que $\varphi = \varphi_A$. On a donc pour toutes $M, N \in \mathcal{M}_n(\mathbb{K})$ l'égalité $\operatorname{tr}(AMN) = \operatorname{tr}(ANM)$, d'où en utilisant les propriétés de la trace $\operatorname{tr}(AMN) = \operatorname{tr}(MAN)$, ou encore $\operatorname{tr}((AM - MA)N) = 0$. Ceci étant pour tout $N\mathcal{M}_n(\mathbb{K})$, on en déduit que φ_{AM-MA} est la forme nulle, et donc par injectivité de l'isomorphisme Φ de la proposition précédente, que $AM - MA$ est la matrice nulle. Ceci étant pour tout $M \in \mathcal{M}_n(\mathbb{K})$, la matrice A est dans le centre de $\mathcal{M}_n(\mathbb{K})$. Il existe donc $\lambda \in \mathbb{K}$ telle que $A = \lambda I_n$. Finalement, pour toute $M \in \mathcal{M}_n(\mathbb{K})$, on a : $\varphi(M) = \operatorname{tr}(AM) = \operatorname{tr}(\lambda M) = \lambda \operatorname{tr}(M)$. □

► On déduit aussi de l'isomorphisme précédent la propriété suivante des hyperplans de $\mathcal{M}_n(\mathbb{K})$.

Corollaire. Tout hyperplan de $\mathcal{M}_n(\mathbb{K})$ a une intersection non-vide avec le groupe linéaire $\mathrm{GL}_n(\mathbb{K})$.

Preuve. Soit H un hyperplan de $\mathcal{M}_n(\mathbb{K})$. Il est le noyau d'une forme linéaire non-nulle $\varphi \in \mathcal{M}_n(\mathbb{K})^*$. D'après la proposition précédente, il existe $A \in \mathcal{M}_n(\mathbb{K})$ non-nulle telle que $\varphi = \varphi_A$. Il s'agit donc de montrer qu'il existe une matrice inversible $S \in \mathrm{GL}_n(\mathbb{K})$ telle que $\varphi_A(S) = 0$.

Considérons la forme canonique $A = PJQ$ de la matrice de A, où $P, Q \in \mathrm{GL}_n(\mathbb{K})$ et $J = \begin{pmatrix} I_r & O_{n-r} \\ O_{n-r} & O_{n-r} \end{pmatrix}$, avec $r = \operatorname{rg} A$. La forme linéaire φ_A s'exprime alors sous la forme $\varphi_A(M) = \operatorname{tr}(PJQM) = \operatorname{tr}(JQMP)$. Il suffit donc de trouver une matrice $T \in \mathrm{GL}_n(\mathbb{K})$ telle que $\operatorname{tr}(JT) = 0$ pour que la matrice $S = Q^{-1}TP^{-1} \in \mathrm{GL}_n(\mathbb{K})$ vérifie $\varphi_A(S) = \operatorname{tr}(JQQ^{-1}TP^{-1}P) = \operatorname{tr}(JT) = 0$. On conclut en choisissant pour T la matrice de permutation associée à la permutation circulaire $(1, 2, \ldots, n)$: son déterminant vaut $\varepsilon(\sigma) \neq 0$ et la diagonale de la matrice JT n'est formée que de zéros. □

Formes quadratiques

L'objectif de ces notes n'est pas de faire un exposé complet de ce qui peut être dit sur cette notion dans le cadre du programme, mais juste de faire un focus sur quelques arguments généraux (en termes d'isomorphismes canoniques et de dualité) pour établir les principaux théorèmes de réduction et de classification des formes quadratiques, en particulier dans les espaces euclidiens.

1. Réduction des formes quadratiques

Dans toute cette partie, E désigne un $\mathbb{K}$-espace vectoriel de dimension finie n. Volontairement, on ne se limite pas ici au contexte prévu par le programme (i.e. $\mathbb{K} = \mathbb{R}$), et $\mathbb{K}$ désigne simplement un corps commutatif de caractéristique différente de 2.

1.1 - Isomorphisme canonique entre formes quadratiques et formes bilinéaires symétriques

Définition. Une *forme quadratique* sur E est une application $q : E \to \mathbb{K}$ qui s'exprime dans toute base de E sous la forme d'un polynôme homogène de degré 2 en les variables coordonnées, ou qui est identiquement nulle.

Comme les formules de changements de base sont linéaires, si la condition de la définition est vraie dans une base, elle l'est dans toute base. Concrètement, cette condition se traduit par le fait que, pour toute base $\mathcal{B}$ de E, il existe des scalaires $(c_{ij})_{1\leq i,j\leq n}$ tels que, pour tout vecteur v de coordonnées $(x_1, \dots, x_n)$ dans la base $\mathcal{B}$, on ait :

$$q(v) = \sum_{i=1}^{n} c_{ii}x_i^2 \ + \ 2\sum_{1\leq i<j\leq n} c_{ij}x_ix_j.$$

Définition. Une *forme bilinéaire* sur E est une application $\varphi : E \times E \to \mathbb{K}$ qui vérifie, pour tous vecteurs $u, v, w \in E$:

(i) $\varphi(u+v, w) = \varphi(u, w) + \varphi(v, w)$ et $\varphi(u, v+w) = \varphi(u, v) + \varphi(u, w)$,

(ii) $\varphi(\lambda u, v) = \varphi(u, \lambda v) = \lambda\varphi(u, v)$ pour tout $\lambda \in \mathbb{K}$.

La forme bilinéaire φ est dite *symétrique* si de plus :

(iii) $\varphi(u, v) = \varphi(v, u)$ pour tous $u, v \in E$.

Si l'on fixe une base $\mathcal{B} = (e_1, \dots, e_n)$ de E et si l'on pose $a_{ij} = \varphi(e_i, e_j)$ pour tous $1 \leq i, j \leq n$, il résulte de la bilinéarité que, quels que soient deux vecteurs $u, v \in E$ de coordonnées respectives $(x_1, \dots, x_n)$ et $(y_1, \dots, y_n)$, on a :

$$\varphi(u, v) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_iy_j.$$

Il est clair que dans ce cas $q(u) := \varphi(u, u)$ pour tout $u \in E$ définit une forme quadratique sur E. Mais a priori plusieurs formes bilinéaires peuvent donner la même forme quadratique (par exemple $\varphi(u, v) = x_1y_1 + x_2y_2$ et $\psi(u, v) = x_1y_1 + x_1y_2 - x_2y_1 + x_2y_2$ donnent toutes les deux $q(u) = x_1^2 + y_1^2$ sur $E = \mathbb{R}^2$). Néanmoins il y a unicité dès lors que l'on suppose de plus que φ est symétrique (i.e. $a_{ij} = a_{ji}$). C'est le résultat d'isomorphisme suivant :

Théorème et définition.

(i) L'ensemble des formes bilinéaires symétriques sur E et l'ensemble des formes quadratiques sur E sont des $\mathbb{K}$-espaces vectoriels, de dimension $\frac{1}{2}n(n+1)$.

(ii) L'application qui, à toute forme bilinéaire symétrique φ sur E, associe la forme quadratique q sur E définie par :

$$q(u) = \varphi(u,u) \quad \text{pour tout } u \in E$$

est un isomorphisme d'espace vectoriel.

(iii) Son isomorphisme réciproque est l'application qui, à toute forme quadratique q sur E, associe la forme bilinéaire symétrique φ sur E définie par :

$$\varphi(u,v) = \tfrac{1}{2}[q(u+v) - q(u) - q(v)] \quad \text{pour tous } u, v \in E,$$

appelée la *forme polaire* associée à q.

Preuve. Vérifications élémentaires ; laissées au lecteur. □

Remarque. On peut déduire de cette correspondance une autre définition (équivalente) de la notion de forme quadratique comme une application $q : E \to \mathbb{K}$ vérifiant $q(\lambda v) = \lambda^2 q(v)$ pour tous $v \in E$, $\lambda \in \mathbb{K}$, et telle que l'application $(u,v) \mapsto \frac{1}{2}[q(u+v) - q(u) - q(v)]$ est bilinéaire.

1.2 - Morphisme canonique de E dans E^* associé à une forme quadratique

On note E^* l'espace dual de E, c'est-à-dire l'espace vectoriel des formes linéaires sur E (i.e. des applications linéaires $\ell : E \to \mathbb{K}$). On sait que E et E^* sont isomorphes, de même dimension n.

Proposition. Soient q une forme quadratique q sur E et φ sa forme polaire associée.

(i) Pour tout vecteur $u \in E$, l'application $\varphi_u : E \to \mathbb{K}$ définie par $\varphi_u(v) = \varphi(u,v)$ pour tout $v \in E$ est une forme linéaire sur E.

(ii) L'application $J_\varphi : E \to E^*$ qui à tout $u \in E$ associe la forme linéaire φ_u est un morphisme de $\mathbb{K}$-espace vectoriel.

Preuve. Vérifications élémentaires ; laissées au lecteur. □

▶ Ce morphisme canoniquement associé à q ou φ permet de définir les notions suivantes :

Définitions. Soient q une forme quadratique q sur E et φ sa forme polaire associée.

(i) On appelle *noyau* de q (ou de φ) le noyau du morphisme J_φ ; en d'autres termes :

$$\operatorname{Ker} q = \operatorname{Ker} \varphi = \{u \in E \,;\, \varphi(u,v) = 0 \text{ pour tout } v \in E\} \,.$$

(ii) On appelle *rang* de q (ou de φ) le rang de l'application J_φ ; en d'autres termes :

$$\operatorname{rg} q = \operatorname{rg} \varphi = n - \dim \operatorname{Ker} q.$$

(iii) On dit que q (ou φ) est *non-dégénérée* lorsque son noyau est nul ; en d'autres termes :

$$[q \text{ non dégénérée}] \Leftrightarrow [\operatorname{Ker} q = \{0_E\}] \Leftrightarrow [\operatorname{rg} q = n] \Leftrightarrow [J_\varphi \text{ isomorphisme}].$$

Preuve. Vérifications élémentaires ; laissées au lecteur. □

▶ Application importante. Un exemple intéressant d'application de l'isomorphisme J_φ entre E et E^* dans le cas non dégénéré est le suivant :

Définitions et proposition. Soient q une forme quadratique q sur E et φ sa forme polaire associée.

(i) On dit que deux vecteurs u et v sont *orthogonaux* pour q (ou pourφ) lorsque $\varphi(u,v)=0$.

(ii) Pour tout sous-espace vectoriel H de E, on appelle *orthogonal* de H l'ensemble $H^\perp$ des vecteurs de E qui sont orthogonaux à tous les vecteurs de H :

$$H^\perp = \{u \in E\,;\, \varphi(u,v)=0 \text{ pour tout } v \in H\}.$$

(a) $H^\perp$ est un sous-espace vectoriel de E.

(b) Si de plus q est non-dégénérée, alors $\dim H + \dim H^\perp = n$ et $(H^\perp)^\perp = H$.

Preuve. Le point (a) est évident. Pour (b), considérons l'isomorphisme J_φ de E sur E^*. L'image $J_\varphi(H^\perp)$ est l'ensemble des formes linéaires φ_y telles que $y \in H^\perp$. Par bijectivité de J_φ, c'est donc l'ensemble des formes linéaires de E^* qui s'annulent en tout vecteur de H. En d'autres termes, $J_\varphi(H^\perp)$ est l'orthogonal H° du sous-espace H au sens de la dualité. Or on sait [3] que $\dim H + \dim H^\circ = n$, ce qui achève la preuve puisque $\dim H^\perp = \dim J_\varphi(H^\perp) = \dim H^\circ$. □

▶ Attention, la somme de H et $H^\perp$ n'est pas forcément directe :

— $E=\mathbb{R}^2$, $\varphi(u,v)=x_1y_1-x_2y_2$ pour tous $u=(x_1,x_2)$ et $v=(y_1,y_2)$; alors la droite $H=\{u\in E\,;\,x_1=x_2\}$ vérifie $H^\perp=H$.

— $E=\mathbb{R}^3$, $\varphi(u,v)=x_1y_1+x_2y_2-x_3y_3$ pour tous $u=(x_1,x_2,x_3)$ et $v=(y_1,y_2,y_3)$; la droite $H=\{u\in E\,;\,x_1=x_3 \text{ et } x_2=0\}$ vérifie $H^\perp=\{u\in E\,;\,x_1=x_3\}$ donc $H\subset H^\perp$ avec $\dim H^\perp=2$.

— $E=\mathbb{R}^4$, $\varphi(u,v)=x_1y_1+x_2y_2+x_3y_3-x_4y_4$ pour tous $u=(x_1,x_2,x_3,x_4)$ et $v=(y_1,y_2,y_3,y_4)$; le plan $H=\{u\in E\,;\,x_1=x_2 \text{ et } x_3=x_4\}$ a pour orthogonal $H^\perp=\{u\in E\,;\,x_1+x_2=0 \text{ et } x_3=x_4\}$, d'où $H\cap H^\perp=\{u\in E\,;\,x=1=x_2=0 \text{ et } x_3=x_4\}$ de dimension 1, avec $\dim H=\dim H^\perp=2$.

1.4 - Représentations matricielles

Rappelons les quelques propriétés suivantes, dont les preuves reposent sur des considérations élémentaires de bilinéarité. Soient q une forme quadratique et φ la forme polaire associée.

1. Pour toute base $\mathcal{B}=(e_1,\dots,e_n)$ de E, la matrice A de q (ou φ) dans la base $\mathcal{B}$ est la matrice $n\times n$ de terme général $a_{ij}=\varphi(e_i,e_j)$. C'est une matrice symétrique, dont le rang est le rang de q. Pour tous vecteurs u et v de E de matrices colonnes de coordonnées respectives X et Y dans la base $\mathcal{B}$, on a : $\varphi(u,v)={}^tXAY$.
2. Si $\mathcal{B}'$ est une autre base de E et si l'on note $P\in \mathrm{GL}(n,\mathbb{K})$ la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$, alors la matrice A' de q (ou φ) dans la base $\mathcal{B}'$ est $A'={}^tPAP$.
3. La base $\mathcal{B}$ est dite *orthogonale* pour q (ou pour φ) lorsque $\varphi(e_i,e_j)=0$ pour tous $1\le i\ne j\le n$, ce qui équivaut au fait que la matrice A est diagonale.

3. Soit $(e_1,\dots,e_n)$ une base de E telle que $(e_1,\dots,e_p)$ soit une base de H. Toute $\ell\in E^*$ se décompose dans la base duale en $\ell=\sum_{i=1}^n \lambda_i e_i^*$, avec $\lambda_i=\ell(e_i)$. Alors $\ell\in H^\circ$ si et seulement si $\ell(e_i)=0$ pour tout $1\le i\le p$, donc si et seulement si $\ell=\sum_{p+1}^n \lambda_i e_i^*$. Ce qui montre que $(e_{p+1}^*,\dots,e_n^*)$ est une base de H°, et donc $\dim H^\circ=n-p$.

1.5 - Théorèmes de réduction et de classification

Théorème fondamental.

Pour toute forme quadratique q sur E, il existe une base orthogonale.

Preuve. On procède par récurrence sur la dimension n de E. Le résultat est clair si $n = 1$. Supposons le théorème vrai au rang n. Soit E de dimension $n+1$. Si q est identiquement nulle sur E, le résultat est évident. Sinon, il existe un vecteur $e_{n+1} \in E$ tel que $q(e_{n+1}) \neq 0$. Soit F la droite vectorielle engendrée par e_{n+1}. Son orthogonal $F^\perp$ est le sous-espace des vecteurs $v \in E$ tels que $\varphi(e_{n+1}, v) = 0$, c'est-à-dire le noyau de la forme linéaire non-nulle $\varphi_{e_{n+1}}$. Donc $F^\perp$ est de dimension n. L'hypothèse $q(e_{n+1}) \neq 0$ implique que $F \cap F^\perp = \{0_E\}$, de sorte que le sous-espace $F + F^\perp$ est de dimension $n+1$, donc est égal à E. En d'autres termes $F \oplus F^\perp = E$. Par hypothèse de récurrence, il existe une base $(e_1, \ldots, e_n)$ de $F^\perp$ orthogonale pour la restriction de q à $F^\perp$. Ainsi $(e_1, \ldots, e_n, e_{n+1})$ est une base de E orthogonale pour q. □

Corollaire. Pour toute forme quadratique q sur E, il existe une base $\mathcal{B}$ de E telle que la matrice de q dans la base $\mathcal{B}$ est diagonale, donc il existe des scalaires $\lambda_1, \ldots, \lambda_n \in \mathbb{K}$ tels que, pour tout vecteur $u \in E$ de coordonnées $(x_1, \ldots, x_n)$ dans la base $\mathcal{B}$, on a :

$$q(u) = \sum_{i=1}^{n} \lambda_i x_i^2.$$

Le nombre de λ_i qui sont non-nuls est indépendant de la base $\mathcal{B}$ puisqu'il s'agit du rang de q.

► Le problème de la classification.

1. Deux formes quadratique q et q' sur E sont dites *équivalentes* lorsqu'il existe un automorphisme f de E tel que $q(u) = q'(f(u))$ pour tout $u \in E$.
2. Ceci équivaut à l'existence de deux bases $\mathcal{B}$ et $\mathcal{B}'$ de E telles que la matrice de q dans la base $\mathcal{B}$ est égale à la matrice de q' dans la base $\mathcal{B}'$.
3. Le problème de la classification des formes quadratiques consiste en la détermination des classes d'équivalence suivant la relation d'équivalence des formes quadratiques, ce qui revient à chercher des bases dans lesquelles la matrice d'une forme quadratique donnée est d'une forme canonique la plus simple possible.
4. Même si cette question se réduit d'après le théorème fondamental ci-dessus à travailler sur des matrices diagonales, cela reste un problème potentiellement difficile en fonction du corps $\mathbb{K}$ sur lequel on travaille. Par exemple les cas où $\mathbb{K} = \mathbb{Q}$ ou où $\mathbb{K}$ est un corps fini donnent lieu à des théories algébriques complexes. Les seules situations vraiment évidentes sont celles où $\mathbb{K} = \mathbb{C}$ et où $\mathbb{K} = \mathbb{R}$, que l'on va résoudre maintenant en montrant que :
   - pour E un $\mathbb{C}$-espace vectoriel, les formes quadratiques sur E sont classifiées par un entier $0 \leq r \leq n$, à savoir le rang.
   - pour E un $\mathbb{R}$-espace vectoriel, les formes quadratiques sur E sont classifiées par un couple (p, p') d'entiers tels que $0 \leq p + p' \leq n$, appelé la signature.

Théorème (classification dans le cas complexe).

Pour toute forme quadratique q de rang r sur un $\mathbb{C}$-espace vectoriel E de dimension n, il existe une base $\mathcal{B}$ de E telle que, pour tout vecteur u de coordonnées $(x_1, \dots, x_n)$ dans la base $\mathcal{B}$, on a :

$$q(u) = x_1^2 + x_2^2 + \cdots + x_r^2.$$

Preuve. D'après le corollaire du théorème fondamental ci-dessus, il existe une base $\mathcal{B} = (e_1, \dots, e_n)$ dans laquelle q s'xprime sous la forme $q(u) = \sum_{i=1}^n \lambda_i x_i^2$ avec les λ_i dans $\mathbb{C}$. Quitte à permuter les vecteurs de $\mathcal{B}$, on peut sans restriction supposer que $\lambda_i \neq 0$ pour $1 \leq i \leq r$ et $\lambda_i = 0$ pour $r+1 \leq i \leq n$. Parce que $\mathbb{C}$ est algébriquement clos, il existe pour tout $1 \leq i \leq r$ un nombre $\alpha_i \in \mathbb{C}$ non-nul tel que $\lambda_i = \alpha_i^2$. En posant $e'_i = \frac{1}{\alpha_i} e_i$ pour $1 \leq i \leq r$ et $e'_i = e_i$ pour $r+1 \leq i \leq n$, on obtient une nouvelle base de E dans laquelle q s'exprime de la façon voulue. □

Théorème (classification dans le cas réel : loi d'inertie de Sylvester).

Pour toute forme quadratique q de rang r sur un $\mathbb{R}$-espace vectoriel E de dimension n, il existe une base $\mathcal{B}$ de E telle que, pour tout vecteur u de coordonnées $(x_1, \dots, x_n)$ dans la base $\mathcal{B}$, on a :

$$q(u) = x_1^2 + x_2^2 + \cdots + x_p^2 - x_{p+1}^2 - x_{p+2}^2 - \cdots - x_r^2 \ ,$$

où p est un entier tel que $0 \leq p \leq r$ qui ne dépend que de q.

Le couple $(p, r-p)$ est appelée la *signature* de la forme quadratique q.

Preuve. On procède de la même façon que précédemment avec les coefficients réels λ_i. Quitte à permuter les vecteurs de $\mathcal{B}$, on peut sans restriction supposer que $\lambda_i = 0$ pour $r+1 \leq i \leq n$ et que, pour un certain entier $1 \leq p \leq r$, on a $\lambda_i > 0$ pour $1 \leq i \leq p$ et $\lambda_i < 0$ pour $p+1 \leq i \leq r$. Il existe pour tout $1 \leq i \leq p$ un nombre $\alpha_i \in \mathbb{R}$ non-nul tel que $\lambda_i = \alpha_i^2$, et pour tout $p+1 \leq i \leq r$ un nombre $\alpha_i \in \mathbb{R}$ non-nul tel que $-\lambda_i = \alpha_i^2$. En posant $e'_i = \frac{1}{\alpha_i} e_i$ pour $1 \leq i \leq r$ et $e'_i = e_i$ pour $r+1 \leq i \leq n$, on obtient une nouvelle base de E dans laquelle q s'exprime de la façon voulue.

Il reste à démontrer que p ne dépend pas du choix de la base. Donnons-nous pour cela deux bases $\mathcal{B} = (e_1, \dots, e_n)$ et $\mathcal{B}' = (e'_1, \dots, e'_n)$ de E dans lesquelles q s'exprime respectivement par :

$$q(u) = x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_r^2 \quad \text{et} \quad q(u) = {x'_1}^2 + \cdots + {x'_{p'}}^2 - {x'_{p'+1}}^2 - \cdots - {x'_r}^2,$$

avec $1 \leq p, p' \leq r$. Considérons les sous-espaces vectoriels :

$$F = \mathrm{Vect}(e_1, \dots, e_p),\ H = \mathrm{Vect}(e_{p+1}, \dots, e_n),\ F' = \mathrm{Vect}(e'_1, \dots, e'_{p'}),\ H' = \mathrm{Vect}(e_{p'+1}, \dots, e_n).$$

Soit $u \in F' \cap H$. Si u était non-nul, on aurait à la fois $q(u) > 0$ et $q(u) \leq 0$, ce qui est impossible. C'est donc que $F' \cap H = \{0_E\}$. On en déduit que le sous-espace $F' + H$ est de dimension $p' + (n-p)$, d'où $p' \leq p$. On a de même $p \leq p'$, ce qui achève la preuve. □

1.6 - Deux compléments importants sur la réduction des formes quadratiques

▶ Procédé pratique de réduction en somme de carrés : méthode de Gauss.

C'est un procédé algorithmique permettant d'exprimer toute forme quadratique q sur $E = \mathbb{R}^n$ sous la forme $\sum_{i \leq n} \lambda_i \ell_i^2$ avec $\lambda_i \in \mathbb{R}^*$, où les ℓ_i sont des formes linéaires *indépendantes* dans E^*. Le nombre p de coefficients $\lambda_i > 0$ et le nombre p' de coefficients $\lambda_i < 0$ donnent la signature de q, et $p + p'$ est le rang de q.

Nous ne développons pas ici la mise en œuvre de cette méthode bien connue, et renvoyons à tout ouvrage classique traitant des formes quadratiques.

► Sur l'existence de bases orthonormales. Pour une forme quadratique q, de forme polaire associée φ, complétons la notion de base orthogonale introduite en 1.4.3.

1. Une base $\mathcal{B} = (e_1, \ldots, e_n)$ de E est dite *orthonormale* pour q (ou pour φ) lorsque
$$\varphi(e_i, e_j) = 0 \text{ pour tous } 1 \leq i \neq j \leq n \quad \text{et} \quad \varphi(e_i, e_i) = 1 \text{ pour tout } 1 \leq i \leq n,$$
ce qui équivaut au fait que la matrice A est égale à la matrice identité I_n.
2. Le théorème fondamental de 1.5 établit l'existence d'une base orthogonale pour toute forme quadratique de E, et ceci quel que soit le corps $\mathbb{K}$ des scalaires. Mais il est clair d'après les deux théorèmes de classification qu'il n'existe pas forcément des bases orthonormales.
3. Si $\mathbb{K} = \mathbb{C}$, il existe une base orthonormale pour une forme quadratique q si et seulement elle est de rang n, c'est-à-dire non dégénérée, ce qui équivaut à $q(u) \neq 0$ pour tout $u \neq 0_E$.
4. Si $\mathbb{K} = \mathbb{R}$, il existe une base orthonormale pour une forme quadratique q si et seulement elle est de signature $(n, 0)$, ce qui équivaut à $q(u) > 0$ pour tout $u \neq 0_E$.

Cette dernière remarque correspond au cas des espaces euclidiens étudiés ci-dessous.

2. Formes quadratiques sur un espace euclidien

Dans toute cette partie, E désigne un $\mathbb{R}$-espace vectoriel de dimension finie n.

2.1 - Notion de produit scalaire

Définitions. Soit q une forme quadratique sur E, de forme polaire associée φ.

(i) On dit que q (ou φ) est *positive* lorsqu'elle est de signature $(r, 0)$, où r désigne le rang de q, ce qui équivaut à : $q(u) \geq 0$ pour tout $u \in E$.

(ii) On dit que q (ou φ) est *définie positive* lorsqu'elle est de signature $(n, 0)$, ce qui équivaut à : $q(u) \geq 0$ pour tout $u \in E$, et $q(u) = 0$ si et seulement si $u = 0_E$.

Une forme bilinéaire symétrique définie positive est appelée un *produit scalaire*.

Un $\mathbb{R}$-espace vectoriel de dimension finie muni d'un produit scalaire s'appelle un *espace vectoriel euclidien*.

► Procédé d'orthonormalisation de Schmidt. On a vu à la fin de la première partie que, si φ est un produit scalaire, il existe une base de E qui est orthonormale pour φ. La méthode d'orthonormalisation de Schmidt est un procédé algorithmique permettant de construire une telle base orthonormale à partir d'une base quelconque de E. Nous ne développons pas ici cette méthode bien connue, et renvoyons à tout ouvrage classique traitant des espaces euclidiens.

► Remarque. Nous ne développons pas ici non plus les résultats standards sur les espaces vectoriels euclidiens concernant les exemples classiques, la norme euclidienne associée, la propriété de Pythagore, l'existence du supplémentaire orthogonal, l'inégalité de Cauchy-Schwarz, le cône isotrope, ... ce sont tous des points importants qui ont leur place dans tout exposé sur le sujet, mais pour lesquels nous renvoyons aux ouvrages usuels.

2.2 - Réduction simultanée des formes quadratiques sur un espace euclidien

Théorème (dit de réduction simultanée).

Soient q_1 et q_2 deux formes quadratiques sur un $\mathbb{R}$-espace vectoriel de dimension finie.

Si q_1 est définie positive, alors il existe une base orthonormale pour q_1 qui est orthogonale pour q_2.

Preuve. On raisonne par récurrence sur $n = \dim E$. Pour $n = 1$, le résultat est clair. Prenons $n \geq 2$, supposons par hypothèse de récurrence le résultat vrai pour tout espace vectoriel euclidien de dimension $n-1$, et considérons un espace vectoriel euclidien E de dimension n. On note φ_1 le produit scalaire de E et q_1 la forme quadratique associée. On considère une forme quadratique q_2 sur E, de forme polaire associée φ_2.

La sphère unité $S^1 = \{w \in E\,;\, q_1(w) = 1\}$ est compacte dans E, donc l'application $q_2 : E \to \mathbb{R}$, qui est continue sur E, atteint son maximum sur S^1. Il existe un vecteur e de S^1 tel que $q_2(w) \leq q_2(e)$ pour tout $w \in S^1$. Notons $\lambda = q_2(e) \in \mathbb{R}$, et introduisons la forme bilinéaire symétrique φ de E définie par :

$$\varphi(u,v) = \lambda\varphi_1(u,v) - \varphi_2(u,v) \ \text{ pour tous } u, v \in E.$$

Sa forme quadratique q associée vérifie donc :

$$q(u) = \lambda q_1(u) - q_2(u) \ \text{ pour tout } u \in E.$$

Soit $u \in E$ quelconque. Posons $w = q_1(u)^{-1/2}u$ de sorte que $w \in S^1$. On a donc $q_1(u)^{-1}q_2(u) = q_2(w) \leq \lambda$, ce qui prouve que $q(u) \geq 0$. Ainsi la forme quadratique q est positive. De plus, e est un vecteur isotrope de q, ce qui signifie que $q(e) = 0$. Or il est bien connu que le cône isotrope d'une forme quadratique *positive* est égale à son noyau (c'est une conséquence de l'inégalité de Cauchy-Schwarz). Donc $e \in \operatorname{Ker} q = \operatorname{Ker} \varphi$. En particulier $\varphi(e,v) = 0$ pour tout $v \in E$. D'où :

$$\varphi_2(e,v) = \lambda\varphi_1(e,v) \ \text{ pour tout } v \in E.$$

Soit F la droite vectorielle de E engendrée par e. Soit H l'hyperplan vectoriel qui est l'orthogonal de F pour le produit scalaire φ_1. Par hypothèse de récurrence, il existe une base $\mathcal{B}' = (e_2, \ldots, e_n)$ de H orthonormale pour q_1 qui est orthogonale pour la restriction q_2' de q_2 à H. En adjoignant e, on obtient une base $\mathcal{B} = (e, e_2, \ldots, e_n)$ de E. Elle est orthonormale pour q_1 puisque e appartient à l'orthogonal F de H et que $e \in S^1$. Elle est aussi orthogonale pour q_2 puisqu'il résulte des calculs précédents que $\varphi_2(e,v) = 0$ pour tout $v \in H$. □

2.3 - Application à la théorie spectrale des espaces euclidiens

On fixe un $\mathbb{R}$-espace vectoriel euclidien E de dimension n.

► NOTATIONS. Par commodité, on modifie dans ce dernier paragraphe la notation $\varphi(u,v)$ employée pour le produit scalaire de deux vecteurs ; on le note maintenant :

$$\langle u \,|\, v\rangle \text{ pour tous } u, v \in E.$$

Le morphisme de dualité $E \to E^*$ associé à ce produit scalaire, tel qu'on l'a introduit en 1.2, est ici un isomorphisme, qui permet d'associer à tout vecteur $a \in E$ une unique forme linéaire $\ell_a : E \to \mathbb{R}$ définie par :

$$\ell_a(v) = \langle a \,|\, v\rangle \text{ pour tout } v \in E,$$

et réciproquement, pour toute forme $\ell \in E^*$, il existe un unique vecteur $a \in E$ tel que $\ell = \ell_a$.

▶ Notion d'endomorphisme symétrique. Rappelons que, par définition, un endomorphisme f de E est dit *symétrique* lorsqu'il vérifie :

$$\langle f(u) \,|\, v\rangle = \langle u \,|\, f(v)\rangle \text{ pour tous } u, v \in E.$$

Il est facile de voir qu'un endomorphisme est symétrique si et seulement si sa matrice dans une base orthonormale de E est une matrice symétrique. Les endomorphismes symétriques forment un sous-espace vectoriel de $\operatorname{End} E$ isomorphe au sous-espace vectoriel des matrices symétriques de $\mathcal{M}_n(\mathbb{R})$. Rappelons (théorème 1.1) que c'est aussi le cas de l'espace vectoriel des formes bilinéaires symétriques (ou des formes quadratiques). On peut effectivement construire canoniquement l'isomorphisme suivant :

▶ Isomorphisme canonique entre formes quadratiques et endomorphismes symétriques

Lemme. Soit E un espace vectoriel euclidien, de produit scalaire $\langle \cdot \,|\, \cdot \rangle$.

(i) Pour tout endomorphisme symétrique f de E, l'application $\varphi_f : E \times E \to \mathbb{R}$ définie par :

$$\varphi_f(u, v) = \langle f(u) \,|\, v\rangle \quad \text{pour tous } u, v \in E$$

est une forme bilinéaire symétrique sur E. Sa forme quadratique $q_f : E \to \mathbb{R}$ associée est définie par $q_f(u) = \langle f(u) \,|\, u\rangle$ pour tout $u \in E$.

(ii) Réciproquement, pour toute forme quadratique q de E, il existe un unique endomorphisme symétrique f de E tel que $q = q_f$. La forme polaire associée à q est alors φ_f.

(iii) Avec ces notations, on a : $\operatorname{Ker} f = \operatorname{Ker} q_f = \operatorname{Ker} \varphi_f$ et $\operatorname{rg} f = \operatorname{rg} q_f = \operatorname{rg} \varphi_f$.

Preuve. Les points (i) et (iii) sont clairs. Pour montrer (ii), considérons une forme quadratique q sur E, et φ sa forme polaire associée. En appliquant à φ la proposition 1.2, on peut considérer pour tout $u \in E$ la forme linéaire $\varphi_u \in E^*$ définie par $\varphi_u(v) = \varphi(u, v)$ pour tout $v \in E$. D'après la même proposition 1.2 mais appliquée cette fois au produit scalaire sur E, il existe un unique vecteur $f(u)$ de E tel que $\varphi_u = \ell_{f(u)}$ (avec la notation introduite ci-dessus) ce qui signifie que, pour tout $v \in E$, on a : $\varphi(u, v) = \langle f(u) \,|\, v\rangle$. La bilinéarité de φ implique que l'application $f : E \to E$ ainsi définie est linéaire. Le fait que la forme bilinéaire φ soit symétrique implique que f est un endomorphisme symétrique. □

▶ Application à une preuve du théorème spectral

Théorème. Tout endomorphisme symétrique f d'un espace vectoriel euclidien E est diagonalisable. Plus précisément, il existe des bases orthonormales de E constituées de vecteurs propres de f.

Preuve. Soit f un endomorphisme symétrique de E. Soit q_f la forme quadratique de E associée à f au sens du lemme précédent. D'après le théorème 2.2 de réduction simultanée, il existe une base $\mathcal{B} = (e_1, \ldots, e_n)$ de E qui est orthonormale pour le produit scalaire et orthogonale pour q_f. On a donc $\varphi_f(e_i, e_j) = 0$ pour tous $1 \leq i \neq j \leq n$, c'est-à-dire $\langle f(e_i) \,|\, e_j\rangle = 0$, ce qui traduit le fait que la matrice de f dans la base $\mathcal{B}$ est diagonale. □

Endomorphismes symétriques d'un espace vectoriel euclidien

Dans tout ce qui suit, on se place dans un espace vectoriel euclidien E. On note $n \geq 1$ sa dimension. Le produit scalaire de deux vecteurs x et y de E est noté $\langle x \,|\, y \rangle$.

1. Notion d'endomorphisme symétrique

1.1 - Adjoint d'un endomorphisme

Lemme préliminaire (représentation des formes linéaires).

(i) *Pour tout vecteur $a \in E$, l'application $\ell_a : E \to \mathbb{R}$ définie par $\ell_a(x) = \langle a \,|\, x \rangle$ pour tout $x \in E$ est une forme linéaire sur E.*

(ii) *Réciproquement, pour toute forme linéaire $\ell \in E^*$, il existe un unique vecteur $a \in E$ tel que $\ell = \ell_a$.*

Preuve. Le point (i) est clair par bilinéarité du produit scalaire. Pour (ii), considérons l'application $\Phi : E \to E^*$ définie par $\Phi(a) = \ell_a$ pour tout $a \in E$. Il est immédiat de vérifier qu'elle est linéaire. Son noyau est le sous-espace des vecteurs a tels que $\ell_a = 0_{E^*}$, ce qui équivaut à $\langle a \,|\, x \rangle = \ell_a(x) = 0$ pour tout $x \in E$. Parce que $\langle \cdot \,|\, \cdot \rangle$ est un produit scalaire, cela équivaut à $a = 0_E$. Ainsi $\operatorname{Ker} \Phi = \{0_E\}$. Ainsi l'application $\Phi : E \to E^*$ est injective. Comme $\dim E = \dim E^*$, cela équivaut à la bijectivité de Φ. Donc, pour tout $\ell \in E^*$, il existe un unique $a \in E$ telle que $\ell = \Phi(a)$, ce qui est l'assertion (ii) voulue. □

Théorème et définition. Pour tout endomorphisme f de E, il existe un unique endomorphisme de E, noté f^*, appelé *l'adjoint* de f, vérifiant :

$$\langle\, f(x) \,|\, y \,\rangle = \langle\, x \,|\, f^*(y) \,\rangle \qquad \text{pour tous } x, y \in E.$$

Preuve. Soit $y \in E$. Considérons l'application $x \mapsto \langle f(x) \,|\, y \rangle$ est une forme linéaire sur E. D'après le lemme ci-dessus,il existe un unique vecteur $f^*(y)$ tel que $\langle\, f(x) \,|\, y \,\rangle = \langle\, x \,|\, f^*(y) \,\rangle$ pour tout $x \in E$. On définit ainsi une application $y \mapsto f^*(y)$ de E dans E. Il s'agit de montrer qu'elle est linéaire.

Soient x, y, z quelconques dans E, λ, μ quelconques dans $\mathbb{R}$. Considérons le réel $\langle f(x) \,|\, \lambda y + \mu z \rangle$.
D'une part d'après ce qui précéde : $\langle f(x) \,|\, \lambda y + \mu z \rangle = \langle x \,|\, f^*(\lambda y + \mu z) \rangle$. D'autre part par bilinéarité :

$$\langle f(x) \,|\, \lambda y + \mu z \rangle = \lambda \langle f(x) \,|\, y \rangle + \mu \langle f(x) \,|\, z \rangle = \lambda \langle x \,|\, f^*(y) \rangle + \mu \langle x \,|\, f^*(z) \rangle = \langle x \,|\, \lambda f^*(y) + \mu f^*(z) \rangle.$$

Ainsi : $\langle x \,|\, f^*(\lambda y + \mu z) \rangle = \langle x \,|\, \lambda f^*(y) + \mu f^*(z) \rangle$, ceci pour tout $x \in E$, ce qui prouve la linéarité de f^*.□

Corollaire. Pour tout endomorphisme f de E et toute base orthonormale $\mathcal{B}$ de E, la matrice de f^* dans la base $\mathcal{B}$ est la transposée de la matrice de f dans $\mathcal{B}$:

$$\operatorname{Mat}_{\mathcal{B}}(f^*) = {}^t\operatorname{Mat}_{\mathcal{B}}(f).$$

Preuve. Notons $\mathcal{B} = (e_1, \ldots, e_n)$, $A = (a_{ij})_{1 \leq i,j \leq n} = \operatorname{Mat}_{\mathcal{B}}(f)$ et $B = (b_{ij})_{1 \leq i,j \leq n} = \operatorname{Mat}_{\mathcal{B}}(f^*)$.
Comme $\mathcal{B}$ est orthonormale, on a : $a_{ij} = \langle f(e_j) \,|\, e_i \rangle$ et $b_{ij} = \langle f^*(e_j) \,|\, e_i \rangle$ pour tous $1 \leq i, j \leq n$. D'où :

$$b_{ij} = \langle f^*(e_j) \,|\, e_i \rangle = \langle e_j \,|\, f(e_i) \rangle = \langle f(e_i) \,|\, e_j \rangle = e_{ji},$$

donc $B = {}^tA$. □

Proposition. Soit f un endomorphisme f de E ; on a les propriétés suivantes :

(i) $(f^*)^* = f$, $\operatorname{Ker} f^* = (\operatorname{Im} f)^\perp$, $\operatorname{Im} f^* = (\operatorname{Ker} f)^\perp$, $\operatorname{rg} f^* = \operatorname{rg} f$.

(ii) $(f \circ g)^* = g^* \circ f^*$ pour tout autre endomorphisme g de E.

(iii) si f est bijective, alors f^* l'est aussi et l'on a $(f^*)^{-1} = (f^{-1})^*$.

Preuve. Laissée au lecteur. □

1.2 - Endomorphisme symétrique

Définition. Un endomorphisme f de E est dit symétrique lorsqu'il est égal à son adjoint.

En d'autres termes :

$$[\ f \text{ symétrique}\ ] \iff [\ f^* = f\ ] \iff [\ \langle f(x) \,|\, y\rangle = \langle x \,|\, f(y)\rangle \text{ pour tous } x, y \in E\ ],$$

et f est symétrique si et seulement si sa matrice dans une base orthonormale de E est une matrice symétrique.

Exemples. Soit F un sous-espace vectoriel de E. La projection orthogonale p_F sur F et la symétrie orthogonale s_F par rapport à F sont des endomorphismes symétriques.

Preuve. Laissée au lecteur (rappelons p_F et s_F sont définies par $p_F(x) = x'$ et $s_F(x) = x' - x''$ pour tout vecteur $x \in E$ décomposé de façon unique en $x = x' + x''$ avec $x' \in F$ et $x'' \in F^\perp$ d'après de la décomposition $E = F \oplus F^\perp$). □

Proposition. L'ensemble des endomorphismes symétriques de E est un sous-espace vectoriel de dimension $\frac{n(n+1)}{2}$.

Preuve. Laissée au lecteur (déterminer une base du sous-espace vectoriel des matrices symétriques). □

1.3 - Quelques propriétés immédiates en exercices

► Montrer que, pour tout endomorphisme f de E, les endomorphismes $f + f^*$ et $f \circ f^*$ sont symétriques.

► Montrer que, si f et g sont deux endomorphismes symétriques de E, l'endomorphisme $f \circ g$ est symétrique si et seulement si f et g commutent.

► Montrer que, si f est un endomorphisme symétrique de E, les sous-espaces vectoriels $\operatorname{Ker} f$ et $\operatorname{Im} f$ sont supplémentaires orthogonaux.

► Soient F et H deux sous-espaces vectoriels de E tels que $E = F \oplus H$. Soient p la projection sur F parallèlement à H, et s la symétrie par rapport à F parallèlement à H.

− Montrer que p est un endomorphisme symétrique si et seulement si H est l'orthogonal de F.

− Montrer que s est un endomorphisme symétrique si et seulement si H est l'orthogonal de F.

2. Diagonalisation des endomorphismes symétriques

2.1 - Le théorème spectral

Proposition. Si λ et μ sont deux valeurs propres réelles distinctes d'un endomorphisme symétrique, alors les sous-espaces propres associés E_λ et E_μ sont orthogonaux.

Preuve. Soit f un endomorphisme symétrique de E. Soient λ et μ deux valeurs propres distinctes de f. Soient x, y respectivement des vecteurs propres associés aux valeurs propres λ et μ. Donc $f(x) = \lambda x$ et $f(y) = \mu y$. Comme f est symétrique, on a : $\langle f(x) \,|\, y \rangle = \langle x \,|\, f(y) \rangle$, donc $\langle \lambda x \,|\, y \rangle = \langle x \,|\, \mu y \rangle$, ou encore $\lambda \langle x \,|\, y \rangle = \mu \langle x \,|\, y \rangle$. Parce que $\lambda \neq \mu$, on déduit que $\langle x \,|\, y \rangle = 0$, c'est-à-dire $x \perp y$. □

Lemme. Le polynôme caractéristique d'un endomorphisme symétrique se décompose complètement dans $\mathbb{R}$ en un produit de polynômes de degré 1.

Preuve. Notons $\dim E = n$. Soient f un endomorphisme symétrique de E, et A sa matrice dans une base orthonormale de E. En particulier A est une matrice symétrique dans $\mathcal{M}_n(\mathbb{R})$. Soient $P_f = P_A$ le polynôme caractéristique de f ou A. C'est un polynôme à coefficients réels, que l'on peut considérer aussi comme polynôme à coefficients complexes. A ce titre, il se décompose dans $\mathbb{C}[x]$ sous la forme $P_A(x) = (-1)^n (x - \lambda_1)(x - \lambda_2) \dots (x - \lambda_n)$ avec les λ_i dans $\mathbb{C}$ (pas forcément deux à deux distincts). Il s'agit de montrer que $\lambda_i \in \mathbb{R}$ pour tout $1 \leq i \leq n$.

La matrice A peut être considérée comme la matrice d'un endomorphisme g de $\mathbb{C}^n$ par rapport à la base canonique de $\mathbb{C}^n$. Prenons l'un des nombres complexes λ_i en le notant simplement λ. C'est une valeur propre de g ; soit $x \in \mathbb{C}^n$ un vecteur propre associé. On a $x \neq 0_{\mathbb{C}^n}$ et $g(x) = \lambda x$. Notons X la matrice colonne des composantes de x dans la base $\mathcal{B}$, de sorte que : $AX = \lambda X$. En prenant les conjugués de tous les coefficients dans cette égalité, on a $\overline{A}\,\overline{X} = \overline{\lambda}\,\overline{X}$. Mais $\overline{A} = A$ puisque A est à coefficients réels. Donc $A\,\overline{X} = \overline{\lambda}\,\overline{X}$, ou encore en transposant : ${}^t\overline{X}\,{}^tA = \overline{\lambda}\,{}^t\overline{X}$, c'est-à-dire ${}^t\overline{X}A = \overline{\lambda}\,{}^t\overline{X}$, puisque A est symétrique.

En combinant les égalités $\overline{\lambda}\,{}^t\overline{X} = {}^t\overline{X}A$ et $AX = \lambda X$, on obtient $\overline{\lambda}\,{}^t\overline{X}\,X = {}^t\overline{X}AX = \lambda\,{}^t\overline{X}\,X$. Or ${}^t\overline{X}\,X$ est un réel strictement positif (c'est la somme des carrés des modules des composantes dans $\mathbb{C}$ du vecteur non-nul x). On conclut que $\overline{\lambda} = \lambda$, c'est-à-dire $\lambda \in \mathbb{R}$. □

Théorème. Tout endomorphisme *symétrique* f d'un espace vectoriel euclidien E est diagonalisable. Plus précisément, il existe des bases *orthonormales* de E constituées de vecteurs propres de f.

Preuve. On raisonne par récurrence sur $n = \dim E$. Pour $n = 1$, le résultat est clair. Prenons $n \geq 2$, supposons par hypothèse de récurrence le résultat vrai pour tout espace vectoriel euclidien de dimension $n - 1$, et considérons un espace vectoriel euclidien E de dimension n.

Soit f un endomorphisme symétrique de E. D'après le lemme, il admet des valeurs propres réelles ; soit λ l'une d'elle. Considérons e un vecteur propre associé à λ. Quitte à multiplier e par le réel $\|e\|^{-1}$, on peut sans restriction choisir e de norme 1. Soit H l'hyperplan vectoriel orthogonal à la droite vectorielle $F = \mathbb{R}e$ engendrée par e. Pour tout $x \in H$, on a : $\langle f(x) \,|\, e \rangle = \langle x \,|\, f(e) \rangle$ puisque f est symétrique, d'où en utilisant le fait que $f(e) = \lambda e$ l'on déduit que : $\langle f(x) \,|\, e \rangle = \langle x \,|\, \lambda e \rangle = \lambda \langle x \,|\, e \rangle = 0$. Ceci prouve que pour tout $x \in H$, le vecteur $f(x)$ est orthogonal à e ; en d'autres termes H est stable par f.

Donc la restriction de f à H détermine un endomorphisme f' de H, qui reste évidemment symétrique. Par hypothèse de récurrence appliquée à f', il existe une base orthonormale $\mathcal{B}' = (e_2, \dots, e_n)$ de H constituée de vecteurs propres de f' donc de f. En adjoignant e, on obtient une famille $\mathcal{B} = (e, e_2, \dots, e_n)$. Par construction, $\mathcal{B}'$ est constituée de vecteurs propres de f. Puisque $E = H \oplus F$ avec $F \perp H$, la famille $\mathcal{B}'$ est une base orthonormale de E. □

Corollaire. Toute matrice *symétrique* A dans $\mathcal{M}_n(\mathbb{R})$ est diagonalisable.

Plus précisément, il existe une matrice diagonale D à coefficients réels et une matrice *orthogonale* $P \in \mathrm{O}(n, \mathbb{R})$ telles que $A = PDP^{-1}$.

Preuve. Soit A une matrice symétrique dans $\mathcal{M}_n(\mathbb{R})$. Soit f l'endomorphisme de l'espace euclidien $E = \mathbb{R}^n$ (muni du produit scalaire canonique) dont A est la matrice de f dans la base canonique $\mathcal{B}$. C'est un endomorphisme symétrique. En appliquant le théorème ci-dessus, il existe une base orthonormale $\mathcal{B}'$ de E telle que la matrice de f dans la base $\mathcal{B}'$ est une matrice diagonale D. On a donc $A = PDP^{-1}$, où P désigne la matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$. Cette matrice P est orthogonale en tant que matrice de passage entre deux bases orthonormales, ce qui achève la preuve. □

► *Application à la diagonalisation simultanée d'endomorphismes symétriques commutant deux à deux.*

Proposition. Soit $f_1, \ldots, f_k$ une famille d'endomorphismes symétriques de E. Si $f_i \circ f_j = f_j \circ f_i$ pour tous $1 \leq i, j \leq n$, alors il existe une base orthonormale $\mathcal{B}$ de E telle que la matrice M_i de f_i dans la base $\mathcal{B}$ soit diagonale pour tout $1 \leq i \leq n$.

Preuve. Le résultat est clair si E est de dimension 1. Supposons la propriété vraie pour tout espace vectoriel de dimension n et prenons E un espace vectoriel de dimension $n+1$, avec des endomorphismes symétriques $f_1, \ldots, f_k$ de E commutant deux à deux. Si tous les f_i sont des homothéties, c'est fini. Si l'un au moins des f_i, par exemple f_1, n'est pas une homothétie, il résulte du théorème spectral que $E = F_1 \oplus \cdots \oplus F_s$ avec $\dim F_j \leq n$ et $F_j \perp F_\ell$ pour tous $1 \leq j \neq \ell \leq s$, où $F_1, \ldots, F_s$ désigne les sous-espaces propres distincts de f_1. L'hypothèse $f_1 \circ f_i = f_i \circ f_1$ implique que F_j est stable par f_i pour tout $1 \leq i \leq k$ et tout $1 \leq j \leq s$. Les restrictions $f_1', \ldots, f_k'$ de $f_1, \ldots, f_k$ à F_j sont donc des endomorphismes symétriques de F_j commutant deux à deux. D'après l'hypothèse de récurrence, il existe pour tout $1 \leq j \leq s$ une base orthonormale $\mathcal{B}_j$ de F_j dont les vecteurs sont vecteurs propres de f_i' pour tout $1 \leq i \leq k$. La réunion $\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_s$ est alors une base orthonormale de E dont les vecteurs sont vecteurs propres de f_i pour tout $1 \leq i \leq k$. □

2.2 - Endomorphismes symétriques et réduction des formes quadratiques

► *Correspondance bijective entre endomorphismes symétriques, formes bilinéaires symétriques, et formes quadratiques.*

Lemme fondamental.

(i) Pour tout endomorphisme symétrique f de E, l'application $\varphi_f : E \times E \to \mathbb{R}$ définie par :
$$\varphi_f(x, y) = \langle f(x) \,|\, y \rangle \quad \text{pour tous } x, y \in E$$
est une forme bilinéaire symétrique sur E. Sa forme quadratique $q_f : E \to \mathbb{R}$ associée est définie par $q_f(x) = \langle f(x) \,|\, x \rangle$ pour tout $x \in E$.

(ii) Réciproquement, pour toute forme quadratique q de E, il existe un unique endomorphisme symétrique f de E tel que $q = q_f$. La forme polaire associée à q est alors φ_f.

(iii) Avec ces notations, on a : $\operatorname{Ker} f = \operatorname{Ker} q_f = \operatorname{Ker} \varphi_f$ et $\operatorname{rg} f = \operatorname{rg} q_f = \operatorname{rg} \varphi_f$.

Preuve. Les points (i) et (iii) sont clairs. Pour montrer (ii), considérons une forme quadratique q sur E. Notons φ sa forme polaire associée. Rappelons que :

$$q(x) = \varphi(x,x) \quad \text{et} \quad \varphi(x,y) = \tfrac{1}{2}(q(x+y) - q(x) - q(y)) \quad \text{pour tous } x, y \in E.$$

Pour tout $x \in E$, notons h_x l'application $E \to \mathbb{R}$ définie par $h_x(y) = \varphi(x,y)$ pour tout $y \in E$. Il est clair que h_x est une forme linéaire sur E. D'après le point (ii) du lemme 1.1, il existe un unique vecteur $f(x)$ de E tel que $h_x = \ell_{f(x)}$, ce qui signifie que, pour tout $y \in E$, on a : $\varphi(x,y) = \langle f(x) \,|\, y \rangle$. La bilinéarité de φ implique aisément que l'application $f : E \to E$ est linéaire. Le fait que la forme bilinéaire φ soit symétrique implique que f est un endomorphisme symétrique. □

▶ *Réduction simultanée des formes quadratiques.*

Théorème. Soit q une forme quadratique sur l'espace vectoriel euclidien E. Il existe une base orthonormale de E qui est orthogonale pour q.

Preuve. Soit f l'endomorphisme symétrique de E tel que $q = q_f$. D'après le théorème spectral, il existe une base orthonormale $\mathcal{B} = (e_1, \ldots, e_n)$ de E telle que la matrice de f dans la base $\mathcal{B}$ est diagonale, ce qui se traduit par $\langle f(e_i) \,|\, e_j \rangle = 0$ pour tous $1 \leq i \neq j \leq n$. On conclut que $\varphi_f(e_i, e_j) = 0$ pour tous $1 \leq i \neq j \leq n$, ce qui prouve le résultat voulu. □

Corollaire (une formulation équivalente). Soient q_1 et q_2 deux formes quadratiques sur un espace vectoriel réel de dimension finie. Si q_1 est définie positive, alors il existe une base orthonormale pour q_1 qui est orthogonale pour q_2.

▶ *Remarque.* On a montré le théorème spectral, puis on en a déduit de façon évidente le théorème de réduction simultanée des formes quadratiques via la correspondance canonique entre formes quadratiques et endomorphismes symétriques. On aurait pu inversement donner d'abord une démonstration directe du théorème de réduction simultanée des formes quadratiques (par exemple suivant la méthode figurant dans le document pour l'agrégation interne sur les formes quadratiques) puis utiliser la correspondance canonique avec les endomorphismes symétriques pour en déduire le théorème spectral.

▶ *Exercice d'application à l'étude des coniques et des quadriques*

∘ Considérons la conique de $\mathbb{R}^2$ d'équation $x^2 - xy + y^2 + \frac{1}{2} = 0$. On note q la forme quadratique de $\mathbb{R}^2$ définie par $q(x,y) = x^2 - xu + y^2$. Utiliser la réduction de Gauss de q pour trouver sa signature. Utiliser la diagonalisation de la matrice de q dans la base canonique pour déterminer une base orthonormée de vecteurs propres. Vérifier que l'équation de la conique dans cette base est $X^2 + 3Y^2 = 1$ (ellipse centrée en l'origine).

∘ Considérons la quadrique de $\mathbb{R}^3$ d'équation $xy+yz+zx+1 = 0$. On note q la forme quadratique de $\mathbb{R}^3$ définie par $q(x,y,z) = xy + yz + zx$. Utiliser la réduction de Gauss de q pour trouver sa signature. Utiliser la diagonalisation de la matrice de q dans la base canonique pour déterminer une base orthonormée de vecteurs propres. Vérifier que l'équation de la quadrique dans cette base est $2X^2 - Y^2 - Z^2 + 2 = 0$ (hyperboloïde à une nappe de révolution autour de l'axe des X).

3. Endomorphismes symétriques positifs

On a vu en 2.2 que l'on peut associer de façon canonique à tout endomorphisme symétrique f de E une forme quadratique q_f. Le cas où cette forme quadratique q_f est positive, ou définie positive, donne lieu à certaines applications particulières développées ici.

3.1 - Spectre d'un endomorphisme symétrique positif

Définitions. Soit f un endomorphisme symétrique de E. On dit que :

(i) f est positif lorsque l'on a $\langle f(x) \,|\, x\rangle \geq 0$ pour tout $x \in E$.

(ii) f est défini positif lorsque l'on a $\langle f(x) \,|\, x\rangle > 0$ pour tout $x \in E$ non-nul.

On a vu que les valeurs propres d'un endomorphisme symétrique sont réelles. Plus précisément :

Théorème. Soit f un endomorphisme symétrique de E.

(i) f est positif si et seulement si toutes ses valeurs propres sont positives.

(ii) f est défini positif si et seulement si toutes ses valeurs propres sont strictement positives.

Preuve. Soit f un endomorphisme symétrique. D'après le théorème 2.1, il existe une base orthonormée $\mathcal{B} = (e_1, \ldots, e_n)$ de E formée de vecteurs propres de f. Pour tout $1 \leq i \leq n$, désignons par λ_i la valeur propre associée à e_i. Ces valeurs propres sont des réels. On a :

$$\langle f(e_i) \,|\, e_i\rangle = \langle \lambda_i e_i \,|\, e_i\rangle = \lambda_i \langle e_i \,|\, e_i\rangle = \lambda_i \quad \text{pour tout } 1 \leq i \leq n.$$

Il est clair que si f est positif (respectivement défini positif), alors tous les réels λ_i sont positifs (respectivement strictement positifs). Pour la réciproque, il suffit d'observer que, pour tout réel $x \in E$ décomposé dans la base $\mathcal{B}$ sous la forme $x = \sum_{i=1}^n \alpha_i e_i$, avec $\alpha_i \in R$, on a par bilinéarité :

$$\langle f(x) \,|\, x\rangle = \langle \sum_{i=1}^n \alpha_i f(e_i) \,|\, \sum_{i=1}^n \alpha_i e_i\rangle = \sum_{i=1}^n \alpha_i^2 \underbrace{\langle f(e_i) \,|\, e_i\rangle}_{=\lambda_i} + \sum_{1 \leq i \neq j \leq n} \alpha_i \alpha_j \underbrace{\langle f(e_i) \,|\, e_j\rangle}_{=0} = \sum_{i=1}^n \alpha_i^2 \lambda_i$$

□

Ce résultat permet une traduction en termes de matrices :

Définition. Une matrice carrée symétrique à coefficients dans $\mathbb{R}$ est dite *positive* (respectivement *définie positive*) lorsque toutes ses valeurs propres sont positives (respectivement strictement positives).

3.2 - Critère de Sylvester (mineurs principaux d'un endomorphisme symétrique positif)

Soit $A = (a_{ij})_{1 \leq i,j \leq n}$ une matrice carrée symétrique à coefficients réels. Pour tout $1 \leq k \leq n$, on note $A_k = (a_{ij})_{1 \leq i,j \leq k}$ la matrice carrée $k \times k$ extraite "au nord-ouest", et Δ_k son déterminant. On a alors :

Théorème. La matrice symétrique A est définie positive si et seulement si $\Delta_k > 0$ pour tout $1 \leq k \leq n$.

Preuve. Laissée au lecteur comme un possible développement d'approfondissement. □

4. Exemples d'applications

4.1 - Racine carrée d'un endomorphisme symétrique positif.

Proposition. Pour tout endomorphisme symétrique positif g de E, il existe un unique endomorphisme symétrique positif f de E tel que $g = f \circ f$.

Preuve. Soit g un endomorphisme symétrique positif. Soit $\mathcal{B} = (e_1, \dots, e_n)$ une base orthonormée de E formée de vecteurs propres de g. On a donc $g(e_i) = \lambda_i e_i$ pour tout $1 \leq i \leq n$ où $\lambda_1, \dots, \lambda_n$ sont les valeurs propres de g, qui appartiennent à $\mathbb{R}_+$ d'après le théorème 3.1. L'endomorphisme f défini par $f(e_i) = \sqrt{\lambda_i} e_i$ pour tout $1 \leq i \leq n$ vérifie bien que $f \circ f = g$.

Pour montrer l'unicité, considérons un endomorphisme symétrique positif f tel que $g = f \circ f$. Pour tout réel positif λ, notons $E_\lambda = \mathrm{Ker}(f - \lambda \,\mathrm{id}_E)$ et $F_\lambda = \mathrm{Ker}(g - \lambda \,\mathrm{id}_E)$. Il est clair que $E_\lambda \subseteq F_{\lambda^2}$. En particulier si λ est une valeur propre de f, alors λ^2 est une valeur propre de g. Les valeurs propres de f (qui sont toutes positives) sont donc de la forme $\sqrt{\lambda_i}$, où $\lambda_1, \dots, \lambda_k$ désignent les valeurs propres distinctes de g (qui sont toutes positives). Comme g et f sont tous les deux diagonalisables d'après le théorème 2.1, on a $\sum_{i=1}^k \dim F_{\lambda_i} = \sum_{i=1}^k \dim E_{\sqrt{\lambda_i}} = n$. Les inclusions $E_{\sqrt{\lambda_i}} \subseteq F_{\lambda_i}$ sont donc en fait des égalités. Il en résulte que, pour tout réel x décomposé par diagonalistion de g sous la forme $x = \sum_{i=1}^k x_i$ avec $x_i \in F_{\lambda_i} = E_{\sqrt{\lambda_i}}$, on a $f(x) = \sum_{i=1}^k f(x_i) = \sum_{i=1}^k \sqrt{\lambda_i} x_i$, ce qui définit f de façon unique. □

Corollaire. Pour toute matrice carrée réelle symétrique positive B, il existe une unique matrice carrée réelle symétrique positive A telle que $B = A^2$.

4.2 - Décomposition polaire d'un endomorphisme bijectif.

Théorème. Pour tout endomorphisme *bijectif* g de E, il existe un unique endomorphisme *orthogonal* u de E et un unique endomorphisme *symétrique défini positif* f de E tel que $g = u \circ f$.

Preuve. Commençons par quelques observations concernant l'endomorphisme $h = g^* \circ g$. Il est symétrique (voir le premier exemple de 1.3). De plus, pour tout vecteur $x \in E$, on a :

$$\langle h(x) \,|\, x \rangle = \langle g^*(g(x)) \,|\, x \rangle = \langle g(x) \,|\, g(x) \rangle = \|g(x)\|^2.$$

Ceci prouve que h est positif, et même défini positif [car $g(x) \neq 0_E$ pour $x \neq 0_E$ par bijectivité de g].

Montrons l'unicité de la décomposition. Supposons que l'on a $g = u \circ f$ avec u orthogonal et f symétrique positif. Remarquons d'abord que f est inversible puisque g et u le sont. Donc f est nécessairement défini positif. De plus, on calcule : $g^* \circ g = (u \circ f)^* \circ u \circ f = f^* \circ u^* \circ u \circ f = f^* \circ (u^* \circ u) \circ f$.

Or par hypthèse, $u^* \circ u = \mathrm{id}_E$ et $f^* = f$, d'où $f \circ f = g^* \circ g = h$. En appliquant le théorème 4.1, l'endomorphisme f satisfaisant $f \circ f = h$ est unique. L'unicité de f implique celle de u car $u = g \circ f^{-1}$.

Montrons maintenant l'existence de la décomposition. Comme h est symétrique défini positif, il existe un unique endomorphisme symétrique positif f tel que $h = f \circ f$, et il est défini positif, et donc bijectif. Posons $u = g \circ f^{-1}$ de façon à avoir $g = u \circ f$. On calcule :

$$u^* \circ u = (g \circ f^{-1})^* \circ g \circ f^{-1} = (f^{-1})^* \circ g^* \circ g \circ f^{-1} = (f^*)^{-1} \circ h \circ f^{-1} = f^{-1} \circ (f \circ f) \circ f^{-1} = \mathrm{id}_E,$$

ce qui montre que u est orthogonal et achève la preuve. □

Corollaire. Pour toute matrice carrée réelle *inversible* M, il existe une unique matrice carrée réelle *orthogonale* U et une unique matrice carrée réelle *symétrique définie positive* A telle que $M = UA$.

4.3 - Quelques propriétés complémentaires des matrices symétriques.

► *Norme et rayon spectral.*

La norme d'une matrice A carrée d'ordre n à coefficients réels induite par la norme euclidienne de $\mathbb{R}^n$ est définie par :

$$\|A\| = \sup_{x\in\mathbb{R}^n, x\neq 0} \frac{\|Ax\|}{\|x\|} = \sup_{x\in\mathbb{R}^n, \|x\|=1} \|Ax\|.$$

On a $\|Ax\| \leq \|A\|\,\|x\|$ pour tout $x \in \mathbb{R}^n$,
et $\|AB\| \leq \|A\|\,\|B\|$ pour toutes matrices carrées A et B.

Le rayon spectral de A est défini par :

$$\rho(A) = \max_{\lambda\in \mathrm{Spec}(A)} |\lambda|,$$

où les valeurs propres considérées peuvent être complexes. Il est bien connu [4] qu'il vérifie :

$$\rho(A) \leq \|A\|.$$

Dans le cas où A est symétrique, on peut montrer que l'on a l'égalité :

Proposition. Pour toute matrice carrée réelle symétrique A, on a : $\|A\| = \rho(A)$.

Preuve. Soit f l'endomorphisme de $\mathbb{R}^n$ dont A est la matrice dans la base canonique. Il est symétrique donc diagonalisable, et il existe une base orthonormale $\mathcal{B} = (e_1, \ldots, e_n)$ telle que $f(e_i) = \lambda_i e_i$ pour tout $1 \leq i \leq n$, avec $\lambda_1, \ldots, \lambda_n$ les valeurs propres, toutes réelles, de f ou A comptées avec leur multiplicité.

Soit x un vecteur de norme 1 dans $\mathbb{R}^n$, décomposé en $x = \sum_{i=1}^n \alpha_i e_i$ avec $\alpha_i \in \mathbb{R}$ tels que $\sum_{i=1}^n \alpha_i^2 = 1$. On calcule alors :

$$\|f(x)\|^2 = \|\sum_{i=1}^n \alpha_i\lambda_i e_i\|^2 = \sum_{i=1}^n \alpha_i^2\lambda_i^2 \leq \rho(A)^2 \sum_{i=1}^n \alpha_i^2 = \rho(A)^2.$$

On a donc $\|A\| \leq \rho(A)$. Il existe un entier $1 \leq k \leq n$ pour lequel $\rho(A) = |\lambda_k|$. Alors $\rho(A) = \|f(e_k)\|$ avec $\|e_k\| = 1$. On conclut que $\|A\| = \rho(A)$. □

Corollaire. Pour toute matrice carrée réelle A, on a :

$$\|A\| = \|{}^tA\| = \sqrt{\|{}^tAA\|} = \sqrt{\rho({}^tAA)}.$$

Preuve. Soit $x \in \mathbb{R}^n$ tel que $\|x\| = 1$. D'après l'inégalité de Cauchy-Schwarz :

$$\|Ax\|^2 = \langle Ax \,|\, Ax\rangle = \langle x \,|\, {}^tAAx\rangle \leq \|x\|\,\|{}^tAAx\| = \|{}^tAAx\| \leq \|x\|\,\|{}^tAA\| = \|{}^tAA\|.$$

D'après les propriété de la norme matricielle, on en déduit $\|A\|^2 \leq \|{}^tAA\| \leq \|{}^tA\|\,\|A\|$, d'où $\|A\| \leq \|{}^tA\|$. En échangeant les rôles des matrices ${}^tA$ et A, il vient $\|{}^tA\| = \|A\|$. La double inégalité ci-dessus devient alors $\|A\|^2 \leq \|{}^tAA\| \leq \|A\|^2$ et donc $\|A\|^2 = \|{}^tAA\|$. Enfin, puisque la matrice ${}^tAA$ est clairement symétrique, on déduit de la proposition précédente que $\|{}^tAA\| = \rho({}^tAA)$. □

4. Ce résultat se démontre de façon simple. Soit λ une valeur propre de A. Soit x un vecteur propre associé. Si l'on note B la matrice carrée dont la première colonne est x et les autres sont nulles, on a $\lambda B = AB$, donc $|\lambda| \times \|B\| = \|AB\| \leq \|A\| \times \|B\|$. Or $\|B\| \neq 0$ puisque x est non-nul, d'où $|\lambda| \leq \|A\|$.

► *Plus petite et plus grande valeur propre d'une matrice symétrique (quotients de Rayleigh).*

Proposition. Pour toute matrice carrée réelle symétrique $A = (a_{ij})_{1\leq i,j\leq n}$, la plus petite valeur propre λ_m et la plus grande λ_M de A sont données par :

$$\lambda_m = \inf_{x\in\mathbb{R}^n, x\neq 0}\left[\frac{{}^t xAx}{{}^t xx}\right] \quad \text{et} \quad \lambda_M = \sup_{x\in\mathbb{R}^n, x\neq 0}\left[\frac{{}^t xAx}{{}^t xx}\right],$$

et vérifient :

$$\lambda_m \leq a_{ii} \leq \lambda_M \quad \text{pour tout } 1 \leq i \leq n.$$

Preuve. On note f l'endomorphisme de $\mathbb{R}^n$ dont A est la matrice par rapport à la base canonique. On introduit les applications $q : \mathbb{R}^n \to \mathbb{R}$ et $r : \mathbb{R}^n \setminus \{0\} \to \mathbb{R}$ définie par :

$$q(x) = f(x)\cdot x = {}^t xAx \quad \text{et} \quad r(x) = \tfrac{1}{\|x\|^2}q(x) = \tfrac{{}^t xAx}{{}^t xx}.$$

La forme quadratique q est continue sur $\mathbb{R}^n$ (rappelons que $q(x)$ s'exprime comme un polynôme homogène de degré 2 en les coordonnées de x) donc elle est bornée sur la sphère unité $S = \{x \in \mathbb{R}^n\,;\, \|x\| = 1\}$ et atteint ses bornes. Il existe donc x_m et x_M dans S_n non-nuls tels que $q(x_m) = \inf\{q(x)\,;\, x \in S\}$ et $q(x_M) = \sup\{q(x)\,;\, x \in S\}$. Posons $\lambda_m = q(x_m)$ et $\lambda_M = q(x_M)$. Comme q et r coïncident sur S, on a encore $\lambda_m = \inf\{r(x)\,;\, x \in S\}$ et $\lambda_M = \sup\{r(x)\,;\, x \in S\}$. De plus, il est clair que pour tout $x \in \mathbb{R}^n$ non-nul et tout $\alpha \in \mathbb{R}^*$, $q(\alpha x) = \alpha^2 q(x)$ et donc $r(\alpha x) = r(x)$. On en déduit que :

$$\lambda_m = \inf\{r(x)\,;\, x \in \mathbb{R}^n, x \neq 0\} \quad \text{et} \quad \lambda_M = \sup\{r(x)\,;\, x \in \mathbb{R}^n, x \neq 0\}.$$

Montrons que λ_m est une valeur propre de f. Considérons pour cela la forme quadratique $Q : \mathbb{R}^n \to \mathbb{R}$ définie par : $Q(x) = q(x) - \lambda_m\|x\|^2 = (r(x) - \lambda_m)\|x\|^2$. Elle vérifie par définition $Q(x) \geq 0$ pour tout $x \in \mathbb{R}^n$, et $q(x_m) = 0$. Sa forme bilinéaire symétrique associée est définie par $\varphi(x, y) = f(x)\cdot y - \lambda_m x\cdot y$ pour tous $x, y \in \mathbb{R}^n$. L'inégalité de Cauchy-Schwarz pour $x = x_m$ et $y = x$ quelconque donne :

$$\big((f(x_m) - \lambda_m x_m)\cdot x\big)^2 = \varphi(x, x_m)^2 \leq Q(x_m)Q(x) = 0 \text{ pour tout } x \in \mathbb{R}^n.$$

Ainsi $(f(x_m) - \lambda_m x_m) \perp x$ pour tout $x \in \mathbb{R}^n$, d'où $f(x_m) = \lambda x_m$. Ceci prouve que λ_m est une vp de f, dont un vecteur propre associé est x_m.

Montrons que c'est la plus petite. Soit λ valeur propre de f. Il existe $y \in \mathbb{R}^n$ non-nul tel que $f(y) = \lambda y$, donc il existe $z \in S$, tel que $f(z) = \lambda z$. Alors $q(z) = f(z)\cdot z = \lambda z\cdot z = \lambda$, et comme $\lambda_m = \inf\{q(x)\,;\, x \in S\}$, on conclut que $\lambda_m \leq \lambda$.

On procède de même pour la plus grande valeur propre, ce qui achève la preuve du premier point.

Le second s'en déduit immédiatement en appliquant l'encadrement $\lambda_m \leq \frac{{}^t xAx}{{}^t xx} \leq \lambda_M$ au vecteur $x = e_i$ de la base canonique. □

► *Propriétés topologiques de certains sous-ensemble de matrices.*

On note $\mathcal{M}_n$ l'espace vectoriel des matrices carrées d'ordre n à coefficients réels, et $\mathcal{S}_n$ le sous-espace vectoriel des matrices symétriques,

Proposition.

(i) Le sous-ensemble $\mathcal{S}_n^{++}$ des matrices symétriques définies positives est un ouvert de $\mathcal{M}_n$.

(ii) Le sous-ensemble $\mathcal{S}_n^{+}$ des matrices symétriques positives est un fermé de $\mathcal{M}_n$ d'intérieur $\mathcal{S}_n^{++}$.

Preuve. Laissée au lecteur comme développement d'approfondissement. □

Polynômes d'endomorphismes en dimension finie

Dans tout ce qui suit, on désigne par E un K-espace vectoriel de dimension finie n.

1. Notion de polynôme d'endomorphisme

1.1 - L'algèbre non-commutative des endomorphismes de E

Considérons le K-espace vectoriel $(\operatorname{End} E, +, .)$ des endomorphismes de l'espace vectoriel E. On sait que $\operatorname{End} E$ est aussi un anneau (non commutatif) unitaire pour les lois $+$ et $\circ$. On a donc une double structure de K-espace vectoriel et d'anneau, avec de plus la propriété de cohérence suivante (évidente à vérifier) :

$$\lambda.(u \circ v) = (\lambda.u) \circ v = u \circ (\lambda.v) \text{ pour tous } u, v \in \operatorname{End} E, \lambda \in K.$$

On déduit par définition que :

$(\operatorname{End} E, +, \circ, .)$ *est une K-algèbre, non commutative, unitaire.*

En particulier l'élément neutre pour le produit interne dans $\operatorname{End} E$ est id_E, et l'on note $u^m = u \circ u \circ \ldots \circ u$, avec m facteurs.

1.2 - L'algèbre commutative des polynômes à coefficients dans K

En considérant sur $K[X]$ à la fois sa structure d'anneau commutatif unitaire et sa structure usuelle de K-espace vectoriel de $K[X]$, on vérifie aisément que :

$K[X]$ *est une K-algèbre, commutative, unitaire.*

▶ *Rappels.* Rappelons au passage quelques propriétés de l'anneau $K[X]$ utiles pour la suite. Parce que l'on considère ici des polynômes à coefficients dans un corps, l'anneau $K[X]$ est euclidien, donc principal. Cela signifie que tout idéal I de $K[X]$ est un idéal principal, i.e. engendré par un élément : il existe $P \in K[X]$ tel que $I = PK[X] = \{PQ\,;\, Q \in K[X]\}$. Si P est un générateur de I, les autres générateurs de I sont les polynômes associés à P, i.e. les polynômes de la forme αP avec $\alpha \in K^*$. Il résulte aussi du fait que $K[X]$ est principal que l'on a dans $K[X]$ une notion de pgcd et la propriété de Bézout.

1.3 - Morphisme canonique de $K[X]$ dans $\operatorname{End} E$ associé à un endomorphisme fixé

Proposition. *Pour tout $u \in \operatorname{End} E$ fixé, il existe un unique morphisme d'algèbres $\varphi_u : K[X] \to \operatorname{End} E$ tel que $\varphi_u(X) = u$. Il est défini par $P \mapsto P(u)$ où l'on pose :*

$$P(u) = \alpha_m.u^m + \alpha_{m-1}.u^{m-1} + \cdots + \alpha_1.u + \alpha_0.\,\mathrm{id}_E$$

lorsque $P = \sum_{i=0}^{m} \alpha_i X^i$ où $\alpha_i \in K$.

Preuve. Il est clair que φ_u est bien un morphisme d'algèbre $K[X] \to \operatorname{End} E$ tel que $\varphi_u(X) = u$. Pour l'unicité, supposons que φ est un morphisme d'algèbres $K[X] \to \operatorname{End} E$ tel que $\varphi(X) = u$. Si $P = \sum_{i=1}^{m} \alpha_i X^i$ est un élément de $K[X]$ quelconque, alors $\varphi(P) = \sum_{i=1}^{m} \varphi(\alpha_i X^i) = \sum_{i=1}^{m} \alpha_i \varphi(X)^i = \sum_{i=1}^{m} \alpha_i u^i$, ce qui prouve que $\varphi = \varphi_u$. □

On dit usuellement que « l'endomorphisme $P(u)$ est un polynôme en l'endomorphisme u ».

Deux remarques importantes au plan pratique.

- ▶ Attention au fait que $\varphi_u(\alpha_0) = \varphi_u(\alpha_0.1_K) = \alpha_0.\varphi_u(1_K) = \alpha_0.\,\mathrm{id}_E$.
- ▶ Bien qu'en général la loi $\circ$ ne soit pas commutative dans $\mathrm{End}\,E$, on a pour tout endomorphisme u de E et tous polynômes P et Q dans $K[X]$ les égalités :
$$P(u)\circ Q(u) = PQ(u) = QP(u) = Q(u)\circ P(u),$$
ceci découlant du fait que les différentes puissances de u commutent entre elles.

1.4 - Lemme des noyaux

Théorème. *Soit u un endomorphisme de E.*

(i) *Soient P et Q deux polynômes premiers entre eux dans $K[X]$, alors on a :*
$$\mathrm{Ker}(P(u)\circ Q(u)) = \mathrm{Ker}\,P(u) \oplus \mathrm{Ker}\,Q(u).$$

(ii) *Soient plus généralement $m \geq 2$ un entier et $P_1, P_2, \ldots, P_m$ des polynômes deux à deux premiers entre eux dans $K[X]$, alors on a :*
$$\mathrm{Ker}\Big(P_1(u)\circ P_2(u)\circ\cdots\circ P_m(u)\Big) = \mathrm{Ker}\,P_1(u) \,\oplus\, \mathrm{Ker}\,P_2(u) \,\oplus\cdots\oplus\, \mathrm{Ker}\,P_m(u)$$

Preuve. Si $x \in \mathrm{Ker}\,Q(u)$, alors $Q(u)(x) = 0_E$, donc $P(u)\big(Q(u)(x)\big) = 0_E$, c'est-à-dire $(P(u)\circ Q(u))(x) = 0_E$, ou encore $(PQ)(u)(x) = 0_E$, c'est-à-dire $x \in \mathrm{Ker}(PQ)(u)$; ceci prouve que $\mathrm{Ker}\,Q(u) \subset \mathrm{Ker}(PQ)(u)$. On montre de même que $\mathrm{Ker}\,P(u) \subset \mathrm{Ker}(PQ)(u)$ en utilisant le fait que $P(u)\circ Q(u) = Q(u)\circ P(u)$. Ansi $\mathrm{Ker}\,P(u)$ et $\mathrm{Ker}\,Q(u)$ sont deux sous-espaces vectoriels de $\mathrm{Ker}(PQ)(u)$, d'où :
$$\mathrm{Ker}\,P(u) + \mathrm{Ker}\,Q(u) \subseteq \mathrm{Ker}(PQ)(u).$$
▶ Pour la réciproque, utilisons le fait que P et Q sont premiers entre eux dans $K[X]$. Par le théorème de Bézout, il existe $H, G \in K[X]$ tels que $HP + GQ = 1$ dans $K[X]$. Donc $H(u)\circ P(u) + G(u)\circ Q(u) = \mathrm{id}_E$ dans $\mathrm{End}\,E$, et donc $x = H(u)(P(u)(x)) + G(u)(Q(u)(x))$ pour tout $x \in E$. Choisissons $x \in \mathrm{Ker}(PQ)(u)$. Il s'écrit comme on vient de le voir $x = y + z$ avec $y = H(u)(P(u)(x))$ et $z = G(u)(Q(u)(x))$. D'une part le vecteur y vérifie :
$Q(u)(y) = (Q(u)\circ H(u)\circ P(u))(x) = (H(u)\circ P(u)\circ Q(u))(x) = H(u)\big((PQ)(u)(x)\big) = H(u)(0_E) = 0_E$,
et donc $y \in \mathrm{Ker}\,Q(u)$.
D'autre part, le vecteur z vérifie :
$P(u)(z) = (P(u)\circ G(u)\circ Q(u))(x) = (G(u)\circ P(u)\circ Q(u))(x) = G(u)\big((PQ)(u)(x)\big) = G(u)(0_E) = 0_E$,
et donc $z \in \mathrm{Ker}\,P(u)$.
On a ainsi montré que $\mathrm{Ker}(PQ)(u) \subseteq \mathrm{Ker}\,P(u) + \mathrm{Ker}\,Q(u)$, et finalement :
$$\mathrm{Ker}(PQ)(u) = \mathrm{Ker}\,P(u) + \mathrm{Ker}\,Q(u).$$
Il reste à montrer que la somme est directe. Pour cela, considérons $x \in \mathrm{Ker}\,P(u) \cap \mathrm{Ker}\,Q(u)$. On a $P(u)(x) = 0_E$ donc $H(u)(P(u)(x)) = H(u)(0_E) = 0_E$. De même $Q(u)(x) = 0_E$ donc $G(u)(Q(u)(x)) = G(u)(0_E) = 0_E$. D'où $x = H(u)(P(u)(x)) + G(u)(Q(u)(x)) = 0_E + 0_E = 0_E$. On a ainsi prouvé que $\mathrm{Ker}\,P(u) \cap \mathrm{Ker}\,Q(u) = \{0_E\}$. On conclut que :
$$\mathrm{Ker}(PQ)(u) = \mathrm{Ker}\,P(u) \oplus \mathrm{Ker}\,Q(u).$$
▶ L'assertion (i) étant établie, l'assertion (ii) s'en déduit par récurrence sur m. Le résultat est vrai pour $m = 2$; supposons-le vrai jusqu'à un rang $m-1$. Soient $P_1, P_2, \ldots, P_m \in K[X]$ que l'on suppose deux à deux premiers entre eux. Alors P_m est premier avec $Q = P_1P_2\ldots P_{m-1}$ (en effet, il existerait sinon un facteur irréductible R commun à la décomposition de P_m et à celle de Q ; R apparaîtrait nécessairement dans la décomposition d'un P_{j_0} où $1 \leq j_0 \leq m-1$, ce qui contredirait le fait que P_m est premier avec P_{j_0}). L'assertion (i) montre alors que $\mathrm{Ker}(P_1P_2\ldots P_m)(u) = \mathrm{Ker}\,Q(u) \oplus \mathrm{Ker}\,P_m(u)$, et l'hypothèse de récurrence impliquant que $\mathrm{Ker}\,Q(u) = \mathrm{Ker}\,P_1(u) \oplus \mathrm{Ker}\,P_2(u) \oplus \cdots \oplus \mathrm{Ker}\,P_{m-1}(u)$, le résultat voulu à l'ordre m est établi. □

1.5 - Polynômes de matrices

En notant $\mathcal{M}_n(K)$ l'ensemble des matrices carrées d'ordre n à coefficients dans K, on a :

$$(\mathcal{M}_n(K), +, \times, .) \text{ est une } K\text{-algèbre, non commutative, unitaire, isomorphe à } \operatorname{End} E.$$

En effet, tout choix d'une base $\mathcal{B}$ de E permet de considérer la bijection $m : \operatorname{End} E \to \mathcal{M}_n(K)$ associant à tout endomorphisme u sa matrice $m(u)$ par rapport à la base $\mathcal{B}$. Elle vérifie :

$$m(u+v) = m(u) + m(v), \quad m(u \circ v) = m(u) \times m(v), \quad m(\lambda.u) = \lambda.m(u)$$

pour tous $u, v \in \operatorname{End} E, \lambda \in K$, et réalise donc un *isomorphisme d'algèbres unitaires*. En particulier on a bien $m(\mathrm{id}_E) = I_n$. Comme en 1.3, on montre que :

Proposition. *Pour tout $A \in \mathcal{M}_n(K)$ fixé, il existe un unique morphisme d'algèbres $\psi_A : K[X] \to \mathcal{M}_n(K)$ tel que $\psi_A(X) = A$. Il est défini par $P \mapsto P(A)$ où l'on pose :*

$$P(A) = \alpha_m.A^m + \alpha_{m-1}.A^{m-1} + \cdots + \alpha_1.A + \alpha_0.I_n$$

lorsque $P = \sum_{i=0}^{m} \alpha_i X^i$ où $\alpha_i \in K$.

On dit usuellement que « la matrice $P(A)$ est un polynôme en la matrice A ».

Avec les notations de 1.3, on a $\psi_A = m \circ \varphi_u$ pour tout choix d'une base de E avec $m(u) = A$.

2. Idéal d'annulation et polynôme minimal

2.1 - Idéal d'annulation

Proposition et définition. *On note O l'endomorphisme nul de E et O_n la matrice nulle dans $\mathcal{M}_n(K)$.*

(i) *Pour tout endomorphisme $u \in \operatorname{End} E$, l'ensemble N_u des polynômes $P \in K[X]$ tels que $P(u) = O$ est un idéal non nul de $K[X]$, appelé l'idéal d'annulation de l'endomorphisme u.*

(ii) *Pour toute matrice $A \in \mathcal{M}_n(K)$, l'ensemble N_A des polynômes $P \in K[X]$ tels que $P(A) = O_n$ est un idéal non nul de $K[X]$, appelé l'idéal d'annulation de la matrice A.*

Preuve. Avec les notations de 1.3, on a $N_u = \operatorname{Ker} \varphi_u$. Comme φ_u est un morphisme d'anneaux, son noyau est un idéal de $K[X]$. En tant que K-espaces vectoriels, $K[X]$ n'est pas de dimension finie alors que $\operatorname{End} E$ est de dimension n^2, donc φ_u n'est pas injectif, et donc l'idéal N_u n'est pas nul. La preuve est identique pour une matrice A. □

2.2 - Polynôme minimal

Proposition et définition.

(i) *Pour tout endomorphisme $u \in \operatorname{End} E$, il existe un unique polynôme unitaire $Q_u \in K[X]$ tel que N_u soit l'idéal principal engendré par Q_u dans $K[X]$. Le polynôme unitaire Q_u est appelé le polynôme minimal de l'endomorphisme u.*

(ii) *Pour toute matrice $A \in \mathcal{M}_n(K)$, il existe un unique polynôme unitaire $Q_A \in K[X]$ tel que N_A soit l'idéal principal engendré par Q_A dans $K[X]$. Le polynôme unitaire Q_A est appelé le polynôme minimal de la matrice A.*

Preuve. Comme on l'a rappelé en 1.2, l'anneau $K[X]$ est principal, donc l'idéal N_u est principal non nul. Il existe un unique polynôme unitaire Q_u tel que $N_u = Q_u K[X]$. La preuve est identique pour une matrice A. □

2.3 - Remarques

(1) Tout endomorphisme u annule son polynôme minimal Q_u, et un polynôme $P \in K[X]$ est annulé par u si et seulement s'il est multiple dans $K[X]$ du polynôme minimal Q_u de u :

$$\begin{cases} Q_u(u) = O, \\ \text{et} \\ \text{pour tout } P \in K[X],\ (P(u) = O) \Leftrightarrow (\text{ il existe } R \in K[X] \text{ tel que } P = RQ_u), \end{cases}$$

avec une formulation analogue en termes de matrices.

(2) Pour tout choix d'une base de E, si l'on a $u \in \operatorname{End} E$ et $A \in \mathcal{M}_n(K)$ avec $m(u) = A$, alors $N_u = N_A$ et $Q_u = Q_A$ d'après la dernière remarque de 1.5.

2.4 - Exemples

(1) Soient F et H deux sous-espaces vectoriels non nuls de E tels que $E = F \oplus H$. Soit s la symétrie par rapport à F parallèlement à H. *Alors le polynôme minimal de la symétrie* s *est* $Q_s = X^2 - 1$.

En effet, on a $s \circ s = \mathrm{id}_E$ dans $\operatorname{End} E$, donc s annule $X^2 - 1$, d'où $X^2 - 1 \in N_s$, et donc Q_s divise $X^2 - 1$. Mais ici $s \neq \mathrm{id}_E$ puisque $H \neq \{0_E\}$ et $s \neq -\mathrm{id}_E$ puisque $F \neq \{0_E\}$, d'où $X - 1 \notin N_s$ et $X + 1 \notin N_s$, et donc Q_s ne divise pas $X - 1$ ni $X + 1$. D'où le résultat. □

(2) En supposant toujours que $E = F \oplus H$ avec F et H non nuls, et en considérant cette fois la projection p de E sur F parallèlement à H, qui vérifie $p \circ p = p$, $p \neq \mathrm{id}_E$ et $p \neq O$, on montre de même que *le polynôme minimal de la projection* p *est* $Q_p = X^2 - X$.

(3) Soit u un endomorphisme de E. On suppose qu'il existe dans l'idéal d'annulation de u un polynôme P tel que $P(0) = 0$ et $P'(0) \neq 0$. On a alors $E = \operatorname{Ker} u \oplus \operatorname{Im} u$.

En effet, les hypothèses $P(0) = 0$ et $P'(0) \neq 0$ impliquent que le développement de P est de la forme $P = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_2 X^2 + a_1 X$ avec $m \geq 1$ et les a_i dans K tels que $a_1 \neq 0$.

Considérons un vecteur $y \in \operatorname{Ker} u \cap \operatorname{Im} u$. Il existe donc $x \in E$ tel que $y = u(x)$ et $u^2(x) = u(y) = 0_E$. Il en résulte que $u^3(x) = u(0_E) = 0_E$ et plus généralement $u^k(x) = 0_E$ pour tout $k \geq 2$. Donc l'endomorphisme $P(u) = \sum_{k=1}^{m} a_k u^k$ vérifie que $P(u)(x) = a_1 u(x) = a_1 y$. Mais $P(u)$ est l'endomorphisme nul puisque par hypothèse P est dans l'idéal d'annulation de u. De plus, a_1 est non-nul. Donc on a $y = 0_E$. On a ainsi montré que $\operatorname{Ker} u \cap \operatorname{Im} u = \{0_E\}$. Comme on sait par ailleurs par la formule du rang que $\dim \operatorname{Ker} u + \dim \operatorname{Im} u = n$, on conclut que $\operatorname{Ker} u \oplus \operatorname{Im} u = E$.

□

3. Polynômes d'endomorphismes et valeurs propres

Quelques rappels. Soit u un endomorphisme de E.

Une *valeur propre* de u dans K est un scalaire $\lambda \in K$ tel qu'il existe un vecteur $x \in E$ non nul vérifiant $u(x) = \lambda.x$. Un tel vecteur non nul x est alors appelé un *vecteur propre* associé à la valeur propre λ.

Si λ est une valeur propre de u dans K, le sous-espace vectoriel $E_\lambda = \mathrm{Ker}(u - \lambda\,\mathrm{id}_E)$ de E est appelé le *sous-espace propre* associé à la valeur propre λ. C'est donc l'ensemble des vecteurs $x \in E$ tels que $u(x) = \lambda x$, c'est-à-dire l'ensemble des vecteurs propres associés à λ auquel on adjoint le vecteur nul 0_E.

On appelle *polynôme caractéristique* de u le polynôme $P_u = \det(u - X.\,\mathrm{id}_E) \in K[X]$. Son degré est égal à la dimension n de E. Les zéros de P_u dans K sont exactement les valeurs propres de u dans K. La multiplicité d'une valeur propre λ dans K est l'exposant avec lequel le facteur $(X - \lambda)$ apparaît dans la décomposition du polynôme P_u en produit de facteurs irréductibles dans $K[X]$.

3.1 - Théorème de Cayley-Hamilton

Théorème. *Pour tout endomorphisme $u \in \mathrm{End}\,E$, le polynôme caractéristique de u appartient à l'idéal d'annulation de u.*

Preuve. Fixons un vecteur $x \in E$ non-nul. Parce que E est de dimension finie, il existe un entier $p \geq 1$ tel que la famille $\mathcal{C} = \{u^k(x)\}_{0 \leq k \leq p-1}$ est libre et $u^p(x)$ est une combinaison linéaire des vecteurs de $\mathcal{C}$. Notons $u_p(x) = \sum_{k=0}^{p-1} \alpha_i u^k(x)$. On peut compléter la famille $\mathcal{C}$ en une base $\mathcal{B}$ de E, et la matrice A de u dans la base $\mathcal{B}$ est alors de la forme :

$$A = \begin{pmatrix} C & B \\ O & D \end{pmatrix}$$

avec $C \in \mathcal{M}_{p,p}(K)$, $B \in \mathcal{M}_{p,n-p}(K)$, $D \in \mathcal{M}_{n-p,n-p}(K)$, et O la matrice nulle dans $\mathcal{M}_{n-p,p}(K)$. On en déduit en calculant les déterminants par blocs que le polynôme caractéristique de u (i.e. de A) est :

$$P_u(x) = P_A(X) = \begin{vmatrix} C - XI_p & N \\ O & D - XI_{n-p} \end{vmatrix} = \det(C - XI_n)\det(D - X_{n-p}) = P_C(X)P_D(X)$$

Or, par construction, on a :

$$C = \begin{pmatrix} 0 & 0 & \dots & 0 & \alpha_0 \\ 1 & 0 & \dots & 0 & \alpha_1 \\ 0 & 1 & \dots & 0 & \alpha_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & \alpha_{p-1} \end{pmatrix} \quad \text{(matrice dite compagnon).}$$

Il est facile de montrer (par exemple par récurrence, en développant par rapport à la première ligne) que

$$P_C(X) = (-1)^p \left[X^p - \textstyle\sum_{k=0}^{p-1} \alpha_k X^k\right].$$

Si l'on applique l'endomorphisme $P_C(u)$ au vecteur x choisi au départ, on a donc :

$$P_C(u)(x) = (-1)^p \left[u^p(x) - \textstyle\sum_{k=0}^{p-1} \alpha_k u^k(x)\right] = 0_E,$$

et donc, en utilisant le calcul de P_A fait précédemment :

$$P_A(u)(x) = (P_D(u) \circ P_C(u))(x) = P_D(u)(P_C(u)(x)) = P_D(u)(0_E) = 0_E.$$

Ceci étant établi pour tout vecteur $x \in E$, on conclut que $P_u(u)$ est l'endomorphisme nul, ce qui montre le résultat voulu. □

► *Un exemple d'application.*

Soient u et v deux endomorphismes d'un $\mathbb{C}$-espace vectoriel E ; les conditions suivantes sont équivalentes :

(i) u et v n'ont aucune valeurs propres communes

(ii) les polynômes caractéristiques P_u et P_v sont premiers entre eux

(iii) $P_u(v) \in \mathrm{GL}(E)$.

Preuve. Montrons que (i) implique (ii). Par contrposée, supposons que P_u et P_v ne sont pas premiers entre eux dans $\mathbb{C}[X]$. Il existe donc un polynôme $R \in \mathbb{C}[X]$ non-inversible (i.e. de degré ≥ 1) qui divise P_u et P_v dans $\mathbb{C}[X]$. Parce qu'on est dans $\mathbb{C}[X]$, ce polynôme non-constant admet au moins un zéro $\lambda \in \mathbb{C}$. Il est clair que λ est alors aussi un zéro de P_u et de P_v, et donc une valeur propre de u et de v.

Montrons que (ii) implique (iii). On suppose que P_u et P_v sont premiers entre eux dans $\mathbb{C}[X]$. Par la propriété de Bézout, il existe donc $U, V \in \mathbb{C}[X]$ tels que $P_u U + P_v V = 1$ dans $\mathbb{C}[X]$. On a donc dans $\mathrm{End}\, E$ l'égalité $P_u(v) \circ U(v) + P_v(v) \circ V(v) = \mathrm{id}_E$. Mais $P_v(v) = O$ d'après le théorème de Cayley-Hamilton ; donc $P_u(v) \circ U(v) = \mathrm{id}_E$. L'endomorphisme $P_u(v)$ est donc bijectif de bijection réciproque l'endomorphisme $U(v)$. En d'autres termes $P_u(v)$ est un automorphisme de l'espace vectoriel E, c'est-à-dire $P_u(v) \in \mathrm{GL}(E)$.

Montrons que (iii) implique (i). Par contraposée, supposons que u et v admettent une valeur propre commune $\lambda \in \mathbb{C}$. Il existe $x \in E$ non-nul tel que $v(x) = \lambda x$, et plus généralement $v^k(x) = \lambda^k x$ pour tout $k \geq 0$ avec la convention que $v^0 = \mathrm{id}_E$ et $\lambda^0 = 1$. Si l'on note $P_u(X) = \sum_{k=0}^m a_k X^k$, alors $P_u(v)$ est l'endomorphisme $P_u(v) = \sum_{k=0}^m a_k v^k$, donc :

$$P_u(v)(x) = \textstyle\sum_{k=0}^m a_k v^k(x) = \sum_{k=0}^m a_k \lambda^k x = P_u(\lambda)x.$$

Mais λ étant une valeur propre de u, on a $P_u(\lambda) = 0$ et donc $P_u(v) = 0_E$. Ceci prouve que le noyau de l'endomorphisme $P_u(v) \in \mathrm{End}\, E$ contient un vecteur non-nul. Donc $P_u(v)$ n'est pas injectif, donc pas bijectif, donc $P_u(v) \notin \mathrm{GL}(E)$. □

3.2 - Valeurs propres et polynôme minimal

Théorème. *Pour tout endomorphisme $u \in \mathrm{End}\, E$, on a :*

(i) *le polynôme caractéristique P_u est un multiple du polynôme minimal Q_u dans $K[X]$,*

(ii) *les zéros dans K du polynôme minimal Q_u sont exactement les valeurs propres de u dans K.*

Preuve. D'après le théorème de Cayley-Hamilton, P_u appartient à l'idéal d'annulation N_u de u. Comme N_u est l'idéal principal engendré par Q_u dans $K[X]$, il existe un polynôme R tel que $P_u = RQ_u$ dans $K[X]$, ce qui prouve (i).

Si $\lambda \in K$ un zéro de Q_u, on a $Q_u(\lambda) = 0$, donc $P_u(\lambda) = R(\lambda)Q_u(\lambda) = 0$, et donc λ est une valeur propre de u. Réciproquement, soit λ une valeur propre de u. Il existe donc un vecteur non nul x de E tel que $u(x) = \lambda.x$. En composant par u, on en déduit $u^2(x) = u(\lambda.x) = \lambda.u(x) = \lambda^2.x$, puis $u^3(x) = \lambda^3.x$ et finalement $u^j(x) = \lambda^j.x$ pour tout $j \geq 0$.

Posons $Q_u = X^m + \beta_{m-1}X^{m-1} + \cdots + \beta_1 X + \beta_0$, où $m = \deg Q_u \leq \deg P_u = n$ et où les β_i appartiennent à K. Par définition du polynôme minimal, $Q_u(u)$ est l'endomorphisme nul O de E. Donc :

$$\begin{aligned} 0_E = Q_u(u)(x) &= \left(u^m + \beta_{m-1}u^{m-1} + \cdots + \beta_1 u + \beta_0 \,\mathrm{id}_E\right)(x) \\ &= u^m(x) + \beta_{m-1}u^{m-1}(x) + \cdots + \beta_1 u(x) + \beta_0 x = \lambda^m.x + \beta_{m-1}\lambda^{m-1}.x + \cdots + \beta_1\lambda.x + \beta_0.x \\ &= Q_u(\lambda).x. \end{aligned}$$

Comme le vecteur x est non nul, on conclut que $Q_u(\lambda)$ est nul dans K. □

► *Un exemple d'application.*

Soient E un $\mathbb{C}$-espace vectoriel de dimension finie, u un endomorphisme de E, et A un polynôme de $\mathbb{C}[X]$. Alors l'endomorphisme $A(u)$ appartient à $\mathrm{GL}(E)$ si et seulement si A est premier avec le polynôme minimal de u dans $\mathbb{C}[X]$, et dans ce cas l'automorphisme réciproque $A(u)^{-1}$ est de la forme $B(u)$ pour un certain $B(X) \in \mathbb{C}[X]$.

Preuve. Posons $v = A(u)$ et considérons son polynôme caractéristique $P_v = \sum_{i=0}^{n} a_i X^i$, où $n \geq 1$ désigne la dimension de E. On sait que $a_n = (-1)^n$ et aussi que $a_0 = \det v$. Si l'on suppose que $v \in \mathrm{GL}(E)$ on a donc $a_0 \neq 0$. Comme d'après le théorème de Cayley-Hamilton $P_v(v) = O$, l'égalité $a_n v^n + \cdots + a_1 v + a_0 \,\mathrm{id}_E = O$ dans $\mathrm{End}\, E$ implique alors :

$$\mathrm{id}_E = -\tfrac{1}{a_0}(a_n v^n + \cdots + a_1 v) = -\tfrac{1}{a_0}(a_n v^{n-1} + \cdots + a_1 \,\mathrm{id}_E) \circ v$$

On en déduit que l'automorphisme réciproque $v^{-1} = A(u)^{-1}$ est de la forme $B(u)$ avec :

$$B(X) = -\tfrac{1}{a_0} \textstyle\sum_{i=1}^{n} a_i X^{i-1} \in \mathbb{C}[X].$$

Supposons que $A(u)$ appartient à $\mathrm{GL}(E)$. D'après la question précédente, il existe un polynôme $B \in \mathbb{C}[X]$ tel que $A(u) \circ B(u) = \mathrm{id}_E$ dans $\mathrm{End}\, E$. Cela signifie que le polynôme $AB - 1$ appartient à l'idéal d'annulation de u, et donc que ce polynôme est un multiple du polynôme minimal Q_u de u dans $\mathbb{C}[X]$: il existe ainsi $R \in \mathbb{C}[X]$ tel que $AB - 1 = RQ_u$, ou encore que $AB + (-R)Q_u = 1$. On conclut avec le théorème de Bézout que A et Q_u sont premiers entre eux.

La réciproque s'obtient en remontant les mêmes arguments et calculs. □

► *Remarque. Ainsi, le polynôme caractéristique P_u et le polynôme minimal Q_u ont exactement les mêmes zéros dans K, qui sont les valeurs propres de u dans K.*
En outre, P_u étant un multiple de Q_u, on a pour toute valeur propre λ de u :

$$1 \;\leq\; \begin{pmatrix}\text{la multiplicité de } \lambda \text{ en}\\ \text{tant que zéro de } Q_u\end{pmatrix} \;\leq\; \begin{pmatrix}\text{la multiplicité de } \lambda \text{ en}\\ \text{tant que zéro de } P_u\end{pmatrix}.$$

Notons enfin que tout ce que l'on vient de formuler en termes de polynôme minimal et de valeurs propres d'un endomorphisme peut être exprimé de façon analogue en termes de polynôme minimal et de valeurs propres d'une matrice carrée.

Exemple. Si une matrice $A \in \mathcal{M}_5(K)$ vérifie $P_A = -(X-2)^3(X+1)^2$. A priori, Q_A peut valoir :

$$\begin{array}{cccccccc} & (X-2)(X+1), & \text{ou} & (X-2)^2(X+1), & \text{ou} & (X-2)^3(X+1), \\ \text{ou} & (X-2)(X+1)^2, & \text{ou} & (X-2)^2(X+1)^2, & \text{ou} & (X-2)^3(X+1)^2. \end{array}$$

Pour déterminer ce que vaut effectivement Q_A, on peut calculer successivement tous les produits matriciels correspondants $(A - 2I_5)(A + I_5)$, $(A - 2I_5)^2(A + I_5)$..., jusqu'à obtenir un produit nul (sachant que de toute façon $(A - 2I_5)^3(A + I_5)^2$ est nul d'après le théorème de Cayley-Hamilton). On conçoit que de tels calculs directs sont vite fastidieux, voire inextricables à la main pour des matrices un peu grandes. D'où l'importance d'arguments théoriques plus généraux.

► *Rappel terminologique.* D'après la remarque précédente, et en vue des résultats suivants, on rappelle que :

1. Un polynôme $P \in K[X]$ est dit *scindé* sur K s'il se décompose en produit de facteurs de degré 1, c'est-à-dire qu'il est de la forme $P(X) = (X - \lambda_1)^{\alpha_1}(X - \lambda_2)^{\alpha_2} \cdots (X - \lambda_p)^{\alpha_p}$ avec $\lambda_1, \lambda_2, \ldots, \lambda_p$ deux à deux distincts dans K, et $\alpha_1, \alpha_2, \ldots, \alpha_p$ des entiers ≥ 1.

2. Un polynôme $P \in K[X]$ est dit *scindé à racines simples* sur K s'il se décompose en produit de facteurs de degré 1 deux à deux distincts, c'est-à-dire qu'il est de la forme $P(X) = (X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_p)$ avec $\lambda_1, \lambda_2, \ldots, \lambda_p$ deux à deux distincts dans K.

3.3 - Condition nécessaire et suffisante de diagonalisabilité

Théorème. *Un endomorphisme u de E est diagonalisable sur K si et seulement s'il existe dans l'idéal d'annulation de u un polynôme scindé à racines simples sur K.*

Preuve. Supposons que u est diagonalisable. Rappelons que cela signifie que u admet des valeurs propres $\lambda_1, \lambda_2, \ldots, \lambda_s$ (supposées par notation deux à deux distinctes) telles que $E = E_1 \oplus E_2 \oplus \cdots \oplus E_s$, où $E_j = \mathrm{Ker}(u - \lambda_j . \mathrm{id}_E)$ est le sous-espace propre associé à λ_j, pour tout $1 \leq j \leq s$. Introduisons dans $K[X]$ les polynômes $F = (X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_s)$ et $G_i = F/(X - \lambda_i) = \prod_{j \neq i}(X - \lambda_j)$ pour tout $1 \leq i \leq s$. On a $F(u) = G_i(u) \circ (u - \lambda_i . \mathrm{id}_E)$. Donc $F(u)(x) = 0_E$ pour tout $x \in E_i$. Donc $F(u)(x) = 0_E$ pour tout $x \in E$ puisque E est somme directe des E_i. On conclut que $F(u)$ est l'endomorphisme nul, ce qui prouve le résultat voulu (avec $p = s$).

Réciproquement, supposons satisfaite la condition de l'énoncé. Les polynômes $(X - \lambda_i)$ sont deux à deux premiers entre eux dans $K[X]$. D'après le lemme des noyaux, on a $E = \bigoplus_{i=1}^{p} \mathrm{Ker}(u - \lambda_i . \mathrm{id}_E)$, donc u est diagonalisable, ses sous-espaces propres étant ceux des $\mathrm{Ker}(u - \lambda_i . \mathrm{id}_E)$ qui ne sont pas nuls (leur nombre s peut être a priori $\leq p$). □

Corollaire. *Un endomorphisme u de E est diagonalisable sur K si et seulement si son polynôme minimal est de la forme $Q_u = (X - \lambda_1)(X - \lambda_2) \cdots (X - \lambda_s)$, où $\lambda_1, \lambda_2, \ldots, \lambda_s$ sont les valeurs propres distinctes de u dans K.*

Preuve. Découle immédiatement du théorème précédent, du point (ii) du théorème 3.2, et de la définition du polynôme minimal. □

3.4 - Condition nécessaire et suffisante de trigonalisabilité

Théorème. *Un endomorphisme u de E est trigonalisable sur K si et seulement s'il existe dans l'idéal d'annulation de u dans un polynôme scindé sur K.*

Preuve. On rappelle (sans le redémontrer ici) que u est trigonalisable sur K si et seulement si son polynôme caractéristique P_u est scindé dans $K[X]$. Comme P_u est dans l'idéal d'annulation de u, la première implication est trivialement vérifiée.

On montre l'implication réciproque par récurrence sur $n = \dim E$. Elle est claire pour $n = 1$, et on fait l'hypothèse de récurrence que tout endomorphisme d'un K-espace vectoriel de dimension $n-1$ dont l'idéal d'annulation N_u contient un polynôme scindé est trigonalisable. On considère alors u un endomorphisme de E de dimension n tel que N_u contienne un polynôme F scindé sur K. Ce dernier étant un multiple dans $K[X]$ du polynôme minimal Q_u, ce dernier est lui aussi scindé sur K. Notons

$$Q_u(X) = (X - \lambda_1)^{\alpha_1}(X - \lambda_2)^{\alpha_2} \cdots (X - \lambda_p)^{\alpha_p}$$

avec $\lambda_1, \ldots, \lambda_p$ deux à deux distincts dans K, et $\alpha_1, \ldots, \alpha_p$ des entiers ≥ 1. Si l'endomorphisme $u - \lambda_1 \mathrm{id}_E$ était bijectif, le polynôme $R(X) = Q_u(X)/(X - \lambda_1)$ vérifierait $R(u) = (u - \lambda_1 \mathrm{id}_E)^{-1} \circ Q_u(u) = O$, donc appartiendrait à N_u, ce qui est impossible par définition du polynôme minimal Q_u. Donc $u - \lambda_1 \mathrm{id}_E$ n'est pas bijectif, donc n'est pas surjectif (on est en dimension finie), donc le sous-espace vectoriel $\mathrm{Im}(u - \lambda_1 \mathrm{id}_E)$ est de dimension $\leq n - 1$. On peut alors considérer un hyperplan H de E qui contient $\mathrm{Im}(u - \lambda_1 \mathrm{id}_E)$. D'une part H est stable par $u - \lambda_1 \mathrm{id}_E$ (car plus généralement $(u - \lambda_1 \mathrm{id}_E)(E) = \mathrm{Im}(u - \lambda_1 \mathrm{id}_E) \subseteq H$), et donc H est stable par u. D'autre part Q_u reste de façon évidente dans l'idéal d'annulation de la restriction u' de u à H.

En appliquant l'hypothèse de récurrence à u', il existe une base $\mathcal{B}'$ de H telle que $\mathrm{Mat}_{\mathcal{B}'}(u')$ est triangulaire. Il suffit de compléter $\mathcal{B}'$ en ajoutant un vecteur de E n'appartenant pas à H pour obtenir une base $\mathcal{B}$ de E telle que $\mathrm{Mat}_{\mathcal{B}}(u)$ soit triangulaire. □

4. Sous-espaces caractéristiques

4.1 - Cas des endomorphismes nilpotents

Proposition. Soit u un endomorphisme de E nilpotent d'indice $m \geq 1$. Alors 0 est la seule valeur propre de E, le polynôme caractéristique de u est $P_u(X) = (-1)^n X^n$ et son polynôme minimal est $Q_u(X) = X^m$.

Preuve. Par hypothèse, $u^m = O$ et $u^k \neq O$ pour tout $0 \leq k \leq m-1$. Donc l'idéal d'annulation N_u contient le polynôme X^m mais ne contient pas X^{m-1}. Par définition du polynôme minimal comme générateur unitaire de N_u, on déduit que $Q_u(X) = X^m$. Donc d'après le point (ii) du théorème 3.2, la seule valeur propre de u est 0. De plus, puisque N_u contient X^m qui est scindé, il résulte du théorème 3.4 que u est trigonalisable. Donc le polynôme caractéristique P_u est scindé. Puisque la seule valeur propre de u est 0 et que P_u est de degré n, on ne peut avoir que $P_u(X) = (-1)^n X^n$. □

4.2 - Notion de sous-espace caractéristique

Définition. Soit u un endomorphisme de E. Soit λ une valeur propre de u, de multiplicité $q \in \mathbb{N}^*$. On appelle *sous-espace caractéristique* associé à la valeur propre λ, noté F_λ, le noyau de l'endomorphisme $(u - \lambda.\,\mathrm{id}_E)^q$.

Rappelons que dire que λ est de multiplicité q signifie que le polynôme caractéristique P_u est divisible dans $K[X]$ par $(X-\lambda)^q$, mais pas par $(X-\lambda)^{q+1}$. On sait que la multiplicité q est supérieure ou égale à la dimension du sous-espace propre E_λ, et que u est diagonalisable sur K si et seulement si ces deux entiers coïncident pour chacune des valeurs propres de u.

Il est clair que, pour toute valeur propre λ de u de multiplcité q dans K, on a :

$$F_\lambda = \mathrm{Ker}(u - \lambda.\,\mathrm{id}_E)^q \quad \supseteq \quad E_\lambda = \mathrm{Ker}(u - \lambda.\,\mathrm{id}_E) \quad \neq \quad \{0_E\}.$$

Proposition. *Soient u un endomorphisme de E. Pour toute valeur propre λ de u, la multiplicité de λ est égale à la dimension du sous-espace caractéristique F_λ.*

Preuve. Par définition de q, le polynôme caractéristique de u est de la forme $P_u = (X-\lambda)^q F$ avec $F \in K[X]$ tel que $F(\lambda) \neq 0$. Introduisons le sous-espace vectoriel $H = \mathrm{Ker}\, F(u)$ de E. Les polynômes $(X-\lambda)^q$ et F étant premiers entre eux dans $K[X]$, il résulte du lemme des noyaux que $E = F_\lambda \oplus H$. Le sous-espace vectoriel H est stable par u ; en effet, si $x \in H$, alors $F(u)(x) = 0_E$, or $F(u)(u(x)) = u(F(u)(x)) = u(0_E) = 0_E$ donc $u(x) \in H$. De même F_λ est stable par u.
On peut donc considérer la restriction v de u à F_λ et la restriction w de u à H, et l'on a $P_u = P_v P_w$ dans $K[X]$ (propriété classique du polynôme caractéristique, il suffit de choisir une base adaptée à la décomposition en somme directe et de faire la calcul des déterminants par blocs), avec la convention $P_w = 1$ dans le cas où $H = \{0_E\}$.
Notons $d = \dim F_\lambda$. Considérons $v' = v - \lambda.\,\mathrm{id}_{F_\lambda}$, qui est la restriction de $u - \lambda.\,\mathrm{id}_E$ à F_λ ; il est clair que c'est un endomorphisme nilpotent de F_λ, d'ordre $\leq q$. Donc d'après la proposition 4.1, on a $P_{v'} = (-1)^d X^d$, ce qui revient à dire que $P_v = (-1)^d (X-\lambda)^d$. Par ailleurs, par définition de H et de w, on a $F(w) = O$. Donc F est un multiple dans $K[X]$ du polynôme minimal Q_w de w. Comme $F(\lambda) \neq 0$, on a forcément $Q_w(\lambda) \neq 0$, ce qui prouve avec le théorème 3.2 que λ n'est pas une valeur propre de w, d'où $P_w(\lambda) \neq 0$. En résumé, $P_u = (-1)^d (X-\lambda)^d P_w$ avec $P_w(\lambda) \neq 0$, ce qui signifie que d est la multiplicité de la valeur propre λ. □

4.3 - Cas trigonalisable

On suppose dans ce paragraphe que P_u est scindé sur K, c'est-à-dire que u est trigonalisable sur K. C'est en particulier le cas pour tout endomorphisme de E si K est algébriquement clos, par exemple si $K = \mathbb{C}$.

On désigne par $\lambda_1, \lambda_2, \ldots, \lambda_s$ les valeurs propres *deux à deux distinctes* de u dans K, on a donc :

$$P_u = (-1)^n (X-\lambda_1)^{q_1}(X-\lambda_2)^{q_2}\cdots(X-\lambda_s)^{q_s}, \quad n = \deg P_u = q_1+q_2+\cdots+q_s,$$
$$Q_u = \qquad (X-\lambda_1)^{p_1}(X-\lambda_2)^{p_2}\cdots(X-\lambda_s)^{p_s}, \quad m = \deg Q_u = p_1+p_2+\cdots+p_s,$$

avec $1 \leq p_i \leq q_i \leq n$ pour tout $1 \leq i \leq s$. De plus, pour tout $1 \leq i \leq s$, on note :

$E_i = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)$ le sous-espace propre associé à λ_i, qui vérifie $\dim E_i \leq q_i$,

$F_i = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{q_i}$ le sous-espace caractéristique associé à λ_i, qui vérifie $\dim F_i = q_i$.

Proposition. *Sous les hypothèses et avec les notations ci-dessus :*

(i) *E est somme directe des sous-espaces caractéristiques : $E = F_1 \oplus F_2 \oplus \cdots \oplus F_s$.*

(ii) *Pour toute valeur propre λ_i de u, on a : $F_i = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{p_i}$.*

(iii) *De plus u est diagonalisable si et seulement si, pour toute valeur propre λ_i de u, on a $F_i = E_i$, ou encore de façon équivalente $p_i = 1$.*

Preuve. D'après le théorème de Cayley-Hamilton, on a $P_u(u) = O$, donc $E = \mathrm{Ker}\, P_u(u)$. Comme il est clair que les polynômes $(X-\lambda_i)^{q_i}$ sont deux à deux premiers entre eux, on applique alors le lemme des noyaux pour conclure que $E = \bigoplus_{i=1}^s \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{q_i}$, ce qui prouve le point (i).

On a aussi $Q_u(u) = O$, donc de la même façon $E = \bigoplus_{i=1}^s \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{p_i}$. Ainsi, en rappelant que $F_i = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{q_i}$ et en introduisant $H_i = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{p_i}$ pour tout $1 \leq i \leq s$, on a $H_i \subseteq F_i$ puisque $p_i \leq q_i$. Les égalités $E = \bigoplus_{i=1}^s F_i = \bigoplus_{i=1}^s H_i$ impliquent alors que $F_i = H_i$ pour tout $1 \leq i \leq s$. Ce qui montre le point (ii).

Le point (iii) découle du fait que u est diagonalisable si et seulement si $E = E_1 \oplus E_2 \oplus \cdots \oplus E_s$, et que par ailleurs chaque $E_i \subseteq F_i$ pour tout $1 \leq i \leq s$. □

4.4 - Application : décomposition de Dunford

Proposition. Pour tout endomorphisme trigonalisable u de E, il existe un unique endomorphisme diagonalisable d de E et un unique endomorphisme nilpotent n de E tels que $u = d + n$ avec $d \circ n = n \circ d$.
De plus, d et n sont des polynômes en l'endomorphisme u.

Preuve. En reprenant les notations de 4.3, on a $E = F_1 \oplus F_2 \oplus \cdots \oplus F_s$. Pour tout $1 \leq j \leq s$, le sous-espace F_j est stable par u (comme on l'a vu dans la preuve de la proposition 4.2) ; notons u_j l'endomorphisme de F_j défini par restriction de u.
Pour tout $1 \leq j \leq s$, considérons p_j la projection vectorielle sur F_j parallèlement à $H_j = \oplus_{i \neq j} F_i$. Posons $d = \sum_{j=1}^s \lambda_j p_j$. Il est clair que d est diagonalisable, qu'il admet les λ_j pour valeurs propres, avec les F_j comme sous-espaces propres associés respectifs. Notons $d_j = \lambda_j\,\mathrm{id}_{F_j}$ l'endomorphisme de F_j défini par restriction de d.

Introduisons alors l'endomorphisme $n = u - d$. Pour tout $1 \leq j \leq s$, le sous-espace F_j est stable par n et la restriction n_j de n à F_j est $n_j = u_j - d_j$. Les n_j sont donc nilpotents (par définition des F_j), d'où l'on déduit que n est nilpotent.
En reprenant la preuve du lemme des noyaux, on observe [5] que p_j est un polynôme en u pour tout $1 \leq j \leq s$. Il en résulte que d aussi (puisque $d = \sum_{j=1}^{s} \lambda_j p_j$), et donc n aussi (puisque $n = u - d$). Il en résulte (voir dernière remarque de 1.3) que n et d commutent pour la loi $\circ$. Ceci montre l'existence d'une décomposition.

Pour l'unicité, supposons qu'il existe une autre décomposition $u = d' + n'$ avec les mêmes propriétés. Comme d' commute avec n', il commute avec u, donc avec tout polynôme en u, donc avec d. D'après un résultat classique [6], il existe alors une même base de E dans laquelle les matrices de d' et de d sont simultanément diagonales, et donc $d - d'$ est diagonalisable.
De même, comme n' commute avec d', il commute avec u, donc avec tout polynôme en u, donc avec n. Il en résulte avec la formule du binôme que $n - n'$ est nilpotent. Ainsi l'endomorphisme $d - d' = n - n'$ est à la fois diagonalisable et nilpotent, donc nul, d'où $d = d'$ et $n = n'$. □

4.5 - Exemples d'utilisation de la suite des noyaux

On reprend ici toutes les hypothèses et notations du paragraphe 4.3. Pour toute valeur propre λ_i de u, on appelle *suite des noyaux* associée à λ_i la suite croissante des sous-espaces vectoriels :

$$\underbrace{E_i}_{\dim = r_i} = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E) \subseteq \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^2 \subseteq \cdots \subseteq \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{q_i} = \underbrace{F_i}_{\dim = q_i}.$$

Cette suite est donc formée de q_i sous-espaces, mais d'après le point (ii) de la proposition 4.3, elle est stationnaire à partir de $\mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{p_i} = \cdots = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{q_i} = F_i$.

Lemme. *Si pour un entier $\ell \geq 1$ on a $\mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{\ell+1} = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{\ell}$, alors $\mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{s} = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{\ell}$ pour tout $s \geq \ell$.*

Preuve. On fait une récurrence sur s pour montrer que la propriété :

$$(P_s) : \ \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{t} = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{\ell} \text{ pour tout } \ell \leq t \leq s$$

est vraie pour tout $s \geq \ell + 1$. Elle l'est pour $s = \ell + 1$ d'après l'hypothèse du lemme. Supposons par hypothèse de récurrence qu'il existe $s \geq \ell + 1$ tel que P_s soit vérifiée. On a en particulier :

$$\mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{s} = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{\ell} = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{s-1}.$$

Soit $x \in \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{s+1}$. On a : $(u - \lambda_i.\,\mathrm{id}_E)^{s}(u - \lambda_i.\,\mathrm{id}_E)(x) = (u - \lambda_i.\,\mathrm{id}_E)^{s+1}(x) = 0_E$, donc $(u - \lambda_i.\,\mathrm{id}_E)(x) \in \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{s}$.
En appliquant l'égalité précédente, il en résulte que : $(u - \lambda_i.\,\mathrm{id}_E)(x) \in \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{s-1}$, donc $(u - \lambda_i.\,\mathrm{id}_E)^{s}(x) = (u - \lambda_i.\,\mathrm{id}_E)^{s-1}(u - \lambda_i.\,\mathrm{id}_E)(x) = 0_E$, c'est-à-dire $x \in \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{s}$.
Ceci prouve que $\mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{s+1} \subset \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{s}$. L'inclusion inverse étant évidente, on conclut que $\mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{s+1} = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{s} = \mathrm{Ker}(u - \lambda_i.\,\mathrm{id}_E)^{\ell}$, ce qui montre (P_{s+1}) et achève la preuve du lemme. □

5. Si l'on reprend la preuve de l'assertion (i) du théorème 1.4, la décomposition d'un vecteur quelconque $x \in E$ sous la forme $x = y + z$ avec $y \in \mathrm{Ker}\, Q(u)$ et $z \in \mathrm{Ker}\, P(u)$ est telle que $y = H(u)(P(u)(x))$ et $z = G(u)(Q(u)(x))$, de sorte que la première projection est égale $p_1 = H(u) \circ P(u)$ et la seconde à $p_2 = G(u) \circ Q(u)$.

6. Si deux endomorphismes v et w sont diagonalisables et vérifient $v \circ w = w \circ v$, il existe une même base de E dans laquelle la matrice de v et celle de w sont simultanément diagonales. La preuve procède par récurrence sur la dimension de E.

▶ **Premier exemple illustratif.** Soit $A = \begin{pmatrix} -4 & 1 & 0 & 1 \\ -2 & -1 & 0 & 1 \\ -12 & 6 & 3 & 1 \\ -2 & 1 & 0 & -1 \end{pmatrix}$. Soit u l'endomorphisme de $\mathbb{R}^4$ dont la matrice dans la base canonique est A. On calcule $P_u = P_A = (X-3)(X+2)^3$.

Par les méthodes habituelles, on détermine $E_1 = \mathrm{Ker}(u - 3.\mathrm{id}_E)$ (on sait qu'il est de dimension 1) et $E_2 = \mathrm{Ker}(u + 2.\mathrm{id}_E)$. On trouve que $\dim E_2 = 1$ ce qui, comme -2 est v.p. triple, prouve que A n'est pas diagonalisable. A priori, le polynôme minimal de A peut valoir :

$$(X-3)(X+2)^3, \text{ ou } (X-3)(X+2)^2, \text{ ou } (X-3)(X+2).$$

Mais ce dernier cas est exclu puisque A n'est pas diagonalisable (voir corollaire 3.3).

Donc $(A-3I_4)(A+2I_4)$ est non nulle. Comme par ailleurs on sait que $(A-3I_4)(A+2I_4)^3$ est nulle d'après le théorème de Cayley-Hamilton, c'est le calcul de $(A-3I_4)(A+2I_4)^2$ qui permet de trancher. On fait le calcul de ce produit matriciel :

$$\begin{pmatrix} -7 & 1 & 0 & 1 \\ -2 & -4 & 0 & 1 \\ -12 & 6 & 0 & 1 \\ -2 & 1 & 0 & -4 \end{pmatrix} \begin{pmatrix} -2 & 1 & 0 & 1 \\ -2 & 1 & 0 & 1 \\ -12 & 6 & 5 & 1 \\ -2 & 1 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} -7 & 1 & 0 & 1 \\ -2 & -4 & 0 & 1 \\ -12 & 6 & 0 & 1 \\ -2 & 1 & 0 & -4 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -50 & 25 & 25 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = O_4.$$

On trouve $(A-3I_4)(A+2I_4)^2 = O_4$; on conclut que le polynôme minimal est $Q_A = (X-3)(X+2)^2$.

▶ **Second exemple illustratif.** Soit $A = \begin{pmatrix} 1 & -1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & -1 & 2 & 0 & 1 \\ 0 & 0 & 0 & 1 & -2 \\ 0 & 0 & 0 & 2 & -3 \end{pmatrix}$. Soit u l'endomorphisme de $\mathbb{R}^5$ dont la matrice dans la base canonique est A. On calcule $P_u = P_A = -(X-1)^3(X+1)^2$.

On détermine les sous-espaces propres ; on obtient :

$\lambda_1 = 1$, $\quad E_1 = \mathrm{Ker}(u - \mathrm{id}_E)$, de dimension $r_1 = 2$ [une base est $(e_1, e_2 + e_3)$] ;
$\lambda_2 = -1$, $\ E_2 = \mathrm{Ker}(u + \mathrm{id}_E)$, de dimension $r_2 = 1$ [une base est $(e_1 + e_2 + e_3 - 2e_4 - 2e_5)$].

Donc A n'est pas diagonalisable. En particulier, $Q_A \neq (X+1)(X-1)$.

On forme la suite des noyaux :

$E_1 = \mathrm{Ker}(u-\mathrm{id}_E) \subseteq \mathrm{Ker}(u-\mathrm{id}_E)^2 \subseteq \mathrm{Ker}(u-\mathrm{id}_E)^3 = F_1$, avec $\dim E_1 = r_1 = 2$ et $\dim F_1 = q_1 = 3$,
$E_2 = \mathrm{Ker}(u+\mathrm{id}_E) \subseteq \mathrm{Ker}(u+\mathrm{id}_E)^2 = F_2$, avec $\dim E_2 = r_2 = 1$ et $\dim F_2 = q_2 = 2$.

Le seul noyau à déterminer est $\mathrm{Ker}(u - \mathrm{id}_E)^2$ qui, au vu des dimensions, est égal à E_1 ou à F_1. Pour trancher, on peut faire la calcul direct de $(A - I_5)^2$. On peut aussi sans calcul utiliser le lemme du début de ce paragraphe : si l'on avait $\mathrm{Ker}(u - \mathrm{id}_E) = \mathrm{Ker}(u - \mathrm{id}_E)^2$, on aurait aussi $\mathrm{Ker}(u - \mathrm{id}_E) = \mathrm{Ker}(u - \mathrm{id}_E)^3$, c'est-à-dire $E_1 = F_1$, ce qui est absurde. Donc $\mathrm{Ker}(u - \mathrm{id}_E)^2 = F_1$.
En résumé :

$$\underbrace{E_1}_{r_1=2} = \mathrm{Ker}(u - \mathrm{id}_E) \subsetneq \mathrm{Ker}(u - \mathrm{id}_E)^2 = \mathrm{Ker}(u - \mathrm{id}_E)^3 = \underbrace{F_1}_{q_1=3},$$
$$\underbrace{E_2}_{r_2=1} = \mathrm{Ker}(u + \mathrm{id}_E) \subsetneq \mathrm{Ker}(u + \mathrm{id}_E)^2 = \underbrace{F_2}_{q_2=2}.$$

D'après le lemme des noyaux, $\mathrm{Ker}\big[(u-\mathrm{id}_E)\circ(u+\mathrm{id}_E)^2\big] = \mathrm{Ker}(u-\mathrm{id}_E) \oplus \mathrm{Ker}(u+\mathrm{id}_E)^2 = E_1 \oplus F_2$. Ce noyau est donc de dimension $r_1 + q_2 = 4 < 5$, de sorte que l'endomorphisme $(u-\mathrm{id}_E)\circ(u+\mathrm{id}_E)^2$ n'est pas nul, ou encore $(A - I_5)(A + I_5)^2 \neq O_5$.
De même, $\mathrm{Ker}\big[(u - \mathrm{id}_E)^2 \circ (u + \mathrm{id}_E)\big] = \mathrm{Ker}(u - \mathrm{id}_E)^2 \oplus \mathrm{Ker}(u + \mathrm{id}_E) = F_1 \oplus E_2$ est de dimension $q_1 + r_2 = 4 < 5$, de sorte que l'endomorphisme $(u - \mathrm{id}_E)^2 \circ (u + \mathrm{id}_E)$ n'est pas nul, ou encore $(A - I_5)^2(A + I_5) \neq O_5$.
En revanche, $\mathrm{Ker}\big[(u - \mathrm{id}_E)^2 \circ (u + \mathrm{id}_E)^2\big] = \mathrm{Ker}(u - \mathrm{id}_E)^2 \oplus \mathrm{Ker}(u + \mathrm{id}_E)^2 = F_1 \oplus F_2 = \mathbb{R}^5$, de sorte que l'endomorphisme $(u - \mathrm{id}_E)^2 \circ (u + \mathrm{id}_E)^2$ est nul, c'est-à-dire $(A - I_5)^2(A + I_5)^2 = O_5$.
On conclut que le polynôme minimal est $Q_A = (X-1)^2(X+1)^2$.

Notion de rang en algèbre linéaire

1. Différentes définitions équivalentes du rang

1.1 - Rang d'une famille de vecteurs

Soient $\mathbb{K}$ un corps commutatif et E un $\mathbb{K}$-espace vectoriel.

Définition. Soit $\mathcal{C} = (u_i)_{i\in I}$ une famille de vecteurs de E. On dit que $\mathcal{C}$ est de *rang fini* si le sous-espace vectoriel $\operatorname{Vect}\mathcal{C}$ engendré par $\mathcal{C}$ est de dimension finie. Dans ce cas, $\dim \operatorname{Vect}\mathcal{C}$ est appelé le *rang de la famille de vecteurs* $\mathcal{C}$. On le note $\operatorname{rg}\mathcal{C}$.

En d'autres termes, $\operatorname{rg}\mathcal{C} = r$ signifie qu'il existe une sous-famille formée de r vecteurs de $\mathcal{C}$ qui est libre, et que toute sous-famille formée de $m > r$ vecteurs de $\mathcal{C}$ est liée.

Remarque 1. Si $\mathcal{C} = (u_1, u_2, \dots, u_n)$ est finie, on a nécessairement $\operatorname{rg}\mathcal{C} \leq n$.

Remarque 2. Si E est de dimension finie p, on a nécessairement $\operatorname{rg}\mathcal{C} \leq p$.

1.2 - Rang d'une application linéaire

Soient $\mathbb{K}$ un corps commutatif, et E et F deux $\mathbb{K}$-espaces vectoriels.

Définition. Soit f une application linéaire de E dans F. On dit que f est de *rang fini* si le sous-espace vectoriel $\operatorname{Im} f$ est de dimension finie. Dans ce cas, $\dim \operatorname{Im} f$ est appelé le *rang de l'application linéaire* f. On le note $\operatorname{rg} f$.

Rappelons que $\operatorname{Im} f = f(E) = \{f(u)\,;\, u \in E\} = \{v \in F,\ \exists\, u \in E,\ v = f(u)\}$ est un sous-espace vectoriel de F.

Remarque 1. Si F est de dimension finie p, on a nécessairement $\operatorname{rg} f \leq p$.

Remarque 2. Si E est de dimension finie n, on a nécessairement $\operatorname{rg} f \leq n$.

Théorème ("formule du rang"). Soit f une application linéaire de E dans F. Si E est de dimension finie, alors on a :

$$\dim \operatorname{Ker} f + \operatorname{rg} f = \dim E.$$

Rappelons que $\operatorname{Ker} f = \{u \in E,\ f(u) = 0_F\}$ est un sous-espace vectoriel de E.

Principales idées de la preuve. Notons $n = \dim E$ et prenons $(u_1, \dots, u_n)$ une base de E. Alors la famille $(f(u_1), \dots, f(u_n)$ est une famille génératrice de $\operatorname{Im} f$. Il en résulte que $\operatorname{Im} f$ est de dimension finie avec $\dim \operatorname{Im} f \leq n$. Par ailleurs, en utilisant le théorème de la base incomplète, on peut considérer un supplémentaire H de $\operatorname{Ker} f$ dans E. La restriction de f à H est alors un isomorphisme de H sur $\operatorname{Im} f$. On conclut que $\operatorname{rg} f = \dim \operatorname{Im} f = \dim H = \dim E - \dim \operatorname{Ker} f$.

Corollaire. Soit f un endomorphisme de E, avec E de dimension finie. Alors f est injective si et seulement si f est surjective (et donc bijective).

1.3 - Rang d'un système d'équations linéaires

Soit $\mathbb{K}$ un corps commutatif.

Définition. Soit (S) un système linéaire de p équations à n inconnues, à coefficients dans $\mathbb{K}$. On appelle *rang du système* (S) l'entier naturel :

$$\mathrm{rg}(S) = n - d$$

où d est la dimension du sous-espace vectoriel des solutions dans $\mathbb{K}^n$ du système homogène (S_0) associée à (S).

Remarque. Si (S) est de rang r, il équivaut à un système de r équations dites équations principales (les $p - r$ autres étant des combinaisons linéaires de celles-ci) à r inconnues dites inconnues principales (les $n - r$ autres étant considérées comme des paramètres dans la résolution).

1.4 - Rang d'une matrice

Soient $\mathbb{K}$ un corps commutatif et $A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & & \vdots \\ a_{p,1} & a_{p,2} & \dots & a_{p,n} \end{pmatrix} \in \mathcal{M}_{p,n}(\mathbb{K})$.

On appelle *matrice extraite de A* toute matrice à p' lignes et n' colonnes (avec $p' \leq p$ et $n' \leq n$) obtenue en supprimant $p - p'$ lignes et $n - n'$ colonnes de A, en laissant à la même position les coefficients restants.

Définition. On appelle *rang de la matrice A*, noté $\mathrm{rg}\, A$, le maximum des ordres des matrices carrées extraites de A qui sont inversibles.

En d'autres termes, $\mathrm{rg}\, A = r$ signifie qu'il existe une matrice d'ordre r extraite de A qui est inversible, et que toute matrice carrée d'ordre $m > r$ extraite de A est non-inversible.

▶ *Lien avec les définitions précédentes.*

Soit $A \in \mathcal{M}_{p,n}(\mathbb{K})$ comme ci-dessus. On associe à cette matrice :

- la famille $\mathcal{C} = (u_1, u_2, \dots, u_n)$ de vecteurs de $\mathbb{K}^p$ formée par les colonnes de A
- l'application linéaire f de $\mathbb{K}^n$ dans $\mathbb{K}^p$ telle que A soit la matrice de f par rapport aux bases canoniques de $\mathbb{K}^n$ et $\mathbb{K}^p$
- le système linéaire homogène de p équations à n inconnues suivant :

$$(S_0)\ \begin{cases} a_{1,1}x_1 + a_{1,2}x_2 + \cdots + a_{1,n}x_n = 0 \\ a_{2,1}x_1 + a_{2,2}x_2 + \cdots + a_{2,n}x_n = 0 \\ \cdots \\ a_{p,1}x_1 + a_{p,2}x_2 + \cdots + a_{p,n}x_n = 0 \end{cases} \quad \text{i.e.} \quad A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Théroème. On a $\mathrm{rg}\, A = \mathrm{rg}\, \mathcal{C} = \mathrm{rg}\, f = \mathrm{rg}(S_0)$, avec $0 \leq \mathrm{rg}\, A \leq \min(n, p)$.

Remarque. La deuxième et la troisième égalités sont évidentes, car $\mathrm{Vect}\, \mathcal{C} = \mathrm{Im}\, f$ et le sous-espace vectoriel des solutions du système (S_0) est égal à $\mathrm{Ker}\, f$. Il n'en est pas de même de la première égalité, dont la preuve utilise les arguments développés dans la section 2 du document.

► *Matrices carrées de rang maximal.*

Corollaire. Soient A une matrice carré d'ordre n à coefficient dans $\mathbb{K}$, $\mathcal{C}$ la famille des n vecteurs colonnes de A dans $\mathbb{K}^n$, f l'endomorphisme de $\mathbb{K}^n$ tel que A soit la matrice de f dans la base canonique de $\mathbb{K}^n$, et (S_0) le système linéaire homogène de n équations à n inconnues dont la matrice des coefficients est A. Les conditions suivantes sont équivalentes :

(i) $\operatorname{rg} A = \operatorname{rg} \mathcal{C} = \operatorname{rg} f = \operatorname{rg} (S_0) = n$,
(ii) la famille $\mathcal{C}$ est une base de $\mathbb{K}^n$,
(iii) l'endomorphisme f est bijectif,
(iv) le système (S_0) admet pour unique solution le vecteur nul de $\mathbb{K}^n$,
(v) la matrice A est inversible.

2. Propriétés et méthodes de calcul du rang

2.1 - Matrices équivalentes

Définition. Soient A et B deux matrices de $\mathcal{M}_{p,n}(\mathbb{K})$. Elles sont dites équivalentes lorsqu'il existe des matrices carrées inversibles P et Q d'ordre n et p respectivement telles que : $B = QAP$.

Remarque. Cela signifie que A et B représentent la même application linéaire f d'un espace vectoriel E de dimension n dans un espace vectoriel F de dimension p, par rapport à deux couples de bases de E et de F respectivement, les matrices Q et P s'interprétant comme les matrices de changement de bases associées.

Lemme. Soit A une matrice de $\mathcal{M}_{p,n}(\mathbb{K})$. Soit r un entier $0 \leq r \leq \min(p, n)$. Alors $\operatorname{rg} A = r$ si et seulement si A est équivalente à la matrice :

$$J_{p,n}^r = \begin{pmatrix} I_r & O_{r,n-r} \\ O_{p-r,r} & O_{p-r,n-r} \end{pmatrix}$$

obtenue en complétant la matrice carrée identité I_r par $n-r$ colonnes de zéros à droite et $p-r$ lignes de zéros en bas.

Remarque 1. C'est de ce lemme (que l'on montre en prenant d'abord pour r le rang de f ou de $\mathcal{C}$ au sens des notations du paragraphe 1.4) que l'on déduit le théorème 1.4.

Remarque 2. On en déduit aussi le résultat suivant qui caractérise le rang comme l'invariant de classification associé à la relation d'équivalence des matrices.

Théorème. Deux matrices de $\mathcal{M}_{p,n}(\mathbb{K})$ sont équivalentes si et seulement si elles ont le même rang.

Corollaire. Toute matrice est de même rang que sa transposée.

2.2 - Rang et transformations élémentaires

Proposition. Soit $A \in \mathcal{M}_{p,n}(\mathbb{K})$. Le rang de A est égal à celui de la matrice obtenue à partir de A en appliquant l'une des six transformations élémentaires suivantes :

1. échanger deux colonnes, ou échanger deux lignes,
2. multiplier une colonne, ou une ligne, par un scalaire non-nul,
3. ajouter à une colonne une combinaison linéaire des autres colonnes, ou ajouter à une ligne une combinaison linéaire des autres lignes.

En appliquant les transformations élémentaires détaillées ci-dessus, on se ramène à une matrice A' de même rang que A et qui est *échelonnée*, c'est-à-dire dont le nombre de zéros en début de chaque ligne augmente strictement de ligne en ligne. Le rang de A' est alors facile à calculer.

3. Exemples et exercices

3.1 - Une illustration numérique des différents point de vue sur le rang

Calculer suivant quatre raisonnements différents le rang de $A = \begin{pmatrix} 1 & 2 & 1 & 3 & 3 \\ 0 & -1 & -1 & -1 & -2 \\ 2 & 0 & -2 & 2 & -2 \\ 1 & 0 & 1 & 1 & 1 \end{pmatrix} \in \mathcal{M}_{4,5}(\mathbb{R})$.

a) Premier point de vue. On introduit la famille $\mathcal{C} = (u_1, u_2, u_3, u_4, u_5)$ formée des 5 vecteurs de $\mathbb{R}^4$ correspondant aux colonnes de A. Donc :

$$u_1 = (1,0,2,1),\ u_2 = (2,-1,0,0),\ u_3 = (1,-1,-2,1),\ u_4 = (3,-1,2,1),\ u_5 = (3,-2,-2,1).$$

On a : $u_4 = u_1 + u_2$ et $u_5 = u_2 + u_3$, de sorte que $\operatorname{Vect}\mathcal{C} = \operatorname{Vect}(u_1, u_2, u_3)$. On montre par un calcul facile que (u_1, u_2, u_3) est libre. Donc (u_1, u_2, u_3) est une base de $\operatorname{Vect}\mathcal{C}$. Ceci prouve que $\dim \operatorname{Vect}\mathcal{C} = 3$. On conclut que $\operatorname{rg} A = 3$.

b) Deuxième point de vue. On introduit le système homogène de 4 équations à 5 inconnues (notées ici x, y, z, t, s) dont A est la matrice :

$$(S_0) \begin{cases} x + 2y + z + 3t + 3s = 0 & (1) \\ -y - z - t - 2s = 0 & (2) \\ 2x - 2z + 2t - 2s = 0 & (3) \\ x + z + t + s = 0 & (4) \end{cases}$$

On obtient un système équivalent en remplaçant (3) par (3) $-\ 2 \times$ (1), et (4) par (4) $-$ (1) :

$$(S_0) \Leftrightarrow \begin{cases} x + 2y + z + 3t + 3s = 0 & (1) \\ -y - z - t - 2s = 0 & (2) \\ -4y - 4z - 4t - 8s = 0 & (3') \\ -2y - 2t - 2s = 0 & (4') \end{cases}, \quad \text{puis} \quad (S_0) \Leftrightarrow \begin{cases} x + 2y + z + 3t + 3s = 0 \\ y + z + t + 2s = 0 \\ y + t + s = 0 \end{cases},$$

en remarquant que (3′) et (2) sont équivalentes, et en simplifiant (2) par -1 et (4′) par -2. On en tire :

$$(S_0) \Leftrightarrow \begin{cases} y = -t - s \\ z = -t - 2s - y = -t - 2s - (-t-s) = -s \\ x = -3t - 3s - z - 2y = -3t - 3s - (-s) - 2(-t-s) = -t \end{cases}$$

Le sous-espace vectoriel des solutions de (S_0) est $F_0 = \{(-t, -t-s, -s, t, s)\,;\, t, s \in \mathbb{R}\}$, c'est-à-dire le plan vectoriel de $\mathbb{R}^5$ de base (u, v) avec $u = (-1,-1,0,1,0)$ et $v = (0,-1,-1,0,1)$. Le rang de (S_0) est égal à $5 - \dim F_0 = 5 - 2 = 3$. On conclut que $\operatorname{rg} A = 3$.

c) Troisième point de vue. Soit f l'application linéaire de $\mathbb{R}^5$ dans $\mathbb{R}^4$ telle que A soit la matrice de f par rapport aux bases canoniques. Pour tout vecteur $u = (x, y, z, t, s) \in \mathbb{R}^5$, on a :

$$u \in \operatorname{Ker} f \quad \Leftrightarrow \quad f(u) = (0,0,0,0) \quad \Leftrightarrow \quad A \begin{pmatrix} x \\ y \\ z \\ t \\ s \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \quad \Leftrightarrow \quad u \text{ est solution de } (S_0).$$

Comme on l'a vu au b) ci-dessus, le sous-espace vectoriel des solutions de (S_0) est un plan. Donc $\dim \operatorname{Ker} f = 2$. Comme $\dim \operatorname{Im} f + \dim \operatorname{Ker} f = \dim \mathbb{R}^5 = 5$, on en déduit $\operatorname{rg} f = \dim \operatorname{Im} f = 5 - 2 = 3$. On conclut que $\operatorname{rg} A = 3$.

d) Quatrième point de vue. On raisonne sur les matrices carrées extraites inversibles. Comme $\operatorname{rg} A$ est inférieur ou égal au nombre de lignes et au nombre de colonnes, on a : $\operatorname{rg} A \leq 4$.

► A est de rang 4 si et seulement s'il existe une matrice carrée d'ordre 4 extraite de A qui est inversible. Or, il existe ici 5 matrices carrées d'ordre 4 extraites de A (on les obtient en supprimant l'une des colonnes de A). Notons-les :

$$A_1 = \begin{pmatrix} 2 & 1 & 3 & 3 \\ -1 & -1 & -1 & -2 \\ 0 & -2 & 2 & -2 \\ 0 & 1 & 1 & 1 \end{pmatrix}, \qquad A_2 = \begin{pmatrix} 1 & 1 & 3 & 3 \\ 0 & -1 & -1 & -2 \\ 2 & -2 & 2 & -2 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \qquad A_3 = \begin{pmatrix} 1 & 2 & 3 & 3 \\ 0 & -1 & -1 & -2 \\ 2 & 0 & 2 & -2 \\ 1 & 0 & 1 & 1 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & -1 & -1 & -2 \\ 2 & 0 & -2 & -2 \\ 1 & 0 & 1 & 1 \end{pmatrix}, \qquad A_5 = \begin{pmatrix} 1 & 2 & 1 & 3 \\ 0 & -1 & -1 & -1 \\ 2 & 0 & -2 & 2 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

Désignons par u_1, u_2, u_3, u_4, u_5 les vecteurs colonnes de A dans $\mathbb{R}^4$.
La matrice A_1 est celle de la famille (u_2, u_3, u_4, u_5). Comme on a $u_5 = u_2 + u_3$, cette famille est liée, donc la matrice A_1 n'est pas inversible.
Par le même raisonnement, A_4 n'est pas inversible car $u_5 = u_2 + u_3$, A_5 et A_3 ne sont pas inversibles car $u_4 = u_1 + u_2$, et A_2 n'est pas inversible car $u_5 = u_3 + u_4 - u_1$.
On a ainsi vérifié que toutes les matrices carrées d'ordre 4 extraites de A sont non-inversibles, ce qui prouve que $\operatorname{rg} A < 4$.

► On regarde ensuite les matrices carrées d'ordre 3 extraites de A. Si l'une au moins est inversible, cela suffit à prouver que $\operatorname{rg} A = 3$. Or, la matrice obtenue en supprimant dans A la 1ère ligne et les deux dernières colonnes est $M = \begin{pmatrix} 0 & -1 & -1 \\ 2 & 0 & -2 \\ 1 & 0 & 1 \end{pmatrix}$, qui est inversible.

Conclusion : on a montré que toutes les matrices carrées d'ordre 4 extraites de A sont non-inversibles, et qu'il existe une matrice carrée d'ordre 3 extraite de A qui est inversible ; ceci prouve que $\operatorname{rg} A = 3$.

3.2 - Une illustration numérique de l'application des opérations élémentaires

Calculer le rang de $A = \begin{pmatrix} 1 & a+1 & 2a^2 & 2a^2+2 \\ -1 & a-1 & a-a^2 & 3a-a^2-2 \\ 0 & a & a^2 & a^2+a \\ 1 & a+1 & 2a & 2a+2 \end{pmatrix} \in \mathcal{M}_{4,4}(\mathbb{R})$, où $a \in \mathbb{R}$ fixé.

On garde L_1 et L_3,
on remplace L_2 par $L_2 + L_1$,
on remplace L_4 par $L_4 - L_1$; on obtient : $A_1 = \begin{pmatrix} 1 & a+1 & 2a^2 & 2a^2+2 \\ 0 & 2a & a+a^2 & 3a+a^2 \\ 0 & a & a^2 & a^2+a \\ 0 & 0 & 2a-2a^2 & 2a-2a^2 \end{pmatrix}$.

On garde L_1, L_2 et L_4,
on remplace L_3 par $2L_3$
puis par $2L_3 - L_2$; on obtient : $A_2 = \begin{pmatrix} 1 & a+1 & 2a^2 & 2a^2+2 \\ 0 & 2a & a+a^2 & 3a+a^2 \\ 0 & 0 & a^2-a & a^2-a \\ 0 & 0 & 2(a-a^2) & 2(a-a^2) \end{pmatrix}$.

On garde L_1, L_2, L_3,
on remplace L_4 par $L_4 + 2L_3$; on obtient : $A_3 = \begin{pmatrix} 1 & a+1 & 2a^2 & 2a^2+2 \\ 0 & 2a & a+a^2 & 3a+a^2 \\ 0 & 0 & a^2-a & a^2-a \\ 0 & 0 & 0 & 0 \end{pmatrix}$.

Finalement, $\operatorname{rg} A = \operatorname{rg} A_3 = \begin{cases} 1 & \text{si } a = 0 \\ 2 & \text{si } a = 1 \\ 3 & \text{si } a \notin \{0, 1\} \end{cases}$.

3.3 - Quelques propriétés classiques en exercice

► *Rang de la somme de deux applications linéaires.*

Soient E et F deux espaces vectoriels de dimensions finies. Soient f et g deux applications linéaires de E vers F. Montrer que :

$$\text{(i) } |\operatorname{rg}(f)-\operatorname{rg}(g)| \leq \operatorname{rg}(f+g) \leq \operatorname{rg}(f)+\operatorname{rg}(g),$$
$$\text{(ii) } \operatorname{rg}(f+g)=\operatorname{rg}(f)+\operatorname{rg}(g) \text{ si et seulement si } \begin{cases}\operatorname{Im} f \cap \operatorname{Im} g = \{0_F\}\\ \operatorname{Ker} f + \operatorname{Ker} g = E.\end{cases}.$$

► *Rang de la composée de deux endomorphismes.*

Soit E un espace vectoriel de dimension finie. Soit f un endomorphisme de E. Montrer que :

$$\text{(i) } \operatorname{rg} f + \operatorname{rg} g - \dim E \leq \operatorname{rg}(g\circ f) \leq \min(\operatorname{rg} f, \operatorname{rg} g),$$
$$\text{(ii) } \operatorname{rg}(g\circ f) = \begin{cases}\operatorname{rg} g & \text{si et seulement si } E = \operatorname{Im} f + \operatorname{Ker} g\\ \operatorname{rg} f & \text{si et seulement si } \operatorname{Im} f \cap \operatorname{Ker} g = \{0_E\}\end{cases}$$

► *Rang d'une sous-famille de vecteurs.*

Soit $\mathcal{C}=(u_1,\dots u_n)$ une famille de finie de vecteurs d'un $\mathbb{K}$-espace vectoriel E. Montrer que :

$$\text{pour tout } p\leq n, \text{ on a } \operatorname{rg}(u_1,\dots,u_p) \geq \operatorname{rg}\mathcal{C} + p - n.$$

► *Rang et produits de matrices.*
- Soient A et B deux matrices dans $\mathcal{M}_{3,3}(\mathbb{K})$ telles que $AB=O_3$. Montrer que l'une (au moins) de ces deux matrices est de rang inférieur ou égal à 1.
- Soient A dans $\mathcal{M}_{3,2}(\mathbb{K})$ et B dans $\mathcal{M}_{2,3}(\mathbb{K})$ deux matrices de rang 2 telles que $(AB)^2=AB$. Montre que $BA=I_2$.
- Soient A dans $\mathcal{M}_{3,2}(\mathbb{K})$ et B dans $\mathcal{M}_{2,3}(\mathbb{K})$ deux matrices telles que $AB=\left(\begin{smallmatrix}1&0&0\\0&1&0\\0&0&0\end{smallmatrix}\right)$. Calculer $\operatorname{rg} A$ et $\operatorname{rg} B$. Déduire de l'égalité $(AB)^2=AB$ le calcul de BA.

► *Rang de matrices présentées par blocs.*
- Soit $M\in\mathcal{M}_{n+p,n+p}(\mathbb{K})$ de la forme $M=\left(\begin{smallmatrix}A & O_{n,p}\\ O_{p,n} & D\end{smallmatrix}\right)$ avec $A\in\mathcal{M}_{n,n}(\mathbb{K})$ et $D\in\mathcal{M}_{p,p}(\mathbb{K})$. Montrer que $\operatorname{rg} M = \operatorname{rg} A + \operatorname{rg} D$.
- Soit $M\in\mathcal{M}_{n+p,n+p}(\mathbb{K})$ de la forme $M=\left(\begin{smallmatrix}I_n & B\\ O_{p,n} & D\end{smallmatrix}\right)$ avec $B\in\mathcal{M}_{n,p}(\mathbb{K})$ et $D\in\mathcal{M}_{p,p}(\mathbb{K})$. Montrer que $\operatorname{rg} M = n + \operatorname{rg} D$.
- Soit $M\in\mathcal{M}_{n+p,n+p}(\mathbb{K})$ de la forme $M=\left(\begin{smallmatrix}A & B\\ O_{p,n} & D\end{smallmatrix}\right)$ avec $A\in\mathcal{M}_{n,n}(\mathbb{K})$, $B\in\mathcal{M}_{n,p}(\mathbb{K})$ et $D\in\mathcal{M}_{p,p}(\mathbb{K})$. Montrer que $\operatorname{rg} M = p$ si et seulement si $A=O_n$.

Idéaux d'un anneau commutatif

Dans tout le texte, A désigne un anneau *commutatif unitaire*. On note $U(A)$ le groupe multiplicatifs des éléments inversibles de A, et A^* l'ensemble des éléments non-nuls de A.

1. Propriété algébriques générales sur les idéaux

1.1 - Notion d'idéal

Définition. On appelle *idéal* de A toute partie non-vide I de A qui vérifie les deux conditions suivantes :
(1) I est un sous-groupe du groupe additif A,
(2) pour tous $x \in I$ et $a \in A$, on a $xa \in I$.

Exemples.
(a) $\{0\}$ et A sont des idéaux de A.
(b) Pour tout $n \in \mathbb{Z}$, l'ensemble $n\mathbb{Z}$ des multiples de n est un idéal de l'anneau $\mathbb{Z}$.
(c) Dans l'anneau $\mathcal{F}(\mathbb{R}, \mathbb{R})$, l'ensemble des fonctions qui s'annulent en 0 est un idéal.
(d) Dans l'anneau $\mathbb{R}[X, Y]$, l'ensemble des polynômes s'annulant sur une partie non-vide Ω du plan $\mathbb{R}^2$ est un idéal de $\mathbb{R}[X, Y]$.

Lemme (très utile dans la pratique). Soit I un idéal de A.
(i) si I contient 1, alors $I = A$.
(ii) plus généralement, si I contient un élément de $U(A)$, alors $I = A$.

Preuve. Supposons $1 \in I$. Tout $a \in A$ s'écrit $a = 1.a$ donc, comme $1 \in I$, il résulte de la propriété (2) que $a \in I$. On a alors $A \subseteq I$, donc $A = I$, ce qui prouve (i). Supposons maintenant que I contienne un élément x inversible dans A. On a $1 = xx^{-1}$ avec $x \in I$ et $x^{-1} \in A$, donc $1 \in I$, et on applique (i) pour conclure que $I = A$. □

Proposition.
1. L'intersection de deux idéaux de A est un idéal de A. Plus généralement, l'intersection d'une famille quelconque d'idéaux de A est un idéal de A.
2. Soient B un anneau commutatif unitaire. Soit $f : A \to B$ un morphisme d'anneaux unitaires. On a :
   (i) Pour tout idéal J de B, l'image réciproque $f^{-1}(J)$ est un idéal de A.
   (ii) En particulier, $\operatorname{Ker} f = \{x \in A\,;\, f(x) = 0_B\}$ est un idéal de A.
   (iii) Pour tout idéal I de A, l'image directe $f(I)$ est un idéal de l'anneau $f(A) = \operatorname{Im} f$; (attention, ce n'est pas en général un idéal de B).

Preuve. Evidente, laissée au lecteur. □

La notion d'idéal permet de construire des anneaux quotients (voir plus loin). Donc, de même que la description des sous-groupes normaux d'un groupe donné est une question cruciale de la théorie des groupes, la question naturelle se pose de déterminer lorsque c'est possible les idéaux d'un anneau donné. Outre les procédés standards permettant de déduire de nouveaux idéaux à partir d'idéaux connus (proposition 1.1, opérations sur les idéaux vues plus loin en 1.3), le type d'idéal le plus simple, que l'on peut toujours considérer, est celui d'idéal principal.

1.2 - Notion d'idéal principal

Proposition et définitions. Pour $x \in A$, on note :

$$xA = \{xy\,;\, y \in A\} = \{z \in A\,;\, \text{il existe } y \in A \text{ tel que } z = xy\}.$$

Alors :

(i) xA est un idéal de A, appelé l'idéal principal engendré par x ;

(ii) xA est le plus petit idéal de A contenant x ;

(iii) on a : ($xA = A$) $\Leftrightarrow$ ($x \in U(A)$).

On appelle *idéal principal* de A tout idéal I de A pour lequel il existe un élément $x \in A$ tel que $I = xA$.

Preuve. Il est clair que xA est non-vide (il contient x puisque $x = x.1$). Soient $y \in xA$ et $z \in xA$ quelconques ; il existe $a, b \in A$ tels que $y = xa$ et $z = xb$, donc $y - z = x(a - b) \in xA$, ce qui prouve que xA est un sous-groupe additif. Soient $y \in xA$ et $c \in A$ quelconques ; il existe $a \in A$ tel que $y = xa$, donc $yc = xac = x(ac) \in xA$. On conclut que xA est un idéal de A.
Soit I un idéal de A contenant x. Comme $x \in I$, on a $xa \in I$ pour tout $a \in A$. Donc $xA \subseteq I$, ce qui prouve (ii). Si $xA = A$, alors $1 \in xA$, de sorte qu'il existe $y \in A$ tel que $xy = 1$, ce qui prouve $x \in U(A)$. L'implication réciproque découle du point (ii) du lemme de 1.1 □

Bien que très simple, le corollaire suivant est important, et montre que *la notion d'idéal n'a d'intérêt que pour des anneaux qui ne sont pas des corps.*

Corollaire. (A est un corps) $\Leftrightarrow$ (les seuls idéaux de A sont $\{0\}$ et A).

Preuve. Supposons que A est un corps. Soit I un idéal de A. Si $I \neq \{0\}$, il existe dans I un élément non-nul, donc inversible dans A puisque A est un corps. On conclut avec le lemme 1.1 que $I = A$. Supposons réciproquement que A n'admette que $\{0\}$ et A comme idéaux. Soit $x \in A$ quelconque non-nul. L'idéal xA étant alors distinct de $\{0\}$, on a nécessairement $xA = A$, d'où $x \in U(A)$ le point (iii) de la proposition ci-dessus. Ainsi tout élément non-nul de A est inversible dans A ; on conclut que A est un corps. □

Puisque dans tout anneau A on peut toujours considérer des idéaux de la forme xA pour $x \in A$, une question naturelle est d'étudier des anneaux où tous les idéaux sont de ce type. D'où la notion suivante.

Définitions. On appelle *anneau principal* tout anneau commutatif unitaire A *qui est intègre* et dans lequel tout idéal est principal.

► Exemples fondamentaux

(i) L'anneau $\mathbb{Z}$ des entiers relatifs est un anneau principal.

(ii) Si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[X]$ des polynômes en une indéterminée à coefficients dans $\mathbb{R}$ est un anneau principal.

(iii) L'anneau $\mathbb{Z}[i]$ des entiers de Gauss est un anneau principal.

Dans le cas de $\mathbb{Z}$, on sait que tout sous-groupe additif de $\mathbb{Z}$ est de la forme $a\mathbb{Z}$ avec $a \in \mathbb{Z}$, ce qui suffit à montrer le résultat. En fait, les trois exemples relèvent du même argument général que l'on montrera plus loin en 3.2, à savoir que tout anneau euclidien est un anneau principal.

► Contre-exemples fondamentaux

(i) Si B est un anneau qui n'est pas un corps, l'anneau $B[X]$ des polynômes en une indéterminée à coefficients dans B n'est pas principal.

(ii) Même si $\mathbb{K}$ est un corps, l'anneau $\mathbb{K}[X_1, \ldots, X_n]$ des polynômes en n indéterminée à coefficients dans $\mathbb{K}$ n'est pas principal lorsque $n \geq 2$.

(iii) L'anneau $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal.

On démontrera le point (i) un peu plus loin. A titre d'exemple, on vérifie ici de façon élémentaire que $\mathbb{Z}[X]$ n'est pas principal.

Exemple. On considère dans $A = \mathbb{Z}[X]$ le sous-ensemble $I = 2A + XA$ formé des polynômes qui s'écrivent $2P + XQ$ avec $P, Q \in A$. Il est facile de vérifier que I est un idéal de A (qui n'est autre que l'idéal engendré par 2 et X au sens où on va le voir au paragraphe suivant). Montrons que I n'est pas un idéal principal.

Par l'absurde, supposons qu'il existe $P \in A$ tel que $I = PA$. Comme $2 \in I$, il existerait $Q \in A$ tel que $2 = PQ$, ce qui impliquerait par un raisonnement sur les degrés que $P \in \mathbb{Z}$. Comme de plus $X \in I$, il existerait $R \in A$ tel que $X = PR$, ce qui impliquerait $P = \pm 1$ (et $R = \pm X$). On aurait donc $1 = \pm P \in I$, de sorte qu'il existerait $S, T \in A$ tels que $1 = 2S + TX$, ce qui est clairement impossible dans $A = \mathbb{Z}[X]$, puisque le coefficient constant de $2S + TX$ est pair. □

Concernant le point (ii), il est facile de vérifier de même que, dans l'anneau $A = \mathbb{K}[X, Y]$, l'idéal $I = XA + YA$ n'est pas un idéal principal. Le point (iii) sera démontré plus lon en 3.4.

1.3 - Opérations sur les idéaux

Proposition et définition (idéal engendré par une partie, somme d'idéaux).

(i) Si I et J sont des idéaux de A, alors l'ensemble $I + J = \{x + y\,;\, x \in I, y \in J\}$ est un idéal de A, appelé l'idéal somme de I et J ; c'est le plus petit idéal contenant I et J.

(ii) En particulier l'ensemble $xA + yA = \{xa + yb\,;\, a, b \in A\}$ est le plus petit idéal de A contenant x et y, quels que soient $x, y \in A$.

Preuve. Evidente ; laissée au lecteur. □

► Remarque. La motivation de la notion d'idéal somme résulte du fait que la réunion de deux idéaux n'est en général pas un idéal (par exemple si $A = \mathbb{Z}$, $I = 2\mathbb{Z}$ et $J = 3\mathbb{Z}$, $I \cup J$ n'est pas un idéal). L'idéal $I + J$ est alors l'idéal engendré par $I \cup J$, c'est-à-dire l'intersection de tous les idéaux contenant $I \cup J$, qui est aussi le plus petit idéal de A contenant $I \cup J$

Définition et proposition (produit d'idéaux). Si I et J sont des idéaux de A, on appelle produit des idéaux I et J, et on note IJ, l'ensemble des éléments de A qui sont somme d'un nombre fini de produits d'un élément de I par un élément de J.

($x \in IJ$) $\Leftrightarrow$ (il existe $n \in \mathbb{N}^*$, $y_1, \ldots, y_n \in I$, $z_1, \ldots, z_n \in J$, tels que $x = \sum_{i=1}^{n} y_i z_i$).

Alors :

IJ est un idéal de A ; c'est le plus petit idéal contenant l'ensemble $\{yz\,;\, y \in I, z \in J\}$, et il vérifie : $IJ \subset I \cap J$.

Preuve. Evidente ; laissée au lecteur. □

▶ Exercice. Montrer que, si I, J et K sont des idéaux de A, on a :

$$I + (J + K) = (I + J) + K, \qquad I(JK) = (IJ)K, \qquad I(J + K) = IJ + IK.$$

2. Applications aux anneaux quotients

2.1 - Quotient d'un anneau par un idéal

Soit I un idéal de A.

• L'idéal I est en particulier un sous-groupe du groupe additif A, et il est trivialement normal puisque A est abélien. On peut considérer le groupe additif quotient A/I. Rappelons que, si l'on note $\overline{a}$ la classe dans A/I d'un élément a de A, on a par définition :

$$\overline{a} = \{b \in A\,;\, a - b \in I\} := a + I,$$

et que l'addition dans A/I est définie par :

$$\overline{a} + \overline{b} = \overline{a + b} \quad \text{pour tous } a, b \in A. \qquad (\star)$$

En particulier le groupe additif A/I est abélien, d'élément neutre $\overline{0} = I$.

Rappel : le point crucial de cette construction du groupe quotient est de montrer que la définition ci-dessus de l'addition est indépendante des représentants choisis. Ceci signifie que, si $a' \in \overline{a}$ et $b' \in \overline{b}$, alors $\overline{a' + b'} = \overline{a + b}$; cela résulte du fait que $a' - a \in I$ et $b' - b \in I$, d'où $(a' + b') - (a + b) = (a' - a) + (b' - b) \in I$. Une fois que l'on a ainsi établi que l'addition est bien définie, vérifier qu'elle est associative, commutative, admet $\overline{0}$ pour élément neutre et que tout éléments $\overline{a}$ admet $\overline{-a}$ pour opposé est évident.

• La surjection canonique $p : A \to A/I$, qui à tout élément a de A associe sa classe $\overline{a}$ est alors un morphisme de groupes pour l'addition.

• On définit ensuite dans A/I une multiplication en posant :

$$\overline{a}.\overline{b} = \overline{ab} \quad \text{pour tous } a, b \in A. \qquad (\star\star)$$

1. Elle est bien définie, indépendamment des représentants choisis.

   En effet. Soient $a' \in \overline{a}$ et $b' \in \overline{b}$, ce qui signifie que : $a' - a \in I$ et $b' - b \in I$. On a : $a'b' - ab = a'(b' - b) + (a' - a)b$. Comme $a' - a \in I$ et que I est un idéal, on a $(a' - a)b \in I$. De même $a'(b' - b) \in I$ puisque $b' - b \in I$. On conclut que $a'b' - ab \in I$ comme somme de deux éléments de I, et donc $\overline{a'b'} = \overline{ab}$.

2. Elle est associative, commutative, distributive sur l'addition dans A/I, et admet $\overline{1}$ comme élément neutre.

   En effet. Quels que soient $a, b, c \in A$, on a $(\overline{a}.\overline{b}).\overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}.(\overline{b}.\overline{c})$, ce qui montre l'associativité. Le reste se montre de même. □

3. La surjection canonique p vérifie $p(1) = \overline{1}$ et $p(ab) = p(a).p(b)$ pour tous $a, b \in A$.

   En effet. Par définition de p d'une part, et de la multiplication dans A/I d'autre part, on a $p(ab) = \overline{ab} = \overline{a}.\overline{b} = p(a).p(b)$. □

On a ainsi démontré :

Proposition. Pour tout idéal I de A, l'ensemble quotient A/I muni de l'addition ($\star$) et de la multiplication ($\star\star$) est un anneau commutatif unitaire ; la surjection canonique $p : A \to A/I$ est un morphisme d'anneaux unitaires.

On a pour les anneaux quotients des résultats de même nature que ceux obtenus pour les groupes quotients, en particulier le théorème fondamental suivant :

Théorème (dit premier théorème d'isomorphisme). Soit B un anneau commutatif unitaire et $f : A \to B$ un morphisme d'anneaux unitaires. Alors l'anneau quotient de A par l'idéal $\operatorname{Ker} f$ est isomorphe au sous-anneau $\operatorname{Im} f = f(A)$ de B. On note :

$$A/\operatorname{Ker} f \simeq \operatorname{Im} f.$$

Preuve. On a vu à la proposition 1.1 que $\operatorname{Ker} f$ est un idéal de A. On peut donc considérer l'anneau quotient A/I. On introduit l'application :

$$\begin{array}{rccc} \varphi : & A/\operatorname{Ker} f & \longrightarrow & \operatorname{Im} f \\ & \overline{a} & \longmapsto & f(a) \end{array}.$$

✓ φ est bien définie : en effet, si $a, a' \in A$ vérifient $\overline{a} = \overline{a'}$, on a $a - a' \in \operatorname{Ker} f$, donc $f(a) - f(a') = f(a - a') = 0_B$, ce qui prouve que $\varphi(\overline{a'}) = \varphi(\overline{a})$.

✓ φ est un morphisme d'anneaux unitaires de $A/\operatorname{Ker} f$ dans B : en effet, $\varphi(\overline{1_A}) = f(1_A) = 1_B$ et, pour tous $a, b \in I$, $\varphi(\overline{a} + \overline{b}) = \varphi(\overline{a + b}) = f(a + b) = f(a) + f(b) = \varphi(\overline{a}) + \varphi(\overline{b})$, ainsi que $\varphi(\overline{a}\ \overline{b}) = \varphi(\overline{ab}) = f(ab) = f(a)f(b) = \varphi(\overline{a})\varphi(\overline{b})$.

✓ φ est une bijection de $A/\operatorname{Ker} f$ sur B : en effet, elle est surjective par construction et un élément $\overline{a}$ de $A/\operatorname{Ker} f$ appartient à $\operatorname{Ker} \varphi$ si et seulement si $f(a) = 0_B$, ce qui équivaut à $a \in \operatorname{Ker} f$, c'est-à-dire $\overline{a} = \overline{0} = 0_{A/I}$. □

▶ Exemple d'application.

Pour tout idéal I de A, on note $I[X]$ le sous-ensemble de $A[X]$ formé des polynômes à coefficients dans I, i.e. de la forme $\sum_{i=0}^{n} a_i X^i$, avec $n \geq 0$ et $a_0, a_1, \ldots, a_n \in I$.

Alors $I[X]$ est un idéal de $A[X]$, et l'anneau quotient $A[X]/I[X]$ est isomorphe à l'anneau $(A/I)[X]$ des polynômes à coefficients dans l'anneau A/I :

$$A[X]/I[X] \simeq (A/I)[X].$$

En effet. Le fait que $I[X]$ soit un idéal est une simple vérification. Considérons la surjection canonique $p : A \to A/I$ et définissons son extension canonique :

$$\begin{array}{rccc} f : & A[X] & \longrightarrow & (A/I)[X] \\ & P = \displaystyle\sum_{i=0}^{n} a_i X^i & \longmapsto & f(P) = \displaystyle\sum_{i=0}^{n} p(a_i) X^i \end{array}$$

Il est clair que f est un morphisme d'anneaux unitaires, qu'il est surjectif, et que son noyau est $\operatorname{Ker} f = I[X]$. L'isomorphisme $A[X]/\operatorname{Ker} f \simeq \operatorname{Im} f$ donne le résultat. □

Une fois obtenu par passage au quotient un nouvel anneau A/I, se pose la question naturelle de décrire ses idéaux, et en particulier de déterminer comment les idéaux de A/I sont liés aux idéaux de l'anneau de départ A. On a une réponse complète dans la proposition suivante.

Théorème (idéaux d'un anneau quotient ; troisième théorème d'isomorphisme).
Soit I un idéal de A.

(i) Tout idéal de A/I est de la forme J/I pour J un unique idéal de A contenant I, avec la notation naturelle $J/I = p(J) = \{\overline{x}\,;\, x \in A\}$.

(ii) On a alors l'isomorphisme d'anneaux unitaires $(A/I)/(J/I) \simeq A/J$.

Preuve. La preuve, classique et sans difficulté, est laissée au lecteur. □

▶ Exemple d'application : idéaux de $\mathbb{Z}/n\mathbb{Z}$.

Fixons un entier $n \geq 2$. Alors $n\mathbb{Z}$ est un idéal de $\mathbb{Z}$, et l'anneau quotient $\mathbb{Z}/n\mathbb{Z}$ n'est autre que l'anneau classique des classes de congruence modulo n.

Pour tout diviseur q de n, il existe un et un seul idéal de $\mathbb{Z}/n\mathbb{Z}$ d'ordre q, qui est $d\mathbb{Z}/n\mathbb{Z}$ où $n = dq$. Réciproquement tout idéal de $\mathbb{Z}/n\mathbb{Z}$ est de ce type.

Exemple : dans $\mathbb{Z}/12\mathbb{Z}$, les idéaux sont :
$\{\overline{0}\} = 12\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0},\overline{6}\} = 6\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0},\overline{4},\overline{8}\} = 4\mathbb{Z}/12\mathbb{Z}$,
$\{\overline{0},\overline{3},\overline{6},\overline{9}\} = 3\mathbb{Z}/12\mathbb{Z}$, $\{\overline{0},\overline{2},\overline{4},\overline{6},\overline{8},\overline{10}\} = 2\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/12\mathbb{Z}$.

▶ Exercice : On considère dans l'anneau $A = \mathbb{Z}[X]$ les idéaux principaux $I = 2A$ et $I' = XA$. On note $J = I + I' = 2A + XA$. Montrer de deux façons différentes que A/J est isomorphe à $\mathbb{F}_2$.

Solution 1. Le morphisme canonique $\phi : A \to \mathbb{F}_2[X]$ défini par $\phi(\sum_{i=0}^n a_i X^i) = \sum_{i=0}^n \overline{a}_i X^i$. est surjectif et de noyau I. D'après le premier théorème d'isomorphisme, $B = A/I$ est isomorphe à $\mathbb{F}_2[X]$. On a $I \subset J$, donc d'après le troisième théorème d'isomorphisme, A/J est isomorphe à $(A/I)/(J/I) = B/(J/I)$. Comme $B \simeq \mathbb{F}_2[X]$ et que $J/I = BX$, on déduit que $B/(J/I) \simeq \mathbb{F}_2$. On conclut que $A/J \simeq \mathbb{F}_2$.

Solution 2. Le morphisme d'évaluation $\psi : A \to \mathbb{Z}$ défini par $\psi(\sum_{i=0}^n a_i X^i) = a_0$ est surjectif et de noyau I'. D'après le premier théorème d'isomorphisme, $C = A/I'$ est isomorphe à $\mathbb{Z}$. On a $I' \subset J$, donc d'après le troisième théorème d'isomorphisme, A/J est isomorphe à $(A/I')/(J/I') = C/(J/I')$. Comme $C \simeq \mathbb{Z}$ et que $J/I' = 2C$, on déduit que $C/(J/I) \simeq \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$. On conclut que $A/J \simeq \mathbb{F}_2$.

Le théorème établit qu'il existe une bijection entre l'ensemble des idéaux de A contenant I et l'ensemble des idéaux de A/I.

2.2 - Idéal premier, idéal maximal

Définitions. Un idéal P de A est dit *premier* lorsque $P \neq A$ et vérifie :

quels que soient deux éléments a et b de A, si $ab \in P$, alors $a \in P$ ou $b \in P$.

Un idéal M de A est dit *maximal* lorsque $M \neq A$ et vérifie :

quel que soit I un idéal de A, si M est strictement inclus dans I, alors $I = A$.

▶ Remarques.

(1) Par définition, (l'idéal nul $\{0\}$ est premier) $\Leftrightarrow$ (l'anneau A est intègre).

(2) Si A n'est pas un corps, $\{0\}$ n'est pas maximal. Si A est un corps, l'idéal $\{0\}$ est l'unique idéal maximal de A.

(3) On peut démontrer que tout anneau commutatif unitaire admet nécessairement au moins un idéal maximal. Ce résultat non trivial (dont la preuve utilise le lemme de Zorn appliqué à l'ensemble partiellement ordonné des idéaux de A distincts de A) est connu sous le nom de théorème de Krull.

Les notions d'idéal premier et d'idéal maximal sont directement liées aux propriétés des anneaux quotients associés, comme le montre le théorème suivant :

Théorème (fondamental). Soit I un idéal de A. On a :

$$\begin{array}{ccc} I \text{ maximal} & \Longleftrightarrow & A/I \text{ corps} \\ \Downarrow & & \Downarrow \\ I \text{ premier} & \Longleftrightarrow & A/I \text{ intègre} \end{array}$$

Preuve. Supposons que M est un idéal maximal de A. Comme $M \neq A$, l'anneau A/M est non-nul. Considérons un idéal quelconque K de A/M. D'après la seconde proposition de 2.1, il existe un idéal J de A tel que $M \subseteq J$ et $K = J/M$. Mais, par maximalité de M, l'inclusion $M \subseteq J$ implique que $J = M$ ou $J = A$, c'est-à-dire $J/M = \{\overline{0}\}$ ou $J/M = A/M$. Ceci prouve que les seuls idéaux de A/M sont $\{\overline{0}\}$ et A/M. On conclut avec le corollaire de 1.2 que A/M est un corps. L'implication réciproque découle des mêmes calculs. L'équivalence de la première ligne est donc vérifiée.

Supposons que P est un idéal premier de A. Comme $P \neq A$, l'anneau A/P est non-nul. Considérons $\overline{a}, \overline{b} \in A/P$ tels que $\overline{a}\,\overline{b} = \overline{0}$. On a $\overline{ab} = \overline{0}$, c'est-à-dire $ab \in P$. Comme P est premier, on a $a \in P$ ou $b \in P$, c'est-à-dire $\overline{a} = \overline{0}$ ou $\overline{b} = \overline{0}$. On a ainsi montré que A/P est intègre. L'implication réciproque découle des mêmes calculs : l'équivalence de la seconde ligne est vérifiée. Il suffit de rappeler que tout corps est un anneau intègre pour achever la preuve. □

► Remarques (lien entre primalité et maximalité)

(a) D'après le théorème ci-dessus, tout idéal maximal est premier.

(b) Il existe des anneaux commutatifs unitaires A possédant des idéaux premiers non-nuls qui ne sont pas maximaux.

Exemple. Prenons $A = \mathbb{Z}[X]$ et $I = XA$ l'idéal principal engendré par X. Soit $f : A \to \mathbb{Z}$ l'application qui à tout polynôme $P = a_m X^m + \cdots + a_1 X + a_0$, avec les $a_i \in \mathbb{Z}$, associe le terme constant a_0. Il est facile de vérifier que f est un morphisme d'anneaux unitaires, qu'il est surjectif, et que son noyau est $I = XA$. D'après le théorème 2.1, on a alors $A/I \simeq \mathbb{Z}$. Comme $\mathbb{Z}$ est intègre sans être un corps, l'idéal I est premier sans être maximal. □

(c) Dans l'anneau $\mathbb{Z}$, considérons un idéal quelconque $I = k\mathbb{Z}$ avec $k \in \mathbb{N}$. Si $k = 1$, alors $I = \mathbb{Z}$ n'est ni premier, ni maximal. Si $k = 0$, alors $I = \{0\}$ est premier mais non maximal. Si maintenant $k \geq 2$, il résulte du théorème précédent que :

($k\mathbb{Z}$ est premier) $\Leftrightarrow$ (k est un nombre premier) $\Leftrightarrow$ ($k\mathbb{Z}$ est maximal)

Ainsi dans l'anneau $\mathbb{Z}$, les notions d'idéal maximal et d'idéal premier non-nul coïncident.

La propriété observée ci-dessus pour $\mathbb{Z}$ est en fait vraie pour tous les anneaux principaux, comme le montre la proposition suivante.

Proposition. Si l'anneau A est principal, tout idéal premier non-nul de A est maximal dans A (et donc, pour les idéaux non-nuls de A, les notions de premier et de maximal coïncident).

Preuve. Soient I un idéal premier non-nul de A et J un idéal de A tel que $I \subset J$. Comme A est un anneau principal, il existe donc $a, b \in A$ non-nuls tels que $I = aA$ et $J = bA$. Comme $a \in I$, on a $a \in J$ donc il existe $x \in A$ tel que $a = bx$. Supposons que $I \neq J$, c'est-à-dire que $b \notin I$. On a $a = bx \in I$ avec $b \notin I$, donc le fait que I soit premier implique que $x \in I$. Il existe alors $y \in A$ tel que $x = ay$. On déduit que $a = bx = bay$, ou encore $a(1 - by) = 0$. L'intégrité de A implique que $1 - by = 0$ puisque $a \neq 0$, d'où $by = 1$, ce qui prouve que $b \in U(A)$. D'après le lemme de 1.1, on conclut que $J = A$. Ainsi, pour tout idéal J de A tel que $I \subset J$ et $J \neq I$, on a $J = A$. On conclut que I est maximal. □

On a vu à la remarque (b) ci-dessus que l'anneau $\mathbb{Z}[X]$ possède des idéaux premiers non-nuls non maximaux, ce qui donne une nouvelle preuve du fait (déjà montré à la fin de 1.2) que $\mathbb{Z}[X]$ n'est pas principal.

La proposition suivante précise le second théorème de 2.1 en montrant que la correspondance bijective entre les idéaux de A contenant I et les idéaux de A/I préserve la primalité et la maximalité.

Proposition. Soit I un idéal de A distinct de A.
(i) Les idéaux premiers de A/I sont les idéaux de la forme P/I où P est un idéal premier de A contenant I.
(ii) Les idéaux maximaux de A/I sont les idéaux de la forme M/I où M est un idéal maximal de A contenant I

Preuve. Soit K un idéal de A/I. D'après le second théorème de 2.1, il existe un unique idéal J de A contenant I tel que $K = J/I$, et l'on a un isomorphisme d'anneaux $(A/I)/K \simeq A/J$. Dès lors, J est premier (resp. maximal) dans A si et seulement si A/J est intègre (resp. est un corps), c'est-à-dire si et seulement si $(A/I)/K$ est intègre (resp. est un corps), ce qui est équivaut à dire que K est un idéal premier (resp. maximal) de A/I. □

3. Applications à la divisibilité

3.1 - Interprétation de la divisibilité en termes d'idéaux

Définitions et proposition (multiples et diviseurs). Soient x et y deux éléments de A. On dit que x est un *diviseur* de y dans A, ou encore que x *divise* y dans A, ou encore que y est un *multiple* de x dans A, lorsque il existe $a \in A$ tel que $y = xa$. On note alors $x|y$, et l'on a :

$$(x|y) \Leftrightarrow (y \in xA) \Leftrightarrow (yA \subseteq xA).$$

Preuve. Supposons que $x|y$. Il existe $a \in A$ tel que $y = xa$. Donc $y \in xA$. De plus, tout élément de yA est de la forme yb avec $b \in A$, donc de la forme xab, et donc appartient à xA, ce qui montre que $yA \subseteq xA$. La réciproque est claire. □

▶ Conséquences. On en déduit immédiatement que :

(1) Pour tous $x, y, z \in A$, $\quad (x|y \text{ et } y|z) \Rightarrow (x|z)$.

(2) Pour tout $u \in A$, $(u \in U(A)) \Leftrightarrow (uA = A) \Leftrightarrow (u|y$ quel que soit $y \in A)$.

(3) Pour tous $x, u \in A$, $\quad (u \in U(A) \text{ et } x|u) \Rightarrow (x \in U(A))$.

Commentaire. La notion de multiple et de diviseur, et donc toute la théorie de la divisibilité que l'on va détailler dans la suite, n'a d'intérêt que dans un anneau *qui n'est pas un corps*. En effet, dans un corps K, deux éléments x et y non-nuls sont toujours à la fois multiple et diviseur l'un de l'autre puisque $x = zy$ avec $z = xy^{-1} \in K$ et $y = tx$ avec $t = yx^{-1} = z^{-1} \in K$.

Définition et proposition (éléments associés). On suppose ici que A est *intègre*. Soient x et y deux éléments de A. On dit que x et y sont *associés* lorsqu'on a à la fois $x|y$ et $y|x$. On note alors $x \sim y$, et l'on a :

$$(x \sim y) \Leftrightarrow (xA = yA) \Leftrightarrow (\text{il existe } u \in U(A) \text{ tel que } x = uy).$$

Preuve. La première équivalence découle directement de la proposition précédente. Pour la seconde, supposons que $x \sim y$. Il existe $u, v \in A$ tels que $x = uy$ et $y = vx$, donc $x = uvx$. Si $x = 0$, alors $y = 0$, et on a $x = uy$ pour tout $u \in U(A)$. Si $x \neq 0$, on écrit $x(1 - uv) = 0$ et on utilise l'intégrité de A pour déduire que $uv = 1$, d'où $u \in U(A)$, ce qui montre le résultat. Réciproquement, supposons $x = uy$ avec $u \in U(A)$; on a $y|x$ et, puisque $y = u^{-1}x$ avec $u^{-1} \in A$, on a aussi $x|y$. On conclut que $x \sim y$. □

▶ Exemples.

✓ Dans $\mathbb{Z}$, deux entiers m et n sont associés si et seulement si $m = \pm n$; rappelons en effet que l'on a $U(\mathbb{Z}) = \{1, -1\}$).

✓ Pour tout anneau intègre A, deux polynômes P et Q de $A[X]$ sont associés si et seulement s'il existe $c \in U(A)$ tel que $P = cQ$ et l'on a alors $Q = c^{-1}P$; en effet on a $U(A[X]) = U(A)$.

✓ En particulier, si $\mathbb{K}$ est un corps, deux polynômes P et Q de $\mathbb{K}[X]$ sont associés si et seulement s'il existe $c \in \mathbb{K}^*$ tel que $P = cQ$.

▶ Remarque. Il résulte imédiatement de ces définitions que *deux éléments associés dans A ont les mêmes multiples et les mêmes diviseurs dans l'anneau A.*

3.2 - Division euclidienne et idéaux principaux

Rappelons que l'on appelle *anneau euclidien* un anneau commutatif unitaire qui est intègre, et pour lequel il existe une application $\delta : A^* \to \mathbb{N}$ vérifiant les deux conditions suivantes :

1. pour tous $a, b \in A^*$, $(a|b \Rightarrow \delta(a) \leq \delta(b))$;

2. pour tout $a \in A$ et $b \in A^*$, il existe $q, r \in A$ tels que : $a = bq + r$ et ($r = 0$ ou $\delta(r) < \delta(b)$).

Une application δ vérifiant ces deux conditions s'appelle un *stathme* euclidien.

▶ Exemples.

(a) L'anneau $\mathbb{Z}$ est euclidien, pour le stathme défini par $\delta(x) = |x|$ pour tout $x \in \mathbb{Z}^*$.

(b) Si K est un corps, l'anneau $K[X]$ est euclidien, avec $\delta(F) = \deg F$ pour tout $F \in K[X]$ non-nul.

(c) L'anneau $\mathbb{Z}[i]$ est euclidien, avec $\delta(z) = z\,\overline{z}$ pour tout $z \in \mathbb{Z}[i]$ non-nul.

Proposition. Tout anneau euclidien est principal.

Preuve. Soit A un anneau euclidien, de stathme δ. Il est intègre, et il s'agit donc de montrer que tout idéal I de A est principal. C'est clair si $I = \{0\}$ (alors $I = 0A$) ou si $I = A$ (alors $I = 1A$). On suppose donc $I \neq \{0\}$ et $I \neq A$. On considère $E = \{\delta(x)\,;\, x \in I, x \neq 0\}$. C'est une partie non-vide de $\mathbb{N}$, elle admet donc un plus petit élément n. Il existe $x \in I$, $x \neq 0$ tel que $n = \delta(x)$. Soit alors $a \in I$ quelconque ; par division euclidienne de a par x, il existe $q, r \in A$ tels que $a = xq + r$ avec $r = 0$ ou $\delta(r) < \delta(x) = n$. On a : $r = a - xq$ avec $a \in I$ et $x \in I$, donc $r \in I$ par définition d'un idéal. Par minimalité de n, on ne peut donc pas avoir $\delta(r) < n$, et donc nécessairement $r = 0$, d'où $a = xq$. Ceci prouve que tout $a \in I$ appartient à xA, c'est-à-dire $I \subseteq xA$. Comme par ailleurs $xA \subseteq I$ puisque $x \in I$, on conclut que $I = xA$. □

▶ Remarques.

(a) La proposition démontre la caractère principal des anneaux $\mathbb{Z}$, $\mathbb{Z}[i]$, et $K[X]$ annoncé précédemment en 1.2.

(b) La réciproque de la proposition ci-dessus est fausse ; on peut par exemple démontrer que l'anneau $\mathbb{Z}[\omega] = \{a+\omega b\,;\, a, b \in \mathbb{Z}\}$ pour $\omega = \frac{1}{2}(1+i\sqrt{19})$ est principal mais non euclidien.

On a montré précédemment que l'anneau $\mathbb{Z}[X]$ n'est pas principal, donc en général : le fait que A soit euclidien n'implique pas que $A[X]$ est euclidien, et le fait que A soit principal n'implique pas que $A[X]$ est principal. On a en fait le résultat général suivant :

Théorème. Soit A un anneau commutatif unitaire. Les conditions suivantes sont équivalentes.

(i) A est un corps. (ii) $A[X]$ est euclidien ; (iii) $A[X]$ est principal.

Preuve. On a déja vu que (i) ⇒ (ii) ⇒ (iii). Supposons maintenant $A[X]$ principal. En particulier, $A[X]$ est intègre, et donc A est intègre. Considérons l'application $f : A[X] \to A$ qui, à tout polynôme $P = \sum_{i=0}^{n} a_i X^i$, associe le coefficient a_0. Il est facile de voir que f est un morphisme d'anneaux, qui est clairement surjectif. Donc le premier théorème d'isomorphisme 2.1 conduit à $A[X]/\operatorname{Ker} f \simeq A$. L'intégrité de A implique que $A[X]/\operatorname{Ker} f$ est intègre donc, d'après le théorème 2.2, $\operatorname{Ker} f$ est un idéal premier non-nul de $A[X]$. Mais comme $A[X]$ est supposé principal, $\operatorname{Ker} f$ est alors, d'après la première proposition de 2.2 un idéal maximal de $A[X]$, et donc, d'après le théorème 2.2, $A[X]/\operatorname{Ker} f$ est un corps. On conclut via l'isomorphisme $A[X]/\operatorname{Ker} f \simeq A$ que A est un corps. □

3.3 - Applications des idéaux à l'arithmétique dans les anneaux principaux

On suppose A intègre ; rappelons d'abord les deux définitions suivantes :

(1) Deux éléments a et b de A sont *premiers entre eux* lorsque les seuls éléments de A qui divisent à la fois a et b sont les éléments de $U(A)$.

(2) Deux éléments a et b de A admettent un *plus grand commun diviseur* dans A lorsqu'il existe un élément $d \in A$ tel que d divise a, d divise b, et tout élément qui divise à la fois a et b divise aussi d. On dit alors que d est un pgcd de a et b.

On a immédiatement les propriétés :

(i) Si deux éléments a et b de A admettent un pgcd d, alors les autres pgcd de a et b sont les éléments $d' \in A$ associés à d. De plus, les deux éléments a' et b' tels que $a = da'$ et $b = db'$ sont premiers entre eux dans A.

(ii) Deux éléments a et b de A sont premiers entre eux si et seulement si $U(A)$ est l'ensemble des pgcd de a et b, ou encore si et seulement si 1 est un pgcd de a et b.

Dans les situations classiques de l'arithmétique dans $\mathbb{Z}$ ou $\mathbb{K}[X]$, deux éléments quelconques ont toujours des pgcd. Les résultats pratiques importants qui leur sont liés (théorèmes de Bézout, de Gauss,...) sont en fait vrais dans tout anneau principal, comme on va le voir.

Théorème (interprétation du pgcd en termes d'idéaux). On suppose A principal. Deux éléments quelconques de A admettent des pgcd dans A. Plus précisément, quels que soient a et b dans A, tout générateur de l'idéal $aA + bA$ est un pgcd de a et b.

$$(\ d \text{ est un pgcd de } a \text{ et } b\ ) \Leftrightarrow (\ aA + bA = dA\ )$$

Preuve. Soient $a, b \in A$ fixés. Comme A est principal, l'idéal $aA + bA$ est principal. Il existe $d \in A$ tel que $aA + bA = dA$. Montrons que d est un pgcd de a et b. On a d'abord $aA \subseteq aA + bA$, donc $aA \subseteq dA$, donc $d|a$. De même, $d|b$. Soit maintenant $c \in A$ tel que $c|a$ et $c|b$. Alors $aA \subseteq cA$ et $bA \subseteq cA$, donc, puisque cA est stable par addition, $aA + bA \subseteq cA$, c'est-à-dire $dA \subseteq cA$, et donc $c|d$. Ceci prouve que d est un pgcd de a et b. Réciproquement, soit d' un pgcd de a et b. Comme on l'a rappelé ci-dessus, on a $d' \sim d$, donc $dA = d'A$, c'est-à-dire $d'A = aA + bA$. □

Théorème de Bézout. On suppose A principal. Pour tous a et b dans A, on a :

$$(\ a \text{ et } b \text{ premiers entre eux dans } A\ ) \Leftrightarrow (\ \text{il existe } u, v \in A \text{ tels que } au + bv = 1\ )$$

Preuve. Soient $a, b \in A$ fixés. Supposons a et b premiers entre eux, donc 1 est un pgcd de a et b, et donc $aA + bA = A$. En particulier $1 \in aA + bA$, et donc il existe $(u, v) \in A^2$ tel que $au + bv = 1$. Supposons réciproquement qu'il existe $u, v \in A$ tels que $au + bv = 1$; alors 1 appartient à $aA + bA$, donc $aA + bA = A$. Or, si d est un pgcd de a et b, on a $dA = aA + bA$. On déduit que $dA = A$, donc $d \in U(A)$, c'est-à-dire a et b premiers entre eux. □

Lemme de Gauss. On suppose A principal. Pour tous a, b, c dans A, on a :

$$(\ a \text{ divise } bc, \text{ et } a \text{ premier avec } b\ ) \Rightarrow (\ a \text{ divise } c\ )$$

Preuve. Comme a et b sont premiers entre eux, il existe d'après le théorème de Bézout $u, v \in A$ tels que $au + bv = 1$. Donc $c = cau + cbv$. Comme a divise bc, on a $bc \in aA$, donc $bcv \in aA$. Par ailleurs il est clair que $acu \in aA$. Par stabilité de l'idéal aA pour l'addition, on conclut que $c = acu + bcv \in aA$. □

Corollaire (une précision sur le théorème de Bézout). On suppose A principal. Soient a et b premiers entre eux dans A. Pour tout couple $(u, v) \in A^2$ tel que $au + bv = 1$, l'ensemble de tous les couples $(x, y) \in A^2$ tels que $ax + by = 1$ est égal à

$$\{(u, v) + c(-b, a)\,;\, c \in A\}.$$

Preuve. Soit $(u, v) \in A^2$ tel que $au + bv = 1$. Pour tout $c \in A$, le couple $(x, y) = (u, v) + c(-b, a) = (u - cb, v + ca)$ vérifie $ax + by = a(u - cb) + b(v + ca) = au - acb + bv + bca = au + bv = 1$. Réciproquement, quel que soit $(x, y) \in A^2$ tel que $ax + by = 1$, on a $ax + by = au + bv$, d'où $a(u - x) = b(y - v)$. Comme a et b sont premiers entre eux, il résulte du lemme de Gauss que a divise $y - v$. Il existe donc $c \in A$ tel que $y - v = ca$. On a alors : $cab = b(y - v) = a(u - x)$. Si

$a \neq 0$, on déduit par intégrité de A que $u - x = cb$; on obtient donc bien $x = u - cb$ et $y = v + ca$.
Si $a = 0$, alors $b \in U(A)$ et la propriété est claire. □

▶ Complément. Si A est principal, on a de même une notion de ppcm :

(a) On appelle ppcm de deux éléments $a, b \in A$ tout élément $m \in A$ tel que $aA \cap bA = mA$.

(b) (m est un ppcm de a et b) $\Leftrightarrow$ ($a|m$, $b|m$, et tout multiple de a et b est multiple de m).

(c) Le produit de tout pgcd de a et b par tout ppcm de a et b est associé à ab.

(d) En particulier (a et b sont premiers entre eux) $\Leftrightarrow$ (ab est un ppcm de a et b).

Comme la notion de pgcd, la notion de ppcm est définie à l'association près, et s'étend naturellement à un nombre fini quelconque d'éléments de A.

3.4 - Eléments irréductibles et idéaux maximaux

Définition. On suppose que A est intègre. Un élément x de A est dit *irréductible* dans A lorsqu'il n'est pas inversible dans A, et vérifie la condition :

$$\text{si } x = ab \text{ avec } a, b \in A, \text{ alors } a \in U(A) \text{ ou } b \in U(A).$$

▶ Remarques.

1. 0 n'est pas irréductible dans A.
2. Dans la définition (a), le "ou" est exclusif. En d'autres termes, si x est irréductible dans A et s'écrit $x = ab$, alors un seul des deux éléments a, b appartient à $U(A)$ (car si les deux étaient dans $U(A)$, alors x appartiendrait aussi à $U(A)$, ce qui est contraire à la définition).
3. Un élément de A peut être irréductible dans A mais ne plus l'être dans un anneau contenant A. Par exemple, 3 est irréductible dans $\mathbb{Z}$ mais pas dans $\mathbb{Q}$ puisqu'il est inversible dans $\mathbb{Q}$.
4. Tout élément associé à un élément irréductible dans A est encore irréductible dans A.

Proposition (caractérisation en termes d'idéaux principaux). On suppose A intègre.

(i) Un élément $x \in A$ est irréductible dans A si et seulement si l'idéal xA est maximal parmi les idéaux principaux distincts de A.

(ii) On suppose de plus que A est un anneau principal. Un élément $x \in A$ est irréductible dans A si et seulement si l'idéal xA est un idéal maximal de A.

Preuve. Supposons x irréducible. L'idéal principal $M = xA$ est distinct de A puisque $x \notin U(A)$. Soit $J = aA$ un idéal principal de A distinct de A, c'est-à-dire tel que $a \notin U(A)$, et supposons que $M \subseteq J$. Alors en particulier $x \in J$, donc il existe $b \in A$ tel que $x = ab$. Puisque $a \notin U(A)$, l'irréductibilité de x implique que $b \in U(A)$. Donc $x \sim a$, d'où $M = J$. Ceci prouve que M est maximal parmi les idéaux principaux distincts de A. Réciproquement soit $x \in A$ tel que xA soit maximal parmi les idéaux principaux distincts de A. Soient $a, b \in A$ tels que $x = ab$. Alors $x \in aA$, et donc $xA \subseteq aA$. Si $a \in U(A)$, alors $aA = A$. Sinon, $aA \neq A$ et la maximalité de xA implique alors que $xA = aA$, donc $x \sim a$, d'où l'existence de $u \in U(A)$ tel que $x = ua$. Mais $x = ua = ba$ implique par intégrité de A que $b = u$, et donc $b \in U(A)$.
Ceci prouve (i). Le point (ii) est alors évident par définition d'un anneau principal. □

► Exemples.

(a) Dans $\mathbb{Z}$, les éléments irréductibles sont les nombres premiers et leurs opposés.

(b) Pour tout corps K, les polynômes de degré un sont toujours irréductibles dans $K[X]$.

(c) Si $K = \mathbb{C}$, les éléments irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré un.

(d) Si $K = \mathbb{R}$, les éléments irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré un, et les polynômes de degré deux de discriminant strictement négatif.

(e) Montrer que le polynôme $X^4 + 7$ est irréductible dans $\mathbb{F}_5[X]$.

(f) C'est un exercice classique d'arithmétique (lié au théorème dit "des deux carrés") que de montrer que, dans l'anneau $\mathbb{Z}[i]$ des entiers de Gauss, les éléments irréductibles sont d'une part les éléments $x + iy$ avec $x, y \in \mathbb{Z}$ tels que $x^2 + y^2$ soit un nombre premier, et d'autre part les nombres premiers congrus à 3 modulo 4.

• Complément 1 : un argument pour montrer qu'un anneau n'est pas principal.

Définition et proposition (éléments premiers.) On suppose que A est intègre. Un élément x de A est dit *premier* dans A lorsqu'il est non-nul et non inversible dans A, et vérifie la condition :

si x divise ab avec $a, b \in A$, alors x divise a ou x divise b.

On a alors les propriétés suivantes :

(i) Un élément $x \in A$ est premier dans A si et seulement si l'idéal xA est un idéal premier non-nul de A.

(ii) Tout élément premier dans A est irréductible dans A.

(iii) Si de plus l'anneau A est principal, alors tout élément irréductible est premier, et donc les notions d'élément premier et d'élément irréductible coïncident dans ce cas.

Preuve. Le point (i) est clair par définition d'un idéal premier.
Pour (ii), soit $x \in A$ premier dans A. On a $x \notin U(A)$. Supposons que $x = ab$ avec $a, b \in A$. En particulier $x|ab$, donc puisque x est premier, $x|a$ ou $x|b$. Supposons que $x|a$. Il existe $y \in A$ tel que $a = xy$, d'où $x = xyb$, ou encore $x(1 - yb) = 0$. Comme x est non-nul car premier, on conclut par intégrité que $yb = 1$, donc $b \in U(A)$. On prouve de même que $a \in U(A)$ si $x|b$.
Pour (iii), soit x un élément irréductible de A. Il est non-inversible et non-nul, et l'idéal $M = xA$ est maximal parmi les idéaux principaux de A distincts de A. Mais ici, tout idéal de A est par hypothèse principal. Donc M est tout simplement un idéal maximal de A. Donc M est un idéal premier de A (voir 2.2), et comme il est non-nul, on déduit du point (i) que x est un élément premier dans A. □

► La réciproque du point (ii) peut être fausse si A n'est pas principal. Ceci donne une méthode pour établir qu'un anneau intègre donné n'est pas principal : il suffit de trouver des éléments irréductibles qui ne sont pas premiers. C'est le cas de l'exemple suivant :

Contre-exemple. Considérons l'anneau $A = \mathbb{Z}[i\sqrt{5}]$. Il est intègre comme sous-anneau de $\mathbb{C}$.
Montrons d'abord que 3 n'est pas premier dans A. Observons d'abord que 3 ne divise pas $2 + i\sqrt{5}$ dans A (en effet, on aurait sinon $(2 + i\sqrt{5}) = 3(a + ib\sqrt{5})$ avec $a, b \in \mathbb{Z}$, d'où $3a = 2$ et $1 = 3b$, ce qui

est impossible), et que de même 3 ne divise pas $2-i\sqrt{5}$. Et pourtant 3 divise $9=(2+i\sqrt{5})(2-i\sqrt{5})$ dans A, puisque $9=3.3$. On conclut que 3 n'est pas premier dans A.

Montrons maintenant que 3 est irréductible dans A. Il est clair que 3 n'est pas inversible dans A. Supposons que $3=xy$ avec $x=a+ib\sqrt{5}$ et $y=c+id\sqrt{5}$, où $a,b,c,d\in\mathbb{Z}$. Posons $N(x)=|x|^2=a^2+5b^2$ et $N(y)=|y|^2=c^2+5d^2$. On a : $9=N(xy)=N(x)N(y)$ dans $\mathbb{N}^*$, et donc trois cas seulement sont possibles : $N(x)=N(y)=3$, ou $N(x)=1$ et $N(y)=9$, ou $N(x)=9$ et $N(y)=1$. Or le premier cas est impossible (car $a^2+5b^2=3$ n'a pas de solutions entières), le second implique que $x\in U(A)$ (car $a^2+5b^2=1$ implique $a=\pm1$ et $b=0$, et donc $x=\pm1$), et le troisième implique de même que $y\in U(A)$. On conclut que 3 est irréductible dans A. □

• Complément 2 : un argument vers la factorialité des anneaux principaux.

L'importance que joue dans l'arithmétique de $\mathbb{Z}$ la décomposition de tout entier non-nul et non inversible en produit de nombres premiers (au signe près), et le fait que la notion de nombre premier s'étend à tout anneau principal en la notion d'éléments irréductible, conduit à la question naturelle de l'existence et de l'unicité d'une décomposition de tout élément non-nul et non inversible d'un anneau principal en un produit déléments irréductibles.

Sans donner ici de preuve complète (on les trouve partout), indiquons seulement quelques jalons pour bien poser le problème. Un anneau intègre A est dit factoriel lorsqu'il vérifie les deux conditions suivantes :

(F1) tout élément non-nul et non inversible de A peut s'écrire comme un produit d'élément irréductibles dans A,

(F2) cette décomposition est unique à l'ordre près des facteurs et à l'association près.

On peut montrer que, lorsque l'on a (F1), la condition (F2) est équivalente à la condition :

(F'2) tout élément irréductible dans A est premier dans A.

Comme on a vu ci-dessus que la condition (F'2) est vérifiée pour les anneaux principaux, il suffit de montrer que tout anneau principal vérifie la condition (F1) pour conclure que :

tout anneau principal est factoriel.

Pour établir la condition (F1) dans un anneau principal, la difficulté est de démontrer que tout élément non nul et non inversible possède un diviseur irréductible, et qu'il n'en possède qu'un nombre fini. Ces deux arguments vont reposer sur les deux lemmes suivants, qui ont tous les deux leur intérêt propre.

Lemme. Si A est un anneau principal, tout élément de A non-nul et non inversible est divisible dans A par un élément irréductible dans A.

Preuve. Soit $x\in A$, $x\notin U(A)$, $x\neq 0$. L'idéal xA est un idéal propre de A. D'après le théorème de Krull, il est contenu dans un idéal maximal M. Parce que A est principal, il existe un élément $z\in A$ tel que $M=xA$. En particulier l'inclusion $xA\subset zA$ signifie que z divise x. Le fait que M est maximal et non-nul (car il contient x qui est non-nul) implique que x est irréductible dans A. □

Lemme. Si A est un anneau principal, toute suite croissante d'idéaux de A est stationnaire.

Preuve. Soit $(I_n)_{n\in\mathbb{N}}$ une suite croissante d'idéaux de A. Il en résulte que la réunion I des idéaux I_n est dans ce cas un idéal (vérification évidente). Parce que A est principal, il existe pour tout $n \in \mathbb{N}$ un élément a_n de A tel que $I_n = a_n A$, et il existe $b \in A$ tel que $I = bA$. En particulier $b \in I$, et donc il existe un idéal I_m tel que $b \in I_m$. Pour tout $n \geq m$, on a $I_m \subseteq I_n$, donc $b \in I_n$, ce qui implique que $bA \subseteq I_n$. Comme par ailleurs $bA \supseteq I_n$ par définition de b, on conclut que $I_n = bA$ dès lors que $n \geq m$, ce qui montre le résultat voulu. □

On laisse au lecteur le soin de compléter la preuve du fait que tout anneau principal est factoriel :
- en démontrant que les deux lemmes ci-dessus permettent détablir qu'un anneau principal vérifie la condition (F1),
- et en établissant qu'alors la condition (F2) est bien équivalente à la condition (F'2) que l'on sait être vraie lorsque A est principal.

4. D'autres exemples d'applications

4.1 - Caractéristique d'un anneau

NOTATION. On travaille toujours dans un anneau commutatif unitaire A. Pour tout $x \in A$, on note $2x = x + x$, $3x = x + x + x$ et de même $nx = x + x + \cdots + x$ (avec n termes) pour tout entier $n \geq 2$. On pose naturellement $1x = x$ et $0x = 0$, ce qui définit la notation nx pour tout $n \in \mathbb{N}$. Si l'on considère maintenant un entier $m \leq 0$, on convient que $mx = n(-x) = -(nx)$ où $n = -m \in \mathbb{N}$. On a ainsi défini la notation nx pour tout $x \in A$ et tout $n \in \mathbb{Z}$. On a :

$$\text{pour tout } n \in \mathbb{Z},\ (\ n1_A = 0_A\ ) \Leftrightarrow (\ nx = 0_A\ \text{ pour tout } x \in A\ ).$$

Lemme et définition. Il existe un unique morphisme d'anneaux unitaires $f : \mathbb{Z} \to A$. Il est défini par $f(n) = n1_A$ pour tout $n \in \mathbb{Z}$. On l'appelle le morphisme canonique de $\mathbb{Z}$ dans A.

Preuve. Si f est un morphisme d'anneaux unitaires $\mathbb{Z} \to A$, on doit avoir $f(1) = 1_A$, d'où par additivité $f(2) = f(1) + f(1) = 1_A + 1_A = 2\,1_A$, et par récurrence $f(n) = n1_A$ pour tout entier $n \geq 1$. Comme f est un morphisme de groupes additifs, on a aussi $f(0) = 0_A$ et $f(m) = f(-n) = -f(n) = -(n1_A) = (-n)1_A = m1_A$ pour tout entier $m \leq 0$ et en posant $n = -m$. En résumé, on a $f(n) = n1_A$ pour tout $n \in \mathbb{Z}$. Réciproquement, il est clair que f ainsi défini est bien un morphisme d'anneaux unitaires. □

Définition. On appelle *caractéristique* de A, notée $\operatorname{car} A$, l'unique entier $k \in \mathbb{N}$ tel que $\operatorname{Ker} f = k\mathbb{Z}$, où f est le morphisme canonique de $\mathbb{Z}$ dans A.

Cette définition est justifiée par le fait que, comme $f : \mathbb{Z} \to A$ est un morphisme d'anneaux unitaires, $\operatorname{Ker} f$ est un idéal de $\mathbb{Z}$; et puisque $\mathbb{Z}$ est principal, il est de la forme $c\mathbb{Z}$ pour un unique entier $c \in \mathbb{N}$.
En d'autres termes :

$$\operatorname{car} A = 0 \ \Leftrightarrow\ \Big[\ \text{pour tout } n \in \mathbb{Z},\ (n1_A = 0_A\ ) \Leftrightarrow (n = 0)\ \Big]$$

$$\operatorname{car} A = c > 0 \ \Leftrightarrow\ \Big[\ \text{pour tout } n \in \mathbb{Z},\ (n1_A = 0_A\ \ ) \Leftrightarrow (n \in c\mathbb{Z})\ \Big]$$

Exemples.

(a) L'anneau $\mathbb{Z}$ est de caractéristique nulle, ainsi que les corps $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

(b) Pour tout $n \geq 2$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ est de caractéristique n. En particulier, pour tout nombre premier p, le corps $\mathbb{Z}/p\mathbb{Z}$ est de caractéristique p.

(c) Pour tout sous-anneau unitaire B de A, on a $\operatorname{car} A = \operatorname{car} B$.

Proposition. Si A intègre, la caractéristique de A est soit 0, soit un nombre premier.

Preuve. Soit c la caractéritique de A. D'après le théorème 2.1, $= \mathbb{Z}/c\mathbb{Z} = \mathbb{Z}/\operatorname{Ker} f \simeq \operatorname{Im} f$. Comme A est intègre, il est en de même du sous-anneau $\operatorname{Im} f$, et donc de l'anneau $\mathbb{Z}/c\mathbb{Z}$. D'après 2.2, l'intégrité de $\mathbb{Z}/c\mathbb{Z}$ équivaut au fait que $c\mathbb{Z}$ est un idéal premier de $\mathbb{Z}$, donc c est nul ou un nombre premier. □

4.2 - Polynôme minimal et lemme des noyaux

On renvoie sur ce point aux sections 2.1 et 2.2 du document sur les polynômes d'endomorphismes (pages précédentes 29 et 30).

4.3 - Radical et idéaux primaires

Proposition et définition. Soit I un idéal d'un anneau commutatif unitaire A. Alors l'ensemble :

$$\sqrt{I} = \{x \in A\,;\ \text{il existe } n \in \mathbb{N}^*,\ x^n \in I\}.$$

est un idéal de A, contenant I.

Preuve. Sans difficulté ; laissée au lecteur. □.

► Les propriétés suivantes sont classiques et sans difficulté (où I et J sont deux idéaux) :

$$I \subseteq J \Rightarrow \sqrt{I} \subseteq \sqrt{J}, \qquad \sqrt{(\sqrt{I})} = \sqrt{I}, \qquad \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.$$

Définition. Soit I un idéal d'un anneau commutatif unitaire A. On dit que I est *primaire* lorsque $I \neq A$ et vérifie :

quels que soient deux éléments a et b de A, si $ab \in I$ et $a \notin I$, alors $b \in \sqrt{I}$.

Proposition. Soit I un idéal d'un anneau commutatif unitaire A.

(i) Si I est premier, alors il est primaire.

(ii) Si I est primaire, alors $\sqrt{I}$ est premier.

(iii) Si $\sqrt{I}$ est maximal, alors I est primaire.

Preuve. Le point (i) est évident par définition puisque $I \subseteq \sqrt{I}$.
Pour montrer (ii), supposons que I est primaire. Observons d'abord que $\sqrt{I} \neq A$ (en effet, on aurait sinon $1 \in \sqrt{I}$, donc $1^n \in I$ pour un certain $n \in \mathbb{N}^*$, donc $1 \in I$, d'où $I = A$, ce qui est exclu puisque I est primaire). Considérons ensuite deux éléments $a, b \in A$ tels que $ab \in \sqrt{I}$. Il existe un entier $n \geq 1$ tel que $a^n b^n = (ab)^n \in I$. Ou bien $a^n \in I$, et donc $a \in \sqrt{I}$. Ou bien $a^n \notin I$,

mais alors $b^n \in \sqrt{I}$ puisque I est primaire, donc il existe un entier $m \geq 1$ tel que $(b^n)^m \in I$, c'est-à-dire $b^{nm} \in I$ et finalement $b \in \sqrt{I}$.
Pour montrer (iii), supposons que $\sqrt{I}$ est maximal. Soient a, b deux élements de A tels que $ab \in I$ et $b \notin \sqrt{I}$. Il s'agit de montrer qu'alors $a \in I$. L'idéal $J = \sqrt{I} + bA$ contient strictement $\sqrt{I}$ donc par maximalité $J = A$. Il existe donc $c \in \sqrt{I}$ et $d \in A$ tels que $1 = c + bd$. On a alors $abd = a - ac$, d'où $a - ac \in I$ puisque $ab \in I$, puis $ac - ac^2 \in I$ en multipliant par c. Alors $a - ac^2 = a - ac + ac - ac^2 \in I$. De même $a - ac^3 = a - ac^2 + (a - ac)c^2 \in I$, et par récurrence $a - ac^q \in I$ pour tout $q \in \mathbb{N}$. Puisque $c \in \sqrt{I}$, il existe $q \in \mathbb{N}$ tel que $c^q \in I$, d'où $a \in I$. □

► Exemple de référence.

> Les idéaux primaires de $\mathbb{Z}$ sont les idéaux $p^n\mathbb{Z}$, où p est un nombre premier et où n est un entier naturel non-nul.

Preuve. Soit I un idéal primaire de $\mathbb{Z}$. Comme $\mathbb{Z}$ est principal, il existe deux entiers $p, q \in \mathbb{Z}$, que l'on peut supposer positifs, tels que $I = q\mathbb{Z}$ et $\sqrt{I} = p\mathbb{Z}$. Puisque $p \in \sqrt{I}$, il existe un entier $m \in \mathbb{N}^*$ tel que $p^m \in q\mathbb{Z}$, donc q divise p^m. Or d'après le point (ii) de la proposition précédente, l'idéal $p\mathbb{Z}$ est premier, donc d'après les résultats vus en 2.2, p est un nombre premier. Dès lors le fait que q divise p^m implique qu'il existe $n \in \mathbb{N}$ tel que $q = p^n$. On a $n \neq 0$ car $I \neq A$ par hypothèse. Ainsi $I = p^n\mathbb{Z}$ avec $n \in \mathbb{N}^*$. La preuve de la réciproque est sans difficulté et laissée au lecteur. □

L'anneau $\mathbf{Z/nZ}$

1. Construction et structure de $\mathbb{Z}/n\mathbb{Z}$

1.1 - L'ensemble $\mathbb{Z}/n\mathbb{Z}$

▶ *Relation de congruence*

Définition. Soit n un entier naturel. Deux entiers x et y sont dits congrus modulo n lorsque $x - y$ est divisible par n dans $\mathbb{Z}$. On note alors $x \equiv y\,[n]$

Remarque. Tout entier x est congru modulo n au reste de la division euclidienne de x par n. Deux entiers x et y sont congrus modulo n si et seulement s'ils ont le même reste dans la division euclidienne par n.

Proposition. Pour tout entier naturel n, la relation de congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$.

Notation. Soit n un entier naturel fixé. Pour tout $x \in \mathbb{Z}$, on note $\overline{x}$ la classe d'équivalence de x pour la relation de congruence modulo n.

$$\overline{x} = \{y \in \mathbb{Z}\,;\, x \equiv y\,[n]\} = \{x + kn\,;\, k \in \mathbb{Z}\}.$$

Rappelons que tout élément d'une classe $\overline{x}$ s'appelle un représentant de la classe $\overline{x}$. Dire qu'un entier y est un représentant de la classe $\overline{x}$ signifie que $x \equiv y\,[n]$, ou encore que $\overline{x} = \overline{y}$.

▶ *Ensemble quotient pour la relation de congruence*

Notation. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble quotient de $\mathbb{Z}$ par la relation de congruence modulo n, c'est-à-dire l'ensemble des classes de congruences de tous les entiers.

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{x}\,;\, x \in \mathbb{Z}\}.$$

Cas particulier 1. Si $n = 0$, la relation de congruence modulo 0 est l'égalité dans $\mathbb{Z}$. Dans ce cas, on a $\overline{x} = \{x\}$ pour tout $x \in \mathbb{Z}$, et $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$.

Cas particulier 2. Si $n = 1$, la relation de congruence modulo 1 est la relation triviale dans $\mathbb{Z}$, c'est-à-dire $x \equiv y\,[1]$ quels que soient les entiers x et y. Dans ce cas, on a $\overline{x} = \mathbb{Z}$ pour tout $x \in \mathbb{Z}$, et $\mathbb{Z}/1\mathbb{Z} = \{\overline{0}\}$.

Dans la suite on ne considérera plus que le cas où $n \geq 2$

Théorème. Pour tout $n \geq 2$, l'ensemble $\mathbb{Z}/n\mathbb{Z}$ est fini, de cardinal n, et l'on a :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}.$$

Le reste de la division euclidienne de x par n est l'unique représentant de $\overline{x}$ qui appartient à $[\![0, n-1]\!]$.

1.2 - Structure d'anneau de $\mathbb{Z}/n\mathbb{Z}$

▶ *Compatibilité de la congruence avec les opérations de $\mathbb{Z}$*

Proposition. Pour tout entier naturel n, la relation de congruence modulo n est compatible avec l'addition et avec la multiplication dans $\mathbb{Z}$, ce qui signifie que, quels que soient des entiers x, x', y, y' :

$$\textit{si}\quad x \equiv x'\,[n]\quad \textit{et}\quad y \equiv y'\,[n],\quad \textit{alors}\quad x+y \equiv x'+y'\,[n]\quad \textit{et}\quad xy \equiv x'y'\,[n].$$

▶ *Lois quotients*

Lemme. Les lois de composition internes + et × construites sur $\mathbb{Z}/n\mathbb{Z}$ en posant :

$$\text{pour tout } (\overline{x},\overline{y}) \in (\mathbb{Z}/n\mathbb{Z})^2,\quad \overline{x}+\overline{y} = \overline{x+y} \quad \text{et} \quad \overline{x}\times\overline{y} = \overline{x\times y},$$

sont bien définies, indépendamment des représentants choisis

Preuve : Fixons $\overline{x}$ et $\overline{y}$ deux éléments quelconques de $\mathbb{Z}/n\mathbb{Z}$. On pose $\overline{x}+\overline{y} = \overline{x+y}$. Prenons un autre représentant x' de la classe $\overline{x}$, et un autre représentant y' de la classe $\overline{y}$. Cela signife que $\overline{x} = \overline{x}'$ et $\overline{y} = \overline{y}'$, ou encore $x \equiv x'\,[n]$ et $y \equiv y'\,[n]$. D'après la proposition ci-dessus, on a alors $x+y \equiv x'+y'\,[n]$, donc $\overline{x'+y'} = \overline{x+y}$, c'est-à-dire $\overline{x}+\overline{y} = \overline{x}'+\overline{y}'$. Ceci prouve le résultat pour l'addition. On raisonne de même pour la multiplication. □

Remarque. Le lemme signifie que la surjection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, qui à tout $x \in \mathbb{Z}$ associe $\pi(x) = \overline{x}$, vérifie :

$$\text{pour tout } (x,y) \in \mathbb{Z}^2,\quad \pi(x+y) = \pi(x)+\pi(y) \quad \text{et} \quad \pi(x\times y) = \pi(x)\times\pi(y). \qquad (\star)$$

Théorème. L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni des deux lois de composition internes définies au lemme précédent est un anneau commutatif unitaire. L'élément neutre pour l'addition est $\overline{0}$ et l'élément neutre pour la multiplication est $\overline{1}$. La surjection canonique $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ est un morphisme d'anneaux unitaires.

Remarque sur la preuve. On peut vérifier par des calculs élémentaires tous les axiomes de la structure d'anneau pour $\mathbb{Z}/n\mathbb{Z}$ simplement en appliquant π à l'axiome correspondant dans l'anneau $\mathbb{Z}$ et en utilisant la propriété $(\star)$; c'est le principe de transport de structure.

On peut définir plus généralement par le même principe l'anneau quotient A/I de tout anneau commutatif A par tout idéal I de A. C'est cette construction qui s'applique ici à l'anneau $\mathbb{Z}$ et à l'idéal $n\mathbb{Z}$ de $\mathbb{Z}$ formé par les multiples de n.

Remarque. Il en résulte que l'on peut calculer dans $\mathbb{Z}/n\mathbb{Z}$ avec les règles de calcul usuelles dans un anneau commutatif, mais avec quelques particularités :

(i) un produit peut être nul sans qu'aucun des facteurs ne le soit (par exemple $\overline{2}\times\overline{3} = \overline{0}$ dans $\mathbb{Z}/6\mathbb{Z}$ bien que $\overline{2} \neq \overline{0}$ et $\overline{3} \neq \overline{0}$) ;

(ii) une équation linéaire de degré 1 dans $\mathbb{Z}/n\mathbb{Z}$ peut avoir plusieurs solutions (par exemple, dans $\mathbb{Z}/16\mathbb{Z}$, l'équation $\overline{4}x = \overline{0}$ a quatre solutions $\overline{0}$, $\overline{4}$, $\overline{8}$, $\overline{12}$).

1.3 - Eléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ et structure de corps de $\mathbb{Z}/p\mathbb{Z}$

► *Caractérisation des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

Théorème. Pour tout entier x, l'élément $\overline{x}$ est inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si les entiers x et n sont premiers entre eux.

Preuve : $\overline{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement s'il existe un élément $\overline{y}$ de $\mathbb{Z}/n\mathbb{Z}$ tel que $\overline{xy} = \overline{1}$, ce qui équivaut à l'existence d'un entier y tel que $xy \equiv 1\,[n]$, ou encore à l'existence d'un entier y et d'un entier k tel que $xy - kn = 1$. D'après le théorème de Bézout, cette dernière condition est satisfaite si et seulement si x et n sont premiers entre eux. □

Corollaire. Les conditions suivantes sont équivalentes :

(i) l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps ;

(ii) l'anneau $\mathbb{Z}/n\mathbb{Z}$ est intègre ;

(iii) l'entier n est un nombre premier.

Preuve : (i) implique (ii) puisque tout corps est un anneau intègre. Pour montrer que (ii) implique (iii), raisonnons par contraposée en supposant que n n'est pas premier. Il existe alors deux entiers non-nuls p et q distincts de 1 et de -1 tels que $n = pq$. On a donc $\overline{pq} = \overline{n} = \overline{0}$. Et pourtant $\overline{p} \neq \overline{0}$ (car sinon, il existerait un entier k tel que $p = kn$, d'où $n = knq$, ce qui contredirait $q \neq \pm 1$), et de même $\overline{q} \neq \overline{0}$. On a ainsi vérifié que n non premier implique $\mathbb{Z}$ non intègre, ce qui prouve que (ii) implique (iii). Montrons enfin que (iii) implique (i). Supposons n premier. Il en résulte que tout entier appartenant à $[\![1, n-1]\!]$ est premier avec n. En appliquant le théorème précédent, on déduit que les éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont $\overline{1}, \overline{2}, \ldots, \overline{n-1}$. En d'autres termes tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ sauf $\overline{0}$ sont inversibles, donc $\mathbb{Z}/n\mathbb{Z}$ est un corps. □

► *Groupe des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.*

D'une façon générale, pour tout anneau commutatif unitaire A, l'ensemble des éléments inversibles de l'anneau A est un groupe pour la multiplication, que l'on note $U(A)$, et que l'on appelle le groupe des unités de A.

Le théorème ci-dessus montre que l'ordre du groupe $U(\mathbb{Z}/n\mathbb{Z})$ est exactement le nombre d'entiers compris entre 1 et $n-1$ et premiers avec n ; ce nombre $\varphi(n)$ sera étudié plus loin.

Remarquons que :

— $U(\mathbb{Z}/10\mathbb{Z}) = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$ est d'ordre 4 ; de plus $\overline{3}^2 = \overline{9}$ et $\overline{3}^3 = \overline{7}$, ce qui montre que le groupe $U(\mathbb{Z}/10\mathbb{Z})$ est cyclique.

— $U(\mathbb{Z}/12\mathbb{Z}) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$ est aussi d'ordre 4 ; de plus $\overline{5}^2 = \overline{7}^2 = \overline{11}^2 = \overline{1}$, ce qui montre que le groupe $U(\mathbb{Z}/12\mathbb{Z})$ n'est pas cyclique, mais isomorphe au groupe de Klein.

— Lorsque p est premier, on a d'après le corollaire ci-dessus $U(\mathbb{Z}/p\mathbb{Z}) = \{\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{p-1}\}$. On peut démontrer que c'est un groupe cyclique.

2. Quelques compléments algébriques classiques.

2.1 - Générateurs du groupe cyclique additif $\mathbb{Z}/n\mathbb{Z}$

▶ *Cyclicité du groupe additif $\mathbb{Z}/n\mathbb{Z}$.*

Proposition. Le groupe additif $\mathbb{Z}/n\mathbb{Z}$ est cyclique.

Preuve : Considérons $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$ muni de sa structure de groupe pour l'addition. On a : $\overline{2} = \overline{1}+\overline{1}$, $\overline{3} = \overline{1}+\overline{1}+\overline{1}$, et d'une façon générale $\overline{x} = \overline{1}+\cdots+\overline{1}$ (somme de x termes) pour tout $x \in [\![1, n]\!]$, jusqu'à $\overline{n} = \overline{0}$. Ceci prouve que $\mathbb{Z}/n\mathbb{Z}$ est engendré, en tant que groupe additif, par le seul élément $\overline{1}$. C'est donc un groupe monogène, et comme il est fini, il est cyclique. □

▶ *Caractérisation des générateurs du groupe cyclique additif $\mathbb{Z}/n\mathbb{Z}$.*

Exemple introductif. Considérons $\mathbb{Z}/6\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$.

- En tant que groupe additif, on a vu que $\mathbb{Z}/6\mathbb{Z}$ est engendré par $\overline{1}$.
- Mais il est aussi engendré par $\overline{5}$ car :

$$\overline{5}+\overline{5} = \overline{4}, \qquad \overline{5}+\overline{5}+\overline{5} = \overline{3}, \qquad \overline{5}+\overline{5}+\overline{5}+\overline{5} = \overline{2},$$
$$\overline{5}+\overline{5}+\overline{5}+\overline{5}+\overline{5} = \overline{1}, \qquad \overline{5}+\overline{5}+\overline{5}+\overline{5}+\overline{5}+\overline{5} = \overline{0}.$$

- En revanche, il n'est pas engendré par $\overline{3}$ car $\overline{3}+\overline{3} = \overline{0}$, et donc une somme de termes tous égaux à $\overline{3}$ ne donnera toujours que $\overline{3}$ ou $\overline{0}$, et non tous les éléments de $Z/6\mathbb{Z}$.

La question qui se dégage est donc, pour un n donné, de déterminer, parmi tous les éléments de $\mathbb{Z}/n\mathbb{Z}$, ceux qui l'engendrent en tant que groupe additif. La proposition suivante y répond.

Proposition. Pour tout entier x, l'élément $\overline{x}$ engendre le groupe additif $\mathbb{Z}/n\mathbb{Z}$ si et seulement si les entiers x et n sont premiers entre eux.

Preuve : Si $\overline{x}$ engendre $\mathbb{Z}/n\mathbb{Z}$, il existe un entier m vérifiant $1 \leq m \leq n-1$ tel que l'élément $\overline{1}$ soit la somme de m termes $\overline{1} = \overline{x}+\cdots+\overline{x}$. Ceci implique que l'on a dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ l'égalité $\overline{mx} = \overline{1}$. D'où $\overline{x}$ inversible, et le résultat voulu d'après le théorème 1.3.
Réciproquement, supposons x et m premiers entre eux. D'après le théorème 1.3, il existe un entier m vérifiant $1 \leq m \leq n-1$ tel que $\overline{1} = \overline{mx} = \overline{x}+\cdots+\overline{x}$. Mais comme $\overline{1}$ engendre $\mathbb{Z}/n\mathbb{Z}$, tout élément de $\mathbb{Z}/n\mathbb{Z}$ s'exprime comme une somme de termes tous égaux à $\overline{1}$, et donc comme une somme de termes tous égaux à $\overline{x}$. On conclut que $\overline{x}$ engendre $\mathbb{Z}/n\mathbb{Z}$. □

▶ *Isomorphisme de tout groupe cyclique avec le groupe additif $\mathbb{Z}/n\mathbb{Z}$.*

Proposition. Tout groupe cyclique est isomorphe à un groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Plus explicitement, si $G = \{e, a, a^2, \ldots, a^{n-1}\}$ est un groupe cyclique d'ordre n (noté multiplicativement), alors l'application $f : G \to \mathbb{Z}/n\mathbb{Z}$ qui, à tout élément a^x (avec $0 \leq x \leq n-1$), associe $\overline{x}$, est un isomorphisme de groupes de $(G, .)$ sur $(\mathbb{Z}/n\mathbb{Z}, +)$.

D'après la proposition précédente, un élément a^x de G est un générateur de G si et seulement si x et n sont premiers entre eux.

2.2 - Théorème chinois

On fixe deux entiers $a \geq 1$ et $b \geq 1$. On considère les anneaux $\mathbb{Z}/a\mathbb{Z}$ et $\mathbb{Z}/b\mathbb{Z}$; pour tout entier x, on note $\overline{x}$ sa classe modulo a et $\widetilde{x}$ sa classe modulo b. On considère l'anneau produit $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$. Ses éléments sont les couples $(\overline{x},\widetilde{y})$, avec $x, y \in \mathbb{Z}$. Il est fini, formé de ab éléments. On considère l'anneau $\mathbb{Z}/ab\mathbb{Z}$. Il est fini, formé de ab éléments. On note $\widehat{x}$ la classe modulo ab d'un entier x.

Théorème. *Avec les données et notations ci-dessus, on considère l'application :*

$$\begin{array}{rccc} f: & \mathbb{Z}/ab\mathbb{Z} & \to & \mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z} \\ & \widehat{x} & \mapsto & (\overline{x},\widetilde{x}). \end{array}$$

Alors

(i) *L'application f est bien définie, et est un morphisme d'anneaux.*

(ii) *Si les entiers a et b sont premiers entre eux, alors f est un isomorphisme.*

Preuve. Pour montrer (i), considérons deux entiers x et y vérifient $\widehat{x} = \widehat{y}$. Alors $x - y$ est un multiple de ab. Donc d'une part $\overline{x} = \overline{y}$ car $x - y$ est multiple de a, et $\widetilde{x} = \widetilde{y}$ car $x - y$ est un multiple de b. D'où $f(\widehat{x}) = f(\widehat{y})$. Ceci prouve que f est bien définie. Le fait que f soit un morphisme d'anneaux se vérifie de façon évidente. Pour (ii), considérons un élément $\widehat{x}$ du noyau de f. On a $f(\widehat{x}) = (\overline{0},\widetilde{0})$, donc $\overline{x} = \overline{0}$ et $\widetilde{x} = \widetilde{0}$, c'est-à-dire $x \in a\mathbb{Z} \cap b\mathbb{Z}$. Donc $x \in \mu\mathbb{Z}$ en notant μ le ppcm de a et b. Or, puisque a et b sont ici supposés premiers entre eux, on a $\mu = ab$. Donc $x \in ab\mathbb{Z}$, ou encore $\widehat{x} = \widehat{0}$. Ceci prouve que f est injective. Il en résulte que f est bijective car les ensembles de départ et d'arrivée sont finis de même cardinal ab. □

Corollaire. *Les conditions suivantes sont équivalentes :*

(i) *les entiers a et b sont premiers entre eux ;*

(ii) *les anneaux $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$ et $\mathbb{Z}/ab\mathbb{Z}$ sont isomorphes ;*

(iii) *les groupes additifs $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$ et $\mathbb{Z}/ab\mathbb{Z}$ sont isomorphes ;*

(iv) *le groupe additif $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$ est cyclique.*

Preuve. On a montré au théorème précédent que (i)⇒(ii). Les implications (ii)⇒(iii) et (iii)⇒(iv) sont évidentes. Pour montrer (iv)⇒(i), raisonnons par contraposée en supposant que a et b ne sont pas premiers entre eux. Le ppcm μ de a et b est donc strictement inférieur au produit ab. Soit $(\overline{x},\widetilde{y})$ un élément quelconque de $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$. Comme a divise μ, on a $\mu x \in a\mathbb{Z}$, d'où $\overline{\mu x} = \overline{0}$. Donc $\mu\overline{x} = \overline{x}+\overline{x}+\cdots\overline{x} = \overline{0}$. De même $\mu\widetilde{y} = \widetilde{0}$. Ainsi tout élément $(\overline{x},\widetilde{y})$ de $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$ vérifie $\mu(\overline{x},\widetilde{y}) = (\overline{0},\widetilde{0})$ avec $\mu < ab$. En d'autres termes, tout élément de $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$ est d'ordre strictement inférieur à ab. Et donc le groupe additif $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}$ n'est pas cyclique. Ce qui achève la preuve. □

Exemples.

	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{0},\overline{1})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{0},\overline{0})$

$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ n'est pas cyclique ; c'est le groupe de Klein $V = \{e, a, b, c\}$ pour :
$e = (\overline{0},\overline{0})$, $a = (\overline{0},\overline{1})$, $b = (\overline{1},\overline{0})$ et $c = (\overline{1},\overline{1})$.

	$(\overline{0},\widetilde{0})$	$(\overline{1},\widetilde{1})$	$(\overline{0},\widetilde{2})$	$(\overline{1},\widetilde{0})$	$(\overline{0},\widetilde{1})$	$(\overline{1},\widetilde{2})$
$(\overline{0},\widetilde{0})$	$(\overline{0},\widetilde{0})$	$(\overline{1},\widetilde{1})$	$(\overline{0},\widetilde{2})$	$(\overline{1},\widetilde{0})$	$(\overline{0},\widetilde{1})$	$(\overline{1},\widetilde{2})$
$(\overline{1},\widetilde{1})$	$(\overline{1},\widetilde{1})$	$(\overline{0},\widetilde{2})$	$(\overline{1},\widetilde{0})$	$(\overline{0},\widetilde{1})$	$(\overline{1},\widetilde{2})$	$(\overline{0},\widetilde{0})$
$(\overline{0},\widetilde{2})$	$(\overline{0},\widetilde{2})$	$(\overline{1},\widetilde{0})$	$(\overline{0},\widetilde{1})$	$(\overline{1},\widetilde{2})$	$(\overline{0},\widetilde{0})$	$(\overline{1},\widetilde{1})$
$(\overline{1},\widetilde{0})$	$(\overline{1},\widetilde{0})$	$(\overline{0},\widetilde{1})$	$(\overline{1},\widetilde{2})$	$(\overline{0},\widetilde{0})$	$(\overline{1},\widetilde{1})$	$(\overline{0},\widetilde{2})$
$(\overline{0},\widetilde{1})$	$(\overline{0},\widetilde{1})$	$(\overline{1},\widetilde{2})$	$(\overline{0},\widetilde{0})$	$(\overline{1},\widetilde{1})$	$(\overline{0},\widetilde{2})$	$(\overline{1},\widetilde{0})$
$(\overline{1},\widetilde{2})$	$(\overline{1},\widetilde{2})$	$(\overline{0},\widetilde{0})$	$(\overline{1},\widetilde{1})$	$(\overline{0},\widetilde{2})$	$(\overline{1},\widetilde{0})$	$(\overline{0},\widetilde{1})$

$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ est cyclique, engendré par $x = (\overline{1},\widetilde{1})$.

3. Quelques compléments arithmétiques classiques.

3.1 - Indicatrice d'Euler

Définition. Pour tout entier $n \geq 2$, on note $\varphi(n)$ le nombre d'entiers compris entre 1 et $n-1$ qui sont premiers avec n :

$$\varphi(n) = \text{Card}\{k \in [\![1, n-1]\!] \ ; \ \text{pgcd}(k,n) = 1\}.$$

En convenant de plus de poser $\varphi(1) = 1$, on définit ainsi une application $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ appelée *fonction indicatrice d'Euler.*

Remarque. $\varphi(n)$ est à la fois le nombre de générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$, et le nombre d'éléments du groupe multiplicatif $U(\mathbb{Z}/n\mathbb{Z})$ des inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Proposition. La fonction φ est une fonction arithmétique multiplicative, ce qui signifie que, pour tout couple $(a,b) \in \mathbb{N}^* \times \mathbb{N}^*$ tel que a et b soient premiers entre eux, on a : $\varphi(ab) = \varphi(a)\varphi(b)$.

Preuve : Fixons deux entiers $a, b \geq 1$ premiers entre eux. D'après le théorème chinois, l'anneau $\mathbb{Z}/ab\mathbb{Z}$ est isomorphe à l'anneau produit $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. En particulier, $\varphi(ab)$ est égal au nombre d'éléments de $U(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z})$. Or on vérifie aisément qu'un élément $(\overline{x}, \widetilde{y})$ de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est inversible si et seulement si $\overline{x}$ est inversible dans $\mathbb{Z}/a\mathbb{Z}$ et $\widetilde{y}$ est inversible dans $\mathbb{Z}/b\mathbb{Z}$. Il en résulte que $U(\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}) = U(\mathbb{Z}/a\mathbb{Z}) \times U(\mathbb{Z}/b\mathbb{Z})$ est formé de $\varphi(a)\varphi(b)$ éléments. D'où l'égalité. □

Pour donner une formule explicite permettant de calculer $\varphi(n)$, on procède en plusieurs étapes :

Lemme. Si p est un nombre premier et si α est un entier strictement positif, alors :

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

Preuve : Soit p un nombre premier. On a $\varphi(p) = p-1$ car tout entier de $[\![1, p-1]\!]$ est premier avec p. Fixons maintenant un entier $\alpha \geq 2$. Il y a $p^\alpha - 1$ entiers compris (au sens large) entre 1 et $p^\alpha - 1$. Parmi eux, ceux qui ne sont pas premiers avec p^α sont exactement ceux qui sont divisibles par p (car p est premier), c'est-à-dire ceux qui sont de la forme mp avec $m \in \mathbb{N}^*$ tel que $mp < p^\alpha$. Il y en a autant que de valeurs de m telles que $1 \leq m < p^{\alpha-1}$, à savoir $p^{\alpha-1} - 1$. On conclut que $\varphi(p^\alpha) = (p^\alpha - 1) - (p^{\alpha-1} - 1) = p^\alpha - p^{\alpha-1}$. □

Théorème. Pour tout entier $n \geq 2$, on a : $\varphi(n) = n \prod_{\substack{p \in \mathcal{P} \\ p|n}} (1 - \frac{1}{p})$.

Preuve : Considérons la décomposition de n en produit de facteurs premiers : $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ avec $p_1, p_2, \ldots, p_s$ premiers deux à deux distincts, et les $\alpha_i \geq 1$. D'après la proposition, on a : $\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_s^{\alpha_s})$. En appliquant le lemme, il vient :

$$\varphi(n) = p_1^{\alpha_1}(1 - \tfrac{1}{p_1}) p_2^{\alpha_2}(1 - \tfrac{1}{p_2}) \cdots p_s^{\alpha_s}(1 - \tfrac{1}{p_s}),$$

d'où le résultat. □

3.2 - Théorème d'Euler

Théorème. Soient a et n deux entiers ≥ 2. Si a et n sont premiers entre eux, alors :

$$a^{\varphi(n)} \equiv 1\,[n].$$

Preuve. Comme a est premier avec n, on sait que $\overline{a} \in U(\mathbb{Z}/n\mathbb{Z})$. On peut donc considérer l'application $t : U(\mathbb{Z}/n\mathbb{Z}) \to U(\mathbb{Z}/n\mathbb{Z})$ définie par $t(\overline{x}) = \overline{ax}$ pour tout $\overline{x} \in U(\mathbb{Z}/n\mathbb{Z})$. Parce que $\overline{a}$ est inversible dans $U(\mathbb{Z}/n\mathbb{Z})$, l'application t est clairement une bijection. Donc :

$$\prod_{\overline{x}\in U(\mathbb{Z}/n\mathbb{Z})} \overline{x} \;=\; \prod_{\overline{x}\in U(\mathbb{Z}/n\mathbb{Z})} \overline{ax} \;=\; \overline{a}^{\,|U(\mathbb{Z}/n\mathbb{Z})|} \times \prod_{\overline{x}\in U(\mathbb{Z}/n\mathbb{Z})} \overline{x},$$

où $|U(\mathbb{Z}/n\mathbb{Z})|$ désigne le nombre d'éléments du groupe $U(\mathbb{Z}/n\mathbb{Z})$, qui n'est autre que $\varphi(n)$. D'où $\overline{a}^{\varphi(n)} = \overline{1}$, ce qui achève la preuve. □

Corollaire. Soit p un nombre premier. Alors :

(i) pour tout $a \in \mathbb{Z}$ tel que $a \notin p\mathbb{Z}$, on a : $a^{p-1} \equiv 1\,[p]$,

(ii) pour tout $a \in \mathbb{Z}$, on a : $a^p \equiv a\,[p]$.

Preuve : Le point (i) est la traduction immédiate du théorème précédent puisque $\varphi(p) = p - 1$ lorsque p est premier. Le point (ii) s'obtient en multipliant les deux membres de (i) par a. □

Remarque. Le point (ii) est appelé le petit théorème de Fermat.

Remarque. Réciproquement (i) implique que p est premier, mais il existe des entiers non premiers qui vérifient (ii) (c'est la notion de nombre pseudo-premier, ou nombres de Carmichael, comme 561, 1105, 1729, 2465, 2821...).

3.3 - Théorème de Wilson

Théorème. Un entier $p \geq 2$ est premier si et seulement si $(p-1)! \equiv -1\,[p]$.

Preuve : Supposons p premier. Donc $\mathbb{Z}/p\mathbb{Z}$ est un corps, que l'on notera $\mathbb{F}_p$. Tous les éléments de $\mathbb{F}_p$ distincts de $\overline{0}$ sont inversibles. Il est clair que $\overline{1}$ a pour inverse lui-même, ainsi que $-\overline{1} = \overline{p-1}$. Réciproquement, soit $\overline{x}$ un élément non-nul de $\mathbb{F}_p$ tel que $\overline{x} = \overline{x}^{-1}$. On a alors $\overline{x}^2 = \overline{1}$, donc $(\overline{x} - \overline{1})(\overline{x} + \overline{1}) = \overline{0}$, ce qui, parce que $\mathbb{F}_p$ est ici un corps donc un anneau intègre, implique $\overline{x} = \pm\overline{1}$. En résumé, $\overline{1}$ et $-\overline{1} = \overline{p-1}$ sont les seuls éléments de $\mathbb{F}_p$ égaux à leur propre inverse. On calcule :

$$\overline{(p-1)!} = \overline{1} \times \underbrace{\overline{2} \times \cdots \times \overline{p-2}}_{\overline{1}} \times \overline{(p-1)} = \overline{1} \times \overline{(p-1)} = -\overline{1},$$

en remarquant que le produit des facteurs situés au centre vaut $\overline{1}$ puisque les facteurs qui y figurent sont deux à deux inverses l'un de l'autre. On conclut que $(p-1)! \equiv -1\,[p]$.

Réciproquement, supposons $(p-1)! \equiv -1\,[p]$. Pour tout $x \in [\![1, p-1]\!]$, on peut écrire $\overline{(p-1)!} = \overline{x} \times \overline{y}$, où $\overline{y}$ désigne le produit de tous les éléments non-nuls de $\mathbb{Z}/p\mathbb{Z}$ distincts de $\overline{x}$. Or, par hypothèse, $\overline{(p-1)!} = -\overline{1}$. Donc $\overline{x} \times \overline{y} = -\overline{1}$, d'où $\overline{x}$ inversible dans $\mathbb{Z}/p\mathbb{Z}$, d'inverse $-\overline{y}$. Ceci étant vrai pour tout élément $\overline{x}$ non-nul de $\mathbb{Z}/p\mathbb{Z}$, on conclut que $\mathbb{Z}/p\mathbb{Z}$ est un corps, et donc p est premier. □

4. Quelques exercices d'application.

4.1 - Identité d'Euler

Montrer que la fonction indicatrice d'Euler vérifie l'égalité : $\sum_{d|n} \varphi(d) = n$.

4.2 - Cyclicité du groupe $(\mathbb{Z}/p\mathbb{Z})^\star$

Soit p un nombre premier. Montrer que le groupe multiplicatif $U(\mathbb{Z}/p\mathbb{Z}) = \mathbb{F}_p^\star$ est cyclique.

> Indications : Notons G le groupe multiplicatif $U(\mathbb{Z}/p\mathbb{Z})$. Puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps, que l'on note $\mathbb{F}_p$, on a $G = \mathbb{F}_p^\star$. Pour tout diviseur d de $p-1$, notons Γ_d l'ensemble des éléments de G d'ordre d et E_d l'ensemble des éléments $\overline{x}$ de G tels que $\overline{x}^d = \overline{1}$. Montrer que E_d est un sous-groupe de G d'ordre $\leq d$ et contenant Γ_d. et que $\operatorname{card}\Gamma_d = \varphi(d)$. En utilisant le théorème de Lagrange et l'identité d'Euler, en déduire que $\Gamma \neq \emptyset$ pour tout diviseur d de $p-1$. Conclure.

4.3 - Exemple de nombre de Carmichael

Montrer que l'entier $p = 561$ n'est pas premier mais vérifie $n^p \equiv n\,[p]$ pour tout $n \in \mathbb{Z}$.

> Indications : Fixons $n \in \mathbb{Z}$ quelconque et posons $N = n(n^{560}-1) = n((n^2)^{280}-1)$. Vérifier qu'il existe $k_1 \in \mathbb{N}$ tel que $N = n(n^2-1)k_1$. En justifiant que 3 divise $n^3 - n$, conclure que 3 divise N. Etablir de de même que 11 et 17 divisent N et conclure.

4.4 - Systèmes de congruence

Soient α et β deux entiers quelconques. Soient a et b deux entiers naturels non-nuls premiers entre eux. Montrer que le système de congruences :

$$(\Sigma)\ \begin{cases} x \equiv \alpha\,[a] \\ x \equiv \beta\,[b] \end{cases}$$

admet des solutions dans $\mathbb{Z}$. Montrer ensuite que l'ensemble des solutions dans $\mathbb{Z}$ de (Σ) est :

$$S = \{au\beta + bv\alpha + \lambda ab\,;\, \lambda \in \mathbb{Z}\},$$

où (u, v) désigne un couple d'entiers tels que $au + bv = 1$.

4.5 - Codage monographique en cryptographie

On note : $\mathcal{A} = \{A, B, C, \ldots, Y, Z\}$ l'alphabet, et $\mathcal{E} = \{0, 1, 2, \ldots, 24, 25\}$ l'ensemble des 26 premiers entiers naturels. Soit g la bijection naturelle de $\mathcal{A}$ sur $\mathcal{E}$ consistant à numéroter :

$$g(A) = 0,\ g(B) = 1,\ g(C) = 2,\ g(D) = 3,\ \ldots\ldots,\ g(Y) = 24,\ g(Z) = 25.$$

Coder un message littéral consiste alors à introduire une bijection f de $\mathcal{E}$ sur $\mathcal{E}$ et à appliquer :

$$\begin{array}{ccccccc} \mathcal{A} & \xrightarrow{g} & \mathcal{E} & \xrightarrow{f} & \mathcal{E} & \xrightarrow{g^{-1}} & \mathcal{A} \\ \alpha & \longmapsto & g(\alpha) & \longmapsto & f(g(\alpha)) & \longmapsto & g^{-1}(f(g(\alpha))) \end{array},$$

et le décodage consiste alors en l'application :

$$\begin{array}{ccccccc} \mathcal{A} & \xrightarrow{g} & \mathcal{E} & \xrightarrow{f^{-1}} & \mathcal{E} & \xrightarrow{g^{-1}} & \mathcal{A} \\ \beta & \longmapsto & g(\beta) & \longmapsto & f^{-1}(g(\beta)) & \longmapsto & g^{-1}(f^{-1}(g(\beta))) \end{array}.$$

Démontrer que, pour $(a, b) \in \mathcal{E} \times \mathcal{E}$ fixé tel que a est premier avec 26, l'application $f_{a,b}$ qui, à tout entier $n \in \mathcal{E}$, associe l'unique entier $f_{a,b}(n)$ dans $\mathcal{E}$ vérifiant :

$$f_{a,b}(n) \equiv an + b\ [26]$$

est une bijection de $\mathcal{E}$ sur $\mathcal{E}$.

Racines des polynômes en une indéterminée

1. Préliminaire : quelques questions sur les polynômes

1.1 - Quelle définition de l'anneau des polynômes en une indéterminée ?

On fixe un anneau commutatif unitaire A.

Notons (provisoirement) $B = A^{(\mathbb{N})}$ l'ensemble des suites d'éléments de A qui sont "à support fini" ce qui signifie que tous les termes sont nuls sauf un nombre fini d'entre eux.

On note $0_B = (0_A, 0_A, \ldots)$. Pour tout élément $f = (a_n)_{n\in\mathbb{N}}$ de B distinct de 0_B, on appelle degré de f le plus grand des entiers $n \in \mathbb{N}$ tels que $a_n \neq 0$. On définit une addition et une multiplication dans B en posant, pour tous $f = (a_n)_{n\in\mathbb{N}}$ et $g = (b_n)_{n\in\mathbb{N}}$ dans B,

$$f + g = (a_n + b_n)_{n\in\mathbb{N}} \quad \text{et} \quad fg = (c_n)_{n\in\mathbb{N}}, \text{ avec } c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

On peut montrer (vérification technique et fastidieuse, mais élémentaire) que, pour ces opérations, B est un anneau commutatif unitaire, avec $0_B = (0_A, 0_A, \ldots)$ et $1_B = (1_A, 0_A, 0_A, \ldots)$. On l'appelle l'anneau des polynômes en une indéterminée à coefficients dans A.

On définit aussi le produit externe d'un élément $\alpha \in A$ par un élément $f = (a_n)_{n\in\mathbb{N}}$ en posant $\alpha f = (\alpha a_n)_{n\in\mathbb{N}}$. A noter que le produit externe αf n'est autre que le produit interne de f par $(\alpha, 0_A, 0_A, \ldots)$. C'est pourquoi on convient de noter encore α l'élément $(\alpha, 0_A, 0_A, \ldots)$ de B, ce qui permet d'identifier A à un sous-ensemble de B. Dans cette identification, les lois définies dans B ci-dessus prolongent celles de A, et donc A est un sous-anneau de B. particulier $0_B = 0_A$ et $1_B = 1_A$.

En posant $e_i = (0_A, 0_A, \ldots, 0_A, 1_A, 0_A, 0_A, \ldots)$, avec 1_A en $(i+1)$-ième position, pour tout $i \in \mathbb{N}$, tout élément de B s'écrit de façon unique $f = \sum_{n\in\mathbb{N}} a_n e_n$ avec les $a_n \in A$ nuls sauf un nombre fini d'entre eux (de sorte que la somme est finie). Il est clair que $e_n e_m = e_{n+m}$ pour tous $n, m \in \mathbb{N}$, et donc $e_n = e_1^n$ pour tout $n \in \mathbb{N}$. On note traditionnellement $X = e_1$ et $B = A[X]$, et l'on retrouve les notations usuellement utilisées pour désigner les polynômes.

On retiendra que :

(a) Pour tout anneau commutatif unitaire A, les polynômes en une indéterminée à coefficients dans A forment un anneau commutatif unitaire, noté $A[X]$, dont A est un sous-anneau. Le neutre pour l'addition est 0_A. Le neutre pour la multiplication est 1_A.

(b) Pour tout élément non nul P de $A[X]$, il existe un unique entier naturel n et un unique $(n+1)$-uplet $(a_0, a_1, \ldots, a_n)$ d'éléments de A, appelés les *coefficients* de P tels que :

$$P = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \quad \text{et} \quad a_n \neq 0.$$

L'entier n est appelé le *degré* de P, noté $\deg P$. L'élément non nul a_n de A est appelé le *coefficient dominant* de P, noté $\mathrm{cd}(P)$. L'élément a_0 est appelé le *terme constant* de P. Par convention, un polynôme est nul si et seulement si tous ses coefficients sont nuls, et l'on pose $\deg 0 = -\infty$ et $\mathrm{cd}(0) = 0$.

(c) Deux polynômes non nuls $P = \sum_{i=0}^{n} a_i X^i$ et $Q = \sum_{i=0}^{m} b_i X^i$ sont égaux si et seulement si $n = m$ et $a_i = b_i$ pour tout $0 \leq i \leq n$.

(d) Si $P = \sum_{i=0}^{n} a_i X^i$ et $Q = \sum_{i=0}^{m} b_i X^i$, on a :

$$P + Q = \sum_{i=0}^{\max(n,m)} (a_i + b_i) X^i \quad \text{et} \quad PQ = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j}\right) X^i,$$

avec la convention de notation $a_i = 0$ si $i > n$ et $b_i = 0$ si $i > m$.

(e) On en déduit que, pour tous P et Q dans $A[X]$, on a :

$$\deg(P+Q) \leq \max(\deg P, \deg Q) \quad \text{et} \quad \deg(PQ) \leq \deg P + \deg Q.$$

1.2 - Importance du fait que l'anneau des cœfficients soit intègre ou non : intégrité et éléments inversibles de l'anneau des polynômes

Proposition. Soit A un anneau commutatif unitaire.

(i) Si A est intègre, alors pour tous polynômes $P, Q \in A[X]$, on a :

$$\deg(PQ) = \deg P + \deg Q \quad \text{et} \quad \mathrm{cd}(PQ) = \mathrm{cd}(P)\,\mathrm{cd}(Q).$$

(ii) $A[X]$ est intègre si et seulement si A est intègre.

(iii) Si A est intègre, alors le groupe des éléments inversibles de $A[X]$ est égal au groupe des éléments inversibles de A.

Preuve. Résulte de façon évidente du fait que, si $P = a_n X^n + \cdots + a_1 X + a_0$ et $Q = b_m X^m + \cdots + b_1 X + b_0$, avec $\mathrm{cd}(P) = a_n \neq 0$ et $\mathrm{cd}(Q) = b_m \neq 0$, alors :

$$PQ = a_n b_m X^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) X^{n+m-1} + \cdots + (a_1 b_0 + a_0 b_1) X + a_0 b_0$$

et de la notion même d'anneau intègre (tout produit de deux éléments non-nuls est non-nul). □

Remarque. Si A n'est pas intègre, $A[X]$ peut contenir des éléments inversibles de degré non-nul.

Par exemple, pour $A = \mathbb{Z}/4\mathbb{Z}$, le polynôme $\overline{2}X + \overline{1}$ est inversible dans $A[X]$, d'inverse égal à lui-même, puisque $(\overline{2}X + \overline{1})(\overline{2}X + \overline{1}) = \overline{1}$. □

Remarque. $A[X]$ n'est jamais un corps, que A soit ou non intègre.

En effet, l'élément X de $A[X]$ vérifie toujours $\deg(PX) = \deg P + 1$ pour tout $P \in A[X]$, de sorte que l'on ne peut pas avoir $PX = 1$, ce qui montre que X n'est jamais inversible. □

1.3 - Importance du fait que l'anneau des cœfficients soit un corps ou non : division euclidienne dans l'anneau des polynômes

Proposition. Soit K un corps commutatif. Quels que soient des polynômes F et G dans $K[X]$, avec $G \neq 0$, il existe $Q \in K[X]$ et $R \in K[X]$ uniques tels que

$$F = GQ + R \quad \text{et} \quad \deg R < \deg G.$$

Preuve. Voir ouvrage de référence. On utilise de façon essentielle le fait que les coefficients des polynômes sont dans un corps, ce qui permet d'inverser le coefficient dominant de G. □

• De fait, le résultat de cette proposition n'est plus vrai si A n'est pas un corps.

Par exemple, prenons dans $\mathbb{Z}[X]$ les polynômes $F = X^2 + 1$ et $G = 3X + 1$. S'il existait $Q, R \in \mathbb{Z}[X]$ tel que $F = GQ + R$ avec $\deg R < \deg G$, on aurait nécessairement $R = r \in \mathbb{Z}$ et $Q = aX + b$ avec $a, b \in \mathbb{Z}$, d'où $X^2 + 1 = (3X + 1)(aX + b) + r$, et en particulier $3a = 1$, ce qui est impossible dans $\mathbb{Z}[X]$.

Attention cependant : on verra un peu plus loin que certaines divisions euclidiennes sont possibles même pour A un anneau quelconque lorsqu'on divise par un polynôme Q unitaire (ou plus généralement de cœfficient dominant inversible dans A), ce qui est utile pour l'étude des racines de polynômes à cœfficients dans un anneau.

• La proposition ci-dessus se traduit en disant que, si K est un corps, alors l'anneau $K[X]$ est euclidien, pour le stathme défini par le degré. En toute généralité, on montre que tout anneau euclidien est principal, mais que la réciproque peut être fausse. Cela ne se produit cependant pas pour les anneaux de polynômes en raison du théorème suivant (pour la preuve, voir ouvrage de référence) :

Théorème. Soit A un anneau commutatif unitaire. Les trois conditions suivantes sont équivalentes :

(i) A est un corps ; (ii) $A[X]$ est euclidien ; (iii) $A[X]$ est principal.

Le fait que $K[X]$ est principal a de nombreuses conséquences importantes, non seulement dans l'arithmétique des polynômes (idéaux premiers et idéaux maximaux, éléments irréductibes et éléments premiers, PPCM et PGCD, Bézout...), mais aussi dans des applications des polynômes dans d'autres domaines (par exemple en algèbre linéaire l'existence du polynôme minimal).

1.4 - Importance du fait que l'anneau des cœfficients soit fini ou non : différence entre polynôme et fonction polynomiale

Soit A un anneau commutatif unitaire.

• Pour tout polynôme $P = \sum_{i=0}^{n} a_i X^i$ de $A[X]$, on appelle fonction polynomiale associée à P l'application $\widetilde{P} : A \to A$ définie par $\widetilde{P}(\alpha) = \sum_{i=0}^{n} a_i \alpha$ pour tout $\alpha \in A$.

L'élément $\widetilde{P}(\alpha)$ est appelé la valeur de P en α. On note parfois simplement $P(\alpha) = \widetilde{P}(\alpha)$.

• Notons $\mathcal{F}(A, A)$ l'ensemble des applications de A dans A. On considère l'application $P \mapsto \widetilde{P}$ de $A[X]$ dans $\mathcal{F}(A, A)$. L'image de $A[X]$ par cette application est appelée l'ensemble des fonctions polynomiales de A dans A, noté $\mathcal{P}(A, A)$. Par construction, on a :

$$\text{l'application } \Phi : A[X] \to \mathcal{P}(A, A),\ P \mapsto \widetilde{P} \text{ est un morphisme d'anneaux surjectif.}$$

• *Attention,* Φ n'est pas nécessairement injective !
Par exemple, pour $A = \mathbb{Z}/3\mathbb{Z}$ et $P = X^3 + \overline{2}X$, $\widetilde{P}$ est la fonction nulle de A dans A bien que P ne soit pas le polynôme nul dans $A[X]$.
On verra cependant plus loin que, si A est infini et intègre, alors Φ est injective, ce qui permet dans ce cas d'identifier la notion de polynôme et de fonction polynomiale, comme on le fait couramment pour les polynômes à coefficients réels ou complexes.

• Soit α un élément de A. En associant à tout polynôme P de $A[X]$ l'élément $\widetilde{P}(\alpha)$ de A, on définit une application de $A[X]$ dans A, noté ev_α dont il est facile de vérifier qu'elle est un morphisme d'anneaux. Cette application

$$\mathrm{ev}_\alpha : A[X] \to A,\ P \mapsto \mathrm{ev}_\alpha(P) = \widetilde{P}(\alpha)$$

est appelé le morphisme d'évaluation en α.

2. Racines d'un polynôme

2.1 - Notion de racine

Définition. Soit A un anneau commutatif unitaire. Soit P un polynôme dans $A[X]$. On dit qu'un élément $\alpha \in A$ est une *racine* de P (ou un *zéro* de P) lorsque $P(\alpha) = 0$.

On a utilisé ici la notation $P(\alpha)$ pour $\widetilde{P}(\alpha)$, la valeur de P en α.

Proposition. Soit A un anneau commutatif unitaire. Soient P un polynôme dans $A[X]$ et α un élément de A. Les conditions suivantes sont équivalentes :

(i) α est une racine de P,

(ii) $(X - \alpha)$ divise P dans $A[X]$ (i.e. il existe $Q \in A[X]$ tel que $P = (X - \alpha)Q$).

Preuve. Il est trivial que (ii) implique (i).

L'implication réciproque est évidente si A est un corps car la division euclidienne permet alors de déduire qu'il existe $Q, R \in A[X]$ tel que $P = (X - \alpha)Q + R$ avec $\deg R < 1$, donc en fait $R = r \in A$. On obtient ainsi une écriture d P de la forme :

$$P = (X - \alpha)Q + r \quad \text{avec } Q \in A[X] \text{ et } r \in A, \quad \text{d'où } r = P(\alpha),$$

d'où le résultat. Mais en fait, même lorsque A n'est pas un corps, on a encore l'écriture ci-dessus (cela provient du fait que le polynôme $(X - \alpha)$ par lequel on divise est unitaire). Vérifions-le de façon élémentaire.

Notons $P = \sum_{i=0}^{n} a_i X^i$. On cherche $Q = \sum_{i=0}^{n-1} b_i X^i$ et $r \in A$ tels que $P = (X - \alpha)Q + r$. Par identification, cette égalité équivaut aux identités :

$$b_{n-1} = a_n, \quad b_{n-k-1} - \alpha b_{n-k} = a_{n-k} \text{ pour } 1 \leq k \leq n-1, \quad r - \alpha b_0 = a_0,$$

qui admettent de proche en proche une unique solution $b_{n-1}, \ldots, b_1, b_0, r$. On achève alors la preuve comme ci-dessus. □

• Donnons à titre d'illustration une première conséquence concrète de la proposition ci-dessus.

Corollaire. Soit A un anneau commutatif unitaire intègre. Soient P un polynôme non-nul dans $A[X]$. Si P admet k racines distinctes dans A, alors $\deg P \geq k$.

Preuve. Notons $\alpha_1, \alpha_2, \ldots, \alpha_k$ des racines deux à deux distinctes de P. D'après la proposition ci-dessus, il existe $Q \in A[X]$ tel que $P = (X - \alpha_1)Q$. Comme $P(\alpha_2) = 0$, on a $(\alpha_1 - \alpha_2)Q(\alpha_2) = 0$. Parce que $\alpha_1 \neq \alpha_2$ et que A est intègre, il en résulte que $Q(\alpha_2) = 0$. En réappliquant la proposition, il existe $S \in A[X]$ tel que $Q = (X - \alpha_2)S$, et donc $P(X - \alpha_1)(X - \alpha_2)S$. On recommence avec α_3 et l'on obtient par itération $P = (X - \alpha_1)(X - \alpha_2) \cdots (X - \alpha_k)T$ pour un certain $T \in A[X]$.

En réutilisant l'intégrité de A, on conclut que $\deg P = k + \deg T$, d'où la minoration voulue. □

Le résultat de ce corollaire peut être faux lorsque A n'est pas intègre.

1. Contre-exemple avec A fini : pour $A = \mathbb{Z}/4\mathbb{Z}$, le polynôme $\overline{2}X$ dans $A[X]$ est de degré 1 mais admet deux racines distinctes $\overline{0}$ et $\overline{2}$.
2. Contre-exemple plus général : soit A un anneau non intègre quelconque, fini ou infini ; soient a, b deux éléments non-nuls de A tels que $ab = 0$. Alors le polynôme $X^2 - (a+b)X$ dans $A[X]$ est de degré 2 mais admet quatre racines distinctes 0, a, b et $a + b$.

• Une autre conséquence concerne l'injectivité de l'application associant une fonction polynomiale à un polynôme.

Corollaire. Soit A un anneau commutatif unitaire intègre infini. L'anneau de polynômes $A[X]$ est isomorphe à l'anneau des fonctions polynomiales $\mathcal{P}(A, A)$.

Preuve. On a déjà vu plus haut que l'application $\Phi : A[X] \to \mathcal{P}(A, A), P \mapsto \widetilde{P}$ est un morphisme d'anneaux surjectif. Si $P \,\mathrm{Ker} \in \Phi$, la fonction $\widetilde{P}$ s'annule en tous les éléments de A, donc le polynôme P admet une infinité de racines. Il résulte alors du corollaire précédent que P est la polynôme nul. Ainsi Φ est injective et réalise donc un isomorphisme d'anneaux. □

2.2 - Ordre de multiplicité

Définitions et proposition. Soit A un anneau commutatif unitaire. Soit P un polynôme dans $A[X]$ et k un entier ≥ 1. On dit qu'un élément $\alpha \in A$ est une racine d'*ordre k* de P lorsque P est divisible par $(X-\alpha)^k$ mais pas par $(X-\alpha)^{k+1}$.

Ceci équivaut à l'existence d'un polynôme $Q \in A[X]$ tel que :

$$P = (X-\alpha)^k Q \quad \text{avec } Q(\alpha) \neq 0.$$

Une racine d'ordre 1 est dite *simple*. Une racine d'ordre ≥ 2 est dite *multiple*. Les racines d'ordre 2, 3... dont dites doubles, triples...

Preuve. Supposons que $\alpha \in A$ est une racine d'ordre k de P. Alors P est divisible par $(X-\alpha)^k$ donc il existe $Q \in A[X]$ tel que $P = (X-\alpha)^k Q$. Si l'on avait $Q(\alpha) = 0$, alors α serait une racine de Q, donc $(X-\alpha)$ diviserait Q d'après la proposition 2.1, donc $(X-\alpha)^{k+1}$ diviserait P, contradiction. Donc $Q(\alpha) \neq 0$. L'implication réciproque est claire. □

Théorème. Soit A un anneau commutatif unitaire intègre. Soit P un polynôme non-nul dans $A[X]$. Soient $\alpha_1, \alpha_2, \ldots, \alpha_s$ des racines deux à deux distinctes de P, d'ordre respectifs $k_1, k_2, \ldots, k_s$. Alors il existe un polynôme $Q \in A[X]$ tels que :

$$P = (X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}\cdots(X-\alpha_s)^{k_s}Q, \quad \text{avec } Q(\alpha_i) \neq 0 \text{ pour tout } 1 \leq i \leq s.$$

Preuve. D'après la proposition précédente, P est divisible par $(X-\alpha_i)^{k_i}$ pour tout $1 \leq i \leq s$.

Dans le cas où A est un corps (on notera alors $A = K$) on conclut rapidement car l'anneau $K[X]$ étant principal, P est divisible par le PGCD des $(X-\alpha_i)^{k_i}$, qui n'est autre que leur produit puisque les $(X-\alpha_i)^{k_i}$ sont premiers entre eux.

Si l'on ne suppose plus que A est un corps, mais seulement un anneau intègre, le résultat reste vrai moyennant une preuve un peu plus élaborée. Comme α_1 et α_2 sont des racines de P dans A d'ordre respectif k_1 et k_2, il existe deux polynômes Q_1 et Q_2 dans $A[X]$ tels que $P = (X-\alpha_1)^{k_1}Q_1 = (X-\alpha_2)^{k_2}Q_2$ avec $Q_1(\alpha_1)$ et $Q_2(\alpha_2)$ non-nuls dans A. Notons K le corps des fractions de A. En tant que polynômes de $K[X]$, les polynômes $(X-\alpha_1)^{k_1}$ et $(X-\alpha_2)^{k_2}$ sont premiers entre eux, donc d'après la propriété de Bézout appliquée dans l'anneau principal $K[X]$, il existe deux polynômes U et V dans $K[X]$ tels que $(X-\alpha_1)^{k_1}U + (X-\alpha_2)^{k_2}V = 1$.

En multipliant les deux membres par le produit c de tous les dénominateurs des cœfficients de U et V dans K, on obtient une égalité dans $A[X]$ de la forme

$$(X-\alpha_1)^{k_1}S + (X-\alpha_2)^{k_2}T = c \quad \text{avec } S, T \in A[X] \text{ et } c \in A.$$

Puisque $P = (X-\alpha_1)^{k_1}Q_1$, le produit par Q_1 des deux membres de cette égalité conduit à :

$$cQ_1 = PS + (X-\alpha_2)^{k_2}TQ_1 = (X-\alpha_2)^{k_2}Q_2S + (X-\alpha_2)^{k_2}TQ_1.$$

Il en résulte que $(X-\alpha_2)^{k_2}$ divise cQ_1 dans $A[X]$, donc divise Q_1, de sorte qu'il existe $Q \in A[X]$ tel que $Q_1 = (X-\alpha_2)^{k_2}Q$, et finalement $P = (X-\alpha_1)^{k_1}(X-\alpha_2)^{k_2}Q$. On achève la preuve en itérant le processus. □

• *Un premier exemple d'application.* Soit K le corps $\mathbb{Z}/p\mathbb{Z}$ avec p un nombre premier. Alors $X^p - X = \prod_{\alpha \in K}(X - \alpha)$.

Preuve. D'après le petit théorème de Fermat, on a $\alpha^p = \alpha$ pour tout $\alpha \in K$. Donc les éléments de K sont p racines distinctes du polynôme $P = X^p - X$. Donc P est divisible par $\prod_{\alpha \in K}(X - \alpha)$. Les deux polynômes étant unitaires de degré p, on en déduit l'égalité voulue. □

• *Un second exemple d'application (interpolation de Lagrange).* Soit K un corps commutatif quelconque. Quels que soient $\alpha_1, \ldots, \alpha_n$ des éléments distincts de K et $\lambda_1, \ldots, \lambda_n$ des éléments de K, il existe un unique polynôme P de degré $\leq n-1$ tel que $P(\alpha_i) = \lambda_i$ pour tout $1 \leq i \leq n$.

Preuve. Pour tout $1 \leq i \leq n$, on introduit le polynôme $Q_i = \prod_{k=1}^{n}(X - \alpha_k)/(X - \alpha_i)$, qui est de degré $n-1$ dans $K[X]$. Il vérifie $Q_i(\alpha_k) = 0$ pour tout $1 \leq k \neq i \leq n$, et $Q_i(\alpha_i) \neq 0$ car les α_k sont supposés distincts. On introduit alors le polynôme interpolateur de Lagrange $L_i = \frac{1}{Q_i(x_i)}Q_i$, qui est aussi de degré $n-1$. Le polynôme $P = \sum_{i=1}^{n} \lambda_i L_i$ est par construction l'unique solution du problème. □

2.3 - Utilisation de la dérivation des polynômes

• L'existence ou non de racines multiples peut être identifiée en utilisant la notion de polynôme dérivé (supposée connue, voir cours de référence). On a d'abord le résultat général suivant.

Proposition. Soit A un anneau commutatif unitaire. Soit P un polynôme dans $A[X]$. Un élément $\alpha \in A$ est une racine multiple de P si et seulement si $P(\alpha) = P'(\alpha) = 0$.

Preuve. Si α est racine multiple de P, il existe $Q \in A[X]$ tel que $P = (X - \alpha)^k Q$ avec $k \geq 2$. On calcule $P' = (X - \alpha)^k Q' + k(X - \alpha)^{k-1}Q$, d'où $P'(\alpha) = 0$ puisque $k - 1 \geq 1$.

Supposons réciproquement que $P(\alpha) = P'(\alpha) = 0$. Puisque $P(\alpha) = 0$, il existe $Q \in A[X]$ tel que $P = (X - \alpha)Q$. D'où $P' = Q + (X - \alpha)Q'$. Puisque $P'(\alpha) = 0$, on en déduit que $Q(\alpha) = 0$ donc il existe $S \in A[X]$ tel que $Q = (X - \alpha)S$. Ainsi $P = (X - \alpha)^2 S$, ce qui montre le résultat voulu. □

• Aller plus loin par la même méthode élémentaire pour spécifier l'existence de racine double ou triple soulève aussitôt des questions quant à la caractéristique de A. On peut effectivement montrer la proposition suivante pour tout anneau A de caractéristique nulle (en particulier en remplaçant l'usage des dérivées par les hyperdérivées) mais on se limite dans le cadre de cet exposé au cas le plus simple où A est un corps commutatif de caractéristique nulle.

Proposition. Soit K un corps de caractéristique nulle. Soit P un polynôme non-nul de $K[X]$. Un élément $\alpha \in K$ est une racine de P d'ordre égal à k si et seulement si :

$$P(\alpha) = P'(\alpha) = \cdots = P^{(k)}(\alpha) = 0 \quad \text{et} \quad P^{(k+1)}(\alpha) \neq 0.$$

Preuve. Soit $P \in K[X]$ de degré n. La formule de Taylor (que l'on suppose ici connue, voir cours de référence) s'écrit

$$P(X) = \sum_{j=0}^{n} \tfrac{1}{j!}(X - \alpha)^j P^{(j)}(\alpha).$$

Il en résulte que, pour tout $1 \leq m \leq n$, le polynôme $(X - \alpha)^m$ divise P si et seulement si $P(\alpha) = P'(\alpha) = \cdots = P^{m-1}(\alpha)$, d'où le résultat. □

• Rappelons pour mémoire que si K est de caractéristique nulle, il est nécessairement infini (tout corps fini est de caractéristique première), propriété qui intervient dans plusieurs des énoncés que l'on a vu ci-dessus.

2.4 - Racines et irréductibilité

• D'une façon générale, un élément x d'un anneau commutatif unitaire intègre A est dit *irréductible* dans A lorsqu'il n'est pas inversible dans A, et vérifie :

$$\text{si } x = ab \text{ avec } a, b \in A, \text{ alors } a \text{ ou } b \text{ est inversible dans } A.$$

Appliquons cette définition à un anneau de polynôme $A[X]$ où A est un anneau commutatif unitaire intègre ; comme on l'a vu en 1.2, l'anneau $A[X]$ est alors lui-même intègre et les polynômes inversibles sont les constantes inversibles, c'est-à-dire les éléments de A inversibles dans A. On obtient ainsi la formulation suivante :

Définition. Soit A un anneau commutatif unitaire intègre. Soit P un polynôme dans $A[X]$. On dit que P est *irréductible* lorsque P n'est pas un élément de A inversible dans A, et qu'il vérifie pour tous $P, Q \in A[X]$:

$$\text{si } P = QR, \text{ alors } Q \text{ ou } R \text{ est un élément de } A \text{ inversible dans } A.$$

Dans le cas particulier où A est un corps, cette définition devient :

Définition. Soit K un corps commutatif. Soit P un polynôme dans $K[X]$. On dit que P est *irréductible* lorsque $P \notin K^*$ et qu'il vérifie pour tous $Q, R \in K[X]$:

$$\text{si } P = QR, \text{ alors } Q \in K^* \text{ ou } R \in K^*.$$

• Il ne s'agit pas ici de faire l'étude de la notion de polynôme irréductible, qui est très riche, mais seulement de souligner, en se limitant au cas de polynômes à cœfficients dans un corps commutatif K, quelques liens évidents entre cette notion et celle de racine :

1. tout polynôme de degré 1 dans $K[X]$ est irréductible dans $K[X]$;
2. un polynôme de $K[X]$ de degré ≥ 2 qui est irréductible n'admet pas racine dans K ;
3. la réciproque de ces deux assertions est fausse.

Un résultat fondamental est que tout polynôme non constant de $K[X]$ se décompose en un produit de polynômes irréductibles, de façon unique (à l'ordre près des facteurs et au produit par des constantes non-nulles près). On dit que l'anneau $K[X]$ est factoriel. En particulier un polynôme est dit *scindé* dans $K[X]$ s'il se décompose en un produit de polynômes de degré 1.

• Les situations où la réciproque de l'assertion 1 ci-dessus est vraie correspondent à la notion suivante :

Définition et proposition. Un corps commutatif K est dit *algébriquement clos* s'il vérifie l'une des conditions équivalentes suivantes :

(i) tout polynôme non constant de $K[X]$ admet au moins une racine dans K ;

(ii) tout polynôme de $K[X]$ de degré $n \geq 1$ admet exatement n racines (comptées avec leur ordre de multiplicité) dans K ;

(iii) les polynômes irréductibles dans $K[X]$ sont les polynômes de degré 1 ;

(iv) tout polynôme non constant de $K[X]$ est scindé.

Preuve. L'équivalence des quatre assertions est immédiate. □

✓ On va voir ci-dessous que le corps $\mathbb{C}$ est algébriquement clos et que les corps que $\mathbb{R}$ et $\mathbb{Q}$ ne sont pas algébriquement clos.

✓ Un corps fini K n'est jamais algébriquement clos (en effet le polynôme $\prod_{a\in K}(X-a)+1$ n'a pas de racine dans K puisqu'il prend la valeur 1 en tous les éléments de K).

✓ On peut montrer en théorie des corps que tout corps commutatif admet une extension (non unique) qui est algébriquement close.

2.5 - Cas particulier des polynômes à cœfficients complexes ou réels

• Un exemple fondamental de corps algébriquement clos est donné par le théorème suivant :

Théorème. Le corps $\mathbb{C}$ des nombres complexes est algébriquement clos.

Ce théorème est connu sous le nom de **théorème de d'Alembert-Gauss**. C'est un résultat non immédiat, mais dont diverses preuves peuvent être abordées au niveau de ce document. Elles sont de fait assez longues et élaborées : nous ne les détaillons pas ici et renvoyons aux ouvrages de référence.

• Cas du corps de nombres réels.

Commençons par rappeler les deux faits élémentaires suivants :

(a) Tout polynôme de $\mathbb{R}[X]$ de degré impair admet au moins une racine dans $\mathbb{R}$.

(b) Soit $P = aX^2+bX+c$ avec $a, b, c \in \mathbb{R}$, $a \neq 0$. Il admet deux racines réelles (éventuellement égales) lorsque son discriminant $\Delta = b^2 - 4ac$ est positif. Il n'admet aucune racine réelle lorsque Δ est strictement négatif.

On déduit du théorème de d'Alembert-Gauss une caractérisation des polynômes irréductibles dans $\mathbb{R}[X]$.

Corollaire. Les polynômes irréductibles dans $\mathbb{R}[X]$ sont les polynômes de degré 1 et les polynômes de degré 2 de discriminant strictement négatif.

Preuve. Soit $P \in \mathbb{R}[X]$ de degré $n \geq 2$ que l'on suppose irréductible dans $\mathbb{R}[X]$. Il n'a donc pas de racine réelle. Mais en tant que polynôme de $\mathbb{C}[X]$, il admet au moins une racine $\alpha \in \mathbb{C}$, avec $\alpha \notin \mathbb{R}$. Le polynôme $S = (X-\alpha)(X-\overline{\alpha}) = X^2 - (\alpha+\overline{\alpha})X + \alpha\overline{\alpha}$ appartient à $\mathbb{R}[X]$. On peut donc effectuer dans $\mathbb{R}[X]$ la division euclidienne $P = QS+R$ avec $Q, R \in \mathbb{R}[X]$ et $\deg R < 2$. Or $P(\alpha) = S(\alpha) = 0$. Donc R est un polynôme de degré ≤ 1 à cœfficients dans $\mathbb{R}$ qui s'annule en $\alpha \notin \mathbb{R}$: ce ne peut être que le polynôme nul. Ainsi $P = S = X^2 + bX + c$ avec $b = -(\alpha+\overline{\alpha})$ et $c = \alpha\overline{\alpha}$, d'où le résultat. □

• On peut citer à titre d'application le résultat classique suivant qui relie la répartition des racines complexes (ou réelles) de P avec celle des racines de P'.

Théorème (dit de Gauss-Lucas). Soit P un polynôme de degré $n \geq 2$ dans $\mathbb{C}[X]$. L'ensemble des points du plan dont les affixes sont les racines de P' est inclus dans l'enveloppe convexe de l'ensemble des points du plan dont les affixes sont les racines de P.

Preuve. Notons $P(X) = a_n(X-r_1)^{\alpha_1}(X-r_2)^{\alpha_2}\cdots(X-r_m)^{\alpha_m}$ où les r_i sont les m racines complexes distincts de P et α_i leur multiplicités. Les α_i sont donc non-nulles et telles que $\alpha_1+\alpha_2+\cdots+\alpha_m = n$. On calcule $P'(X) = \sum_{j=1}^{m} \frac{\alpha_j P(X)}{X-r_j}$, d'où l'on déduit que :

$$\frac{P'(z)}{P(z)} = \sum_{j=1}^{m} \frac{\alpha_j}{z-r_j} \quad \text{pour tout } z \in \mathbb{C}\setminus\{r_1, r_2, \ldots, r_m\}.$$

En appliquant cette identité à un nombre complexe r qui est une racine de P' mais n'est pas une racine de P, on déduit par des calculs simples dans $\mathbb{C}$ que :

$$\sum_{j=1}^{m} \frac{\alpha_j}{|r-r_j|^2}(r-r_j) = 0, \quad \text{d'où} \quad r = \Big[\sum_{j=1}^{m} \frac{\alpha_j}{|r-r_j|^2}\Big]^{-1} \sum_{j=1}^{m} \frac{\alpha_j}{|r-r_j|^2}\, r_j.$$

Pour tout $1 \le j \le m$, on pose $\lambda_j = \Big[\sum_{j=1}^{m} \frac{\alpha_j}{|r-r_j|^2}\Big]^{-1} \frac{\alpha_j}{|r-r_j|^2}$. On a donc $r = \sum_{j=1}^{m} \lambda_j r_j$, où les λ_j sont des réels positifs vérifiant $\lambda_1+\lambda_2+\cdots+\lambda_m = 1$, ce qui montre que le point d'affixe r est barycentre à coefficients positifs des points $A_1, A_2, \ldots, A_r$ d'affixes respectives $r_1, r_2, \ldots, r_m$.

On a ainsi montré que tout point du plan dont l'affixe est une racine de P' mais pas de P est dans l'enveloppe convexe de l'ensemble des points $A_1, A_2, \ldots, A_r$. C'est encore vrai pour un point dont l'affixe est une racine de P' et de P (puisque c'est alors l'un des points A_j), ce qui achève la preuve. □

Corolllaire. Soit P un polynôme de degré $n \ge 2$ dans $\mathbb{R}[X]$. Si P est scindé sur $\mathbb{R}$, alors P' est scindé sur $\mathbb{R}$. De plus, l'ensemble des racines de de P' est inclus dans le segment $[r_1, r_m]$ où r_1 est la plus petite racine et r_m la plus grande racine de P.

Exercice. Sous les hypothèses du théorème, l'isobarycentre des points dont les affixes sont les racines de P est égal à l'isobaycentre des points dont les affixes sont les racines de P'.

En effet : notons $P(X) = \sum_{i=0}^{n} a_i X^i$ avec $a_i \in \mathbb{C}$, $a_n \neq 0$. Si l'on désigne par $z_1, \ldots, z_n$ les n racines de P (non nécessairement distinctes), alors $z_1+\cdots+z_n = -\frac{a_{n-1}}{a_n}$. De même, si l'on désigne par $z'_1, \ldots, z'_{n-1}$ les n racines de $P'(X) = \sum_{i=1}^{n} i a_i X^{i-1}$ (non nécessairement distinctes), on a $z'_1+\cdots+z'_{n-1} = -\frac{(n-1)a_{n-1}}{n a_n}$.

On en déduit que $\frac{1}{n}(z_1+\cdots+z_n) = \frac{1}{n-1}(z'_1+\cdots+z'_{n-1})$, ce qui prouve le résultat voulu.□

2.6 - Racines et extension de corps

Rappelons d'abord que si K est un corps commutatif et L est un corps commutatif tel que K est un sous-corps de L, on dit que L est une extension de K.

Lemme. Soient K un corps commutatif et P un polynôme irréductible dans $K[X]$. Alors il existe une extension L de K telle que P admette au moins une racine dans L.

Preuve. On considère l'anneau de polynômes $A = K[X]$ et l'idéal principal I de A engendré par P. Parce que K est un corps, A est un anneau principal, et parce que P est un élément irréductible de A, l'idéal I est alors un idéal maximal de A. Il en résulte que l'anneau quotient $L = A/I$ est un corps. Soit π la surjection canonique $K[X] \to L$, définie par $\pi(F) = \overline{F}$ pour tout $F \in K[X]$, qui est un morphisme d'anneau.

En restreignant π à K, on obtient l'application $i : K \to L$ qui associe à tout $a \in K$ sa classe $\overline{a}$ dans L. Cette application i est un morphisme de corps, qui est clairement injectif (car $\overline{a} = \overline{0}$ signifie que a est un multiple de P dans $K[X]$, ce qui n'est possible que si $a = 0$). Le corps K peut donc être identifié à son image $i(K)$ dans L, en notant donc $\overline{a} = a$. L'image $i(K)$ étant un sous-corps de L, on obtient ainsi L comme une extension de K.

Notons ensuite $x = \pi(X) = \overline{X}$, de sorte que pour tout polynôme $Q = \sum_{i=0}^{n} a_i X^i \in K[X]$, avec $a_1, a_2, \ldots, a_n \in K$, on a $\pi(Q) = \pi(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \overline{a_i}\,\overline{X}^i = \sum_{i=0}^{n} a_i x^i$. Si l'on choisit pour Q le polynôme irréductible P donné au départ, on a $\pi(P) = 0$ par construction, donc $P(x) = 0$, ce qui fait apparaître x comme une racine de P dans L. □

Premier exemple : prenons $\mathbb{K} = \mathbb{R}$ et $P = X^2 + 1$, qui est irréductible dans $\mathbb{R}[X]$. On a $L = \mathbb{R}[X]/(X^2+1)$ qui correspond au corps $\mathbb{C}$, avec $i = \pi(X)$ qui vérifie $i^2 + 1 = 0$ donc $i^2 = -1$.

Second exemple : prenons $\mathbb{K} = \mathbb{Q}$ et $P = X^2 - 3$, qui est irréductible dans $\mathbb{Q}[X]$. On a $L = \mathbb{Q}[X]/(X^2-3)$ qui correspond au corps $\mathbb{Q}[\sqrt{3}] = \{x + y\sqrt{3}\,;\, x, y \in \mathbb{Q}\}$, avec $\sqrt{3} = \pi(X)$ qui vérifie $(\sqrt{3})^2 - 3 = 0$, donc $(\sqrt{3})^2 = 3$.

Théorème. Soient K un corps commutatif et P un polynôme non-constant dans $K[X]$. Alors :

(i) il existe une extension L de K telle que P admette au moins une racine dans L.

(ii) il existe une extension L de K telle que P soit scindé dans $L[X]$.

Preuve. Pour l'assertion (i), il suffit de considérer un polynôme Q irréductible dans $K[X]$ qui divise P. D'après le lemme, il existe une extension L de K telle que Q admette dans L une racine α. Comme Q divise P, cet élément $\alpha \in L$ est aussi une racine de P.

Pour l'assertion (ii), on raisonne par récurrence sur le degré n. Plus précisément, on démontre par récurrence sur n l'assertion : pour tout corps commutatif K et tout polynôme $P \in K[X]$ de degré n, il existe une extension L de K telle que P est scindé sur L. Pour les détails de rédaction voir ouvrage de référence. □

Une extension L vérifiant l'assertion (i) est parfois appelé un corps de rupture du polynôme P. Une extension L vérifiant l'assertion (ii) est appelé un corps de décomposition du polynôme P.

3. Relations entre racines et cœfficients

3.1 - Polynômes symétriques élémentaires

Commençons par rappeler la définition générale suivante.

Définition. Soit $A[X_1, X_2, \ldots, X_n]$ l'anneau des polynômes en n indéterminées à cœfficients dans un anneau commutatif unitaire A intègre. On appelle *polynômes symétriques élémentaires* les n polynômes suivants :

$$\begin{aligned}
&\Sigma_1 = X_1 + X_2 + \cdots + X_n,\\
&\Sigma_2 = X_1X_2 + X_1X_3 + \cdots + X_1X_n + X_2X_3 + \cdots + X_2X_n + \cdots + X_{n-1}X_n,\\
&\cdots\\
&\Sigma_k = \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} X_{i_1}X_{i_2}\ldots X_{i_k} \quad \text{pour tout } 1 \le k \le n, \text{ (somme de } \tbinom{n}{k} \text{ termes)},\\
&\cdots\\
&\Sigma_n = X_1X_2\ldots X_n.
\end{aligned}$$

Les polynômes Σ_i sont symétriques au sens où ils sont invariants par toute permutation des indéterminés. Aux côtés d'autres formes classiques (somme de Newton, polynômes de Wronski...),

ils jouent un rôle important dans l'étude des polynômes symétriques (ils engendrent l'algèbre des polynômes symétriques).

Remarque. On vérifie par un calcul élémentaire que dans l'anneau $A[X_1, X_2, \ldots, X_n][T]$, le polynôme $P(T) = (T - X_1)(T - X_2)\ldots(T - X_n)$ vérifie :

$$P(T) = T^n - \Sigma_1 T^{n-1} + \Sigma_2 T^{n-2} - \cdots + (-1)^{n-1}\Sigma_{n-1}T + (-1)^n\Sigma_n.$$

Cette simple observation est à la base du résultat suivant, qui relie les racines et les cœfficients d'un polynôme P à coefficient dans un corps commutatif.

3.2 - Fonctions symétriques élémentaires des racines d'un polynôme

Proposition. Soit K un corps commutatif. Soient $\alpha_1, \alpha_2, \ldots, \alpha_n$ des éléments quelconques de K. Pour tout $1 \leq i \leq n$, posons $\sigma_i = \Sigma_i(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Alors $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont les racines du polynôme :

$$X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \cdots + (-1)^n\sigma_n \quad \text{de } K[X].$$

Preuve. Conséquence immédiate de la dernière remarque de 3.1, où $\sigma_k = \Sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ désigne l'évaluation en les α_i du k-ième polynôme symétrique élémentaire. □

Théorème. Si K est un corps algébriquement clos, alors pour tout polynôme $P = \sum_{i=0}^n a_i X^i$ de $K[X]$ de degré $n \geq 1$, les n racines $\alpha_1, \alpha_2, \ldots, \alpha_n$ de P vérifient :

$$\Sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n) = (-1)^k \frac{a_{n-k}}{a_n}, \quad \text{pour tout } 1 \leq k \leq n.$$

Preuve. Soit $P = \sum_{i=0}^n a_i X^i$ un polynôme de $K[X]$, de degré $n \geq 1$. Comme K est algébriquement clos, P admet n racines $\alpha_1, \alpha_2, \ldots, \alpha_n$ dans K, et se factorise en :

$$P(X) = \textstyle\sum_{i=0}^n a_i X^i = a_n \prod_{j=1}^n (X - \alpha_j), \quad \text{avec } a_n \neq 0.$$

Comme ci-dessus, on a en notant $\sigma_k = \Sigma_k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ l'égalité :

$$\textstyle\prod_{j=1}^n (X - \alpha_i) = X^n - \sigma_1 X^{n-1} + \sigma_2 X^{n-2} - \cdots + (-1)^{n-1}\sigma_{n-1}X + (-1)^n\sigma_n.$$

On en déduit par identification que : $a_{n-1} = -a_n\sigma_1$, $a_{n-2} = a_n\sigma_2$, …, jusqu'à $a_1 = (-1)^{n-1}a_n\sigma_{n-1}$, $a_0 = (-1)^n a_n\sigma_n$. □

• *Exemple 1.* Pour $P(X) = aX^2 + bX + c \in \mathbb{C}[X]$, avec $a \neq 0$, on retrouve le résultat bien connu :

$$\sigma_1 = \alpha_1 + \alpha_2 = -\frac{b}{a} \quad \text{et} \quad \sigma_2 = \alpha_1\alpha_2 = \frac{c}{a}.$$

• *Exemple 2.* Pour $P(X) = X^3 + pX + q \in \mathbb{C}[X]$, on retrouve le résultat bien connu :

$$\sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 = 0, \quad \sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = p \quad \text{et} \quad \sigma_3 = \alpha_1\alpha_2\alpha_3 = -q.$$

• *Exemple 3.* Si A est une matrice carrée d'ordre n à cœfficients dans $\mathbb{C}$, alors l'application du théorème ci-dessus au polynôme caractéristique de A donne en particulier que :

$$\det A = \textstyle\prod_{i=1}^n \lambda \;\text{ et }\; \operatorname{tr} A = \sum_{i=1}^n \lambda_i,$$

où $\lambda_1, \ldots, \lambda_n$ désignent les valeurs propres distinctes de A comptées avec leur multiplicité.

4. Résultant et discriminant

4.1 - Notion de résultant de deux polynômes

Dans toute cette partie, K est un corps algébriquement clos. On cherche à résoudre la question suivante : étant donnés deux polynômes distincts P et Q de degré ≥ 1 dans $K[X]$, trouver une condition nécessaire et suffisante pour qu'ils admettent au moins une racine commune. Dire que P et Q admettent une racine commune $\alpha \in K$ équivaut à dire que le polynôme $X - \alpha$ divise à la fois P et Q dans $K[X]$, ou encore que leur pgcd dans l'anneau $K[X]$ est de degré ≥ 1.

Définition. Soit K un corps algébriquement clos. Soient P et Q deux polynômes non-nuls dans $K[X]$ de degrés respectifs $m \geq 1$ et $n \geq 1$. Notons :

$$P = \sum_{i=0}^{m} a_i X^i \quad \text{et} \quad Q = \sum_{i=0}^{n} b_i X^i, \qquad a_i, b_i \in K, \ \ a_m \neq 0, \ \ b_n \neq 0.$$

On appelle *résultant de P et Q* le déterminant d'ordre $m+n$ suivant :

$$R(P,Q) = \left| \begin{array}{cccccccccc}
a_m & 0 & . & 0 & 0 & b_n & 0 & . & 0 & 0 \\
a_{m-1} & a_m & . & . & . & b_{n-1} & b_n & . & . & . \\
a_{m-2} & a_{m-1} & . & . & . & b_{n-2} & b_{n-1} & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & a_m & 0 & . & . & . & . & . \\
a_{m-n+1} & a_{m-n+2} & . & a_{m-1} & a_m & b_1 & . & . & . & . \\
a_{m-n} & a_{m-n+1} & . & a_{m-2} & a_{m-1} & b_0 & b_1 & . & . & . \\
a_{m-n-1} & a_{m-n} & . & . & a_{m-2} & 0 & b_0 & . & . & . \\
. & . & . & . & . & 0 & 0 & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & 0 & . \\
a_2 & a_3 & . & a_n & a_{n+1} & 0 & . & . & b_n & 0 \\
a_1 & a_2 & . & a_{n-1} & a_n & 0 & . & . & b_{n-1} & b_n \\
a_0 & a_1 & . & a_{n-2} & a_{n-1} & 0 & . & . & b_{n-2} & b_{n-1} \\
0 & a_0 & . & . & . & . & . & . & . & . \\
. & . & . & . & . & . & . & . & . & . \\
. & . & . & a_0 & a_1 & . & . & . & b_0 & b_1 \\
0 & 0 & . & 0 & a_0 & 0 & 0 & . & 0 & b_0
\end{array} \right|
\begin{array}{l}
\leftarrow 1 \\ \leftarrow 2 \\ \leftarrow 3 \\ \\ \\ \leftarrow n \\ \leftarrow n+1 \\ \leftarrow n+2 \\ \\ \\ \\ \leftarrow m-1 \\ \leftarrow m \\ \leftarrow m+1 \\ \\ \\ \\ \leftarrow m+n
\end{array}$$

$$\underbrace{\qquad\qquad\qquad\qquad}_{n} \qquad \underbrace{\qquad\qquad\qquad\qquad}_{m}$$

Remarque. On a supposé ci-dessus que $m > n$, pour fixer clairement l'écriture du déterminant. L'analogue pour $m \leq n$ s'en déduit mutatis mutandis.

Lemme. Soit K un corps algébriquement clos. Soient P et Q deux polynômes dans $K[X]$ de degrés respectifs $m \geq 1$ et $n \geq 1$. Ils admettent une racine commune dans K si et seulement s'il existe des polynômes R et S dans $K[X]$ tels que :

$$\deg R \leq m-1, \quad \deg S \leq n-1, \quad RQ = SP.$$

Preuve. Supposons les trois conditions du lemme vérifiées. Appelons $\alpha_1, \alpha_2, \ldots, \alpha_m$ les racines (non nécessairement distinctes) de P dans K. Alors, pour tout $1 \leq i \leq m$, le polynôme $X - \alpha_i$ divise P, donc divise RQ, dans $K[X]$. Puisque $X - \alpha_i$ est de degré 1, on a nécessairement $X - \alpha_i$ qui divise R ou $X - \alpha_i$ qui divise Q, et ceci quel que soit $1 \leq i \leq m$. Comme $\deg R < m$, on ne peut pas avoir R divisible par $(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_m)$. C'est donc qu'il existe au moins un indice $1 \leq i_0 \leq m$ tel que $X - \alpha_{i_0}$ divise Q. Ainsi α_{i_0} est une racine commune à P et Q dans K.

Réciproquement, supposons que P et Q aient une racine commune $\alpha \in K$. Si D est un pgcd de P et Q dans $K[X]$, on a $\deg D \geq 1$, et il existe des polynômes non-nuls R et S dans $K[X]$ tels que $P = RD$ et $Q = SD$, avec $\deg R < \deg P$ et $\deg S < \deg Q$. On a alors l'égalité $RQ = RSD = SP$.□

Théorème. Soit K un corps algébriquement clos. Deux polynômes non-constants de $K[X]$ ont au moins une racine commune dans K si et seulement si leur résultant est nul.

Preuve. Soient $P = \sum_{i=0}^{m} a_i X^i$ et $Q = \sum_{i=0}^{n} b_i X^i$ dans $K[X]$, de degrés respectifs $m \geq 1$ et $n \geq 1$. D'après le lemme, l'existence d'une racine commune à P et Q équivaut à l'existence de deux polynômes non-nuls $R = \sum_{i=0}^{m-1} \lambda_i X^i$, de degré $\leq m-1$, et $S = \sum_{i=0}^{n-1} \mu_i X^i$, de degré $\leq n-1$, tels que $RQ = SP$. Par identification, cette égalité équivaut aux relations :

$$\begin{cases} a_m\mu_{n-1} & = & b_n\lambda_{m-1} \\ a_{m-1}\mu_{n-1} + a_m\mu_{n-2} & = & b_{n-1}\lambda_{m-1} + b_n\lambda_{m-2} \\ a_{m-2}\mu_{n-1} + a_{m-1}\mu_{n-2} + a_m\mu_{n-3} & = & b_{n-2}\lambda_{m-1} + b_{n-1}\lambda_{m-2} + b_n\lambda_{m-3} \\ \cdots & \cdots & \cdots \\ a_0\mu_1 + a_1\mu_0 & = & b_0\lambda_1 + b_1\lambda_0 \\ a_0\mu_0 & = & b_0\lambda_0 \end{cases}$$

En faisant "tout passer" dans le premier membre, on obtient un système linéaire homogène, de $m+n$ équations à $m+n$ inconnues, qui sont $\mu_{n-1}, \mu_{n-2}, \ldots, \mu_0, -\lambda_{m-1}, -\lambda_{m-2}, \ldots, -\lambda_0$. Il admet une solution non-nulle si et seulement si son déterminant est nul. Or ce dernier n'est autre que le résultant $R(P,Q)$, d'où le résultat. □

Corollaire. Soit K un corps algébriquement clos. Deux polynômes non-constants de $K[X]$ sont premiers entre eux dans $K[X]$ si et seulement si leur résultant est non-nul.

Preuve. On a déjà observé au début du paragraphe que l'existence d'une racine commune à P et Q équivaut au fait que leur pgcd est de degré ≥ 1, c'est-à-dire que P et Q ne sont pas premiers entre eux. D'où le résultat d'après le théorème précédent. □

Exemples en petits degrés.

- Si $P = aX + b$ et $Q = cX + d$, alors $R(P,Q) = ad - bc$.
- Si $P = aX^2 + bX + c$ et $Q = pX + q$, alors $R(P,Q) = p^2c + q^2a - pqb$.
- Si $P = aX^2 + bX + c$ et $Q = pX^2 + qX + r$, alors $R(P,Q) = (ar - cp)^2 - (aq - bp)(br - cq)$.

Exercice. Soit $a \in K$ un paramètre quelconque. Montrer qu'il existe au plus 7 valeurs de a pour lesquelles les polynômes $P = X^4 + X^3 + X + a + 1$ et $Q = aX^3 + X + a$ ont une racine commune. (Indication : vérifier que $R(P,Q) = a^7 + 2a^4 + 3a^3 + a^2 + a + 1$.)

4.2 - Application : notion de discriminant d'un polynôme

Définition. Soit K un corps algébriquement clos. On appelle *discriminant* d'un polynôme P de degré au moins égal à 2 dans $K[X]$ le résultant de P et de son polynôme dérivé P'. On note :

$$\Delta(P) = R(P, P').$$

On peut appliquer alors les résultats du paragraphe précédent.

Théorème. Soit K un corps algébriquement clos. Soient P un polynôme de degré au moins égal à 2 dans $K[X]$ et P' son polynôme dérivé. Alors le polynôme P a au moins une racine multiple dans K si et seulement si $\Delta(P) = 0$.

Preuve. D'après la première proposition de 2.3, P admet une racine multiple si et seulement si P et P' admettent une racine commune, d'où le résultat d'après le théorème de 4.1. □

On formule souvent ce résultat sous la forme :

Corollaire. Soit K un corps algébriquement clos. Un polynôme P de degré au moins égal à 2 dans $K[X]$ n'admet que des racines simples dans K si et seulement si son discriminant est non-nul.

Exemple 1. Dans $\mathbb{C}[X]$, considérons $P(X) = aX^2 + bX + c$, avec $a \neq 0$. On a $P'(X) = 2aX + b$, et donc :

$$\Delta(P) = R(P, P') = \begin{vmatrix} a & 2a & 0 \\ b & b & 2a \\ c & 0 & b \end{vmatrix} = a(4ac - b^2).$$

L'application du corollaire ci-dessus montre que P n'a que des racines simples si et seulement si $b^2 - 4ac \neq 0$, résultat bien connu !

Exemple 2. Dans $\mathbb{C}[X]$, considérons $P(X) = X^3 + pX + q$. On a $P'(X) = 3X^2 + p$, et donc :

$$\Delta(P) = R(P, P') = \begin{vmatrix} 1 & 0 & 3 & 0 & 0 \\ 0 & 1 & 0 & 3 & 0 \\ p & 0 & p & 0 & 3 \\ q & p & 0 & p & 0 \\ 0 & q & 0 & 0 & p \end{vmatrix} = 4p^3 + 27q^2.$$

Supposons que $\Delta(P) = 0$, et notons α la racine multiple de P dans K (elle est forcément unique puisque P est de degré 3). Comme α est alors aussi racine de P', on a $\alpha^2 = -\frac{p}{3}$.

Si $p = 0$, alors la nullité de $\Delta(P) = 4p^3 + 27q^2$ implique que l'on a aussi $q = 0$, donc $P(X) = X^3$, qui admet 0 comme racine triple.

Si $p \neq 0$, alors la nullité de $\Delta(P) = 4p^3 + 27q^2$ implique que l'on a $p = -\frac{27q^2}{4p^2}$, d'où $\alpha^2 = -\frac{p}{3} = \frac{9q^2}{4p^2}$. On vérifie que seul $\alpha = -\frac{3q}{2p}$ est racine de P, et c'est une racine double.

4.3 - Expression du résultant et du discriminant en fonction des racines

Théorème. Soit K un corps algébriquement clos. Soient P et Q deux polynômes non-nuls dans $K[X]$ de degrés respectifs $m \geq 1$ et $n \geq 1$. Notons :

$$P = \sum_{i=0}^{m} a_i X^i = a_m \prod_{j=1}^{m} (X - \alpha_j) \quad \text{et} \quad Q = \sum_{i=0}^{n} b_i X^i = b_n \prod_{j=1}^{n} (X - \beta_j).$$

Alors le résultant est donné par : $R(P, Q) = a_m^n b_n^m \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (\alpha_i - \beta_j)$.

Preuve. Les a_i pour $1 \leq i \leq m$ et les b_j pour $1 \leq j \leq n$ sont les coefficients dans K de P et Q respectivement, avec donc $a_m \neq 0$ et $b_n \neq 0$. Les α_i pour $1 \leq i \leq m$ et les β_j pour $1 \leq j \leq n$ sont les racines dans K de P et Q respectivement, comptées avec leur ordre de multiplicité. On raisonne en plusieurs étapes.

Première étape. Soient P_1 et Q_1 les polynômes unitaires dans $K[X]$ définis par $P = a_m P_1$ et $Q = b_n Q_1$. On a :

$$P_1 = \prod_{j=1}^{m}(X - \alpha_j) \qquad \text{et} \qquad Q_1 = \prod_{j=1}^{n}(X - \beta_j).$$

Notons $\sigma_1, \ldots, \sigma_m$ les fonctions symétriques élémentaires en les racines $\alpha_1, \ldots, \alpha_m$ de P, et $\sigma'_1, \ldots, \sigma'_n$ les fonctions symétriques élémentaires en les racines $\beta_1, \ldots, \beta_n$ de Q. D'après 3.2, on a :

$$\sigma_1 = -\frac{a_{m-1}}{a_m}, \quad \cdots \quad \sigma_m = (-1)^m \frac{a_0}{a_m}, \quad \sigma'_1 = -\frac{b_{n-1}}{b_n}, \quad \cdots \quad \sigma'_n = (-1)^n \frac{b_0}{b_n},$$

et donc :
$$P_1 = X^m - \sigma_1 X^{m-1} + \sigma_2 X^{m-2} - \ldots + (-1)^{m-1}\sigma_{m-1} X + (-1)^m \sigma_m,$$
$$Q_1 = X^n - \sigma'_1 X^{n-1} + \sigma'_2 X^{n-2} - \ldots + (-1)^{n-1}\sigma'_{n-1} X + (-1)^n \sigma'_n.$$

Deuxième étape. Reprenons les expressions développées $P = \sum_{i=0}^{m} a_i X^i$ et $Q = \sum_{i=0}^{n} b_i X^i$.
L'expression de $R(P, Q)$ vu en 4.3 permet de voir $R(P, Q)$ comme un polynôme en les $n + m + 2$ indéterminées $a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n$. Plus précisément, la forme du déterminant permet d'observer que ce polynôme est homogène de degré n en les indéterminées $a_0, a_1, \ldots, a_m$ et homogène de degré m en les indéterminées $b_0, b_1, \ldots, b_n$. Dans l'anneau $K[a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n]$, notons :

$$R(P, Q) = F(a_0, a_1, \ldots, a_m, b_0, b_1, \ldots, b_n).$$

D'après les observations précédentes :

$$R(P, Q) = a_m^n b_n^m F(\tfrac{a_0}{a_m}, \tfrac{a_1}{a_m}, \ldots, \tfrac{a_{m-1}}{a_m}, 1, \tfrac{b_0}{b_n}, \tfrac{b_1}{b_n}, \ldots, \tfrac{b_{n-1}}{b_n}, 1).$$

Cette relation appliquée aux polynômes P_1 et Q_1 développés comme à la fin de la première étape s'écrit :

$$R(P_1, Q_1) = F\big((-1)^m \sigma_m, (-1)^{m-1}\sigma_{m-1}, \ldots, -\sigma_1, 1, (-1)^n \sigma'_n, (-1)^{n-1}\sigma'_{n-1}, \ldots, -\sigma'_1, 1\big).$$

On en déduit d'abord que $R(P_1, Q_1)$ est un polynôme symétrique en $\alpha_1, \alpha_2, \ldots, \alpha_m$ d'une part, et en $\beta_1, \beta_2, \ldots, \beta_n$ d'autre part.

On en déduit ensuite que $R(P, Q) = a_m^n b_n^m R(P_1, Q_1)$, d'où $R(P_1, Q_1) = 0$ si et seulement si $R(P, Q) = 0$, c'est-à-dire d'après le théorème de 4.1 si et seulement s'il existe un couple (i, j) avec $1 \leq i \leq m$ et $1 \leq j \leq n$ tel que $\alpha_i = \beta_j$.

Ces deux remarques impliquent que, dans $K[\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n]$, le polynôme $R(P_1, Q_1)$ est divisible par $(\alpha_i - \beta_j)$ pour tous $1 \leq i \leq m$ et $1 \leq j \leq n$, donc par le produit $\prod_{1 \leq i \leq m, 1 \leq j \leq n}(\alpha_i - \beta_j)$.

En notant S ce produit et en comparant pour chacun des polynômes $R(P_1, Q_1)$ et S les degrés en $\alpha_1, \alpha_2, \ldots, \alpha_m$ et en $\beta_1, \beta_2, \ldots, \beta_n$, ainsi que le coefficient de $(\alpha_1 \alpha_2 \cdots \alpha_m)^n$, on en tire que $R(P_1, Q_1) = S$. On conclut $R(P, Q) = a_m^n b_n^m S$, ce qui achève la preuve. □

REMARQUE. On a donc les expressions suivantes du résultant :

$$R(P, Q) = a_m^n b_m^n \prod_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} (\alpha_i - \beta_j) = a_m^n \prod_{1 \leq i \leq m} Q(\alpha_i) = (-1)^{mn} b_n^m \prod_{1 \leq j \leq n} P(\beta_j).$$

qui rendent explicite la conclusion du théorème de 4.1

Corollaire Soit K un corps algébriquement clos. Soit $P = a_n X^n + \cdots + a_1 X + a_0$ un polynôme de degré $n \geq 2$ dans $K[X]$. Soient $\alpha_1, \ldots, \alpha_n$ les racines de P dans K. Alors le discriminant de P est donné par :

$$\Delta(P) = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-1} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

Preuve. On a : $P(X) = a_n \prod_{1\leq k\leq n}(X-\alpha_k)$, donc : $P'(X) = a_n \sum_{1\leq j\leq n}\Big(\prod_{1\leq k\leq n, k\neq j}(X-\alpha_k)\Big)$
d'où, pour tout $1 \leq i \leq n$, l'égalité :

$$P'(\alpha_i) = a_n(\alpha_i-\alpha_1)(\alpha_i-\alpha_2)\dots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\dots(\alpha_i-\alpha_n).$$

On calcule alors en utilisant les expressions de la remarque ci-dessus :

$$\begin{aligned}
\Delta(P) = R(P,P') &= a_n^{n-1}\prod_{1\leq i\leq n} P'(\alpha_i)\\
&= a_n^{n-1}\prod_{1\leq i\leq n} a_n(\alpha_i-\alpha_1)(\alpha_i-\alpha_2)\dots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\dots(\alpha_i-\alpha_n)\\
&= a_n^{2n-1}\prod_{1\leq i\leq n} (\alpha_i-\alpha_1)(\alpha_i-\alpha_2)\dots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\dots(\alpha_i-\alpha_n)\\
&= a_n^{2n-1}\prod_{1\leq i\leq n} (-1)^{i-1}(\alpha_1-\alpha_i)(\alpha_2-\alpha_i)\dots(\alpha_{i-1}-\alpha_i)(\alpha_i-\alpha_{i+1})\dots(\alpha_i-\alpha_n)\\
&= a_n^{2n-1}(-1)^{n(n-1)/2}\prod_{1\leq i<j\leq n}(\alpha_i-\alpha_j)^2. \qquad \square
\end{aligned}$$

Fractions rationnelles

1. Corps des fractions d'un anneau commutatif unitaire intègre

Il existe bien sûr des anneaux intègres qui ne sont pas des corps. Le but de ce qui suit est de montrer que, néanmoins, on peut construire de façon canonique pour tout anneau commutatif untaire intègre A un corps K qui le contient, et qui est (en un sens que l'on précisera) le plus petit corps qui le contient. Puisque tout corps est un anneau intègre et que tout sous-anneau d'un anneau intègre est intègre, la question n'a de sens qu'en partant d'un anneau A intègre.

1.1 - Construction

▶ *Données.*

Fixons A un anneau commutatif unitaire intègre. Posons $A^* = A \setminus \{0\}$. On définit dans $A \times A^*$ la relation $\sim$ par : $(a,b) \sim (c,d) \;\Leftrightarrow\; ad = bc$.

▶ Etape 1. – *la relation $\sim$ est une relation d'équivalence dans $A \times A^*$.*

Preuve. La réflexivité et la symétrie sont évidentes. Pour la transitivité, considérons trois couples (a,b), (c,d) et (e,f) dans $A \times A^*$. Supposons que $(a,b) \sim (c,d)$ et $(c,d) \sim (e,f)$. On a donc : $ad = bc$ et $cf = de$. Il vient $adf = bcf = bde$, et comme $d \neq 0$, l'intégrité de A implique $af = be$, d'où $(a,b) \sim (e,f)$. □

Pour tout couple $(a,b) \in A \times A^*$, on note $\frac{a}{b}$ la classe d'équivalence de (a,b) pour la relation $\sim$:

$$\tfrac{a}{b} = \{(c,d) \in A \times A^* \,;\, (c,d) \sim (a,b)\} = \{(c,d) \in A \times A^* \,;\, ad = bc\}.$$

Une telle classe s'appelle une fraction. On note $K = (A \times A^*)/\sim$ l'ensemble quotient de $A \times A^*$ par la relation $\sim$, c'est-à-dire l'ensemble des fractions. Tout couple (c,d) appartenant à $\frac{a}{b}$ s'appelle un représentant de la fraction $\frac{a}{b}$. En résumé :

$$(\ \tfrac{a}{b} = \tfrac{c}{d} \text{ dans } K\ ) \;\Leftrightarrow\; (\ (a,b) \sim (c,d) \text{ dans } A \times A^*\ ) \;\Leftrightarrow\; (\ ad = bc \text{ dans } A\ ).$$

▶ Etape 2. – *L'application $\phi : A \to K$ qui, à un élément $a \in A$ associe la fraction $\phi(a) = \frac{a}{1}$, est injective, et est appelée injection canonique de A dans K.*

Preuve. Soient $a, c \in A$ tels que $\phi(a) = \phi(c)$. Alors $\frac{a}{1} = \frac{c}{1}$, d'où $a.1 = 1.c$, donc $a = c$. □

On convient d'identifier A avec le sous-ensemble $\phi(A)$ de K, qui lui est équipotent. Via cette identification, A est un sous-ensemble de K, et on pose $a = \frac{a}{1}$, pour tout $a \in A$. Donc :

$$\text{quel que soit } a \in A, \text{ on a : } \; a = \tfrac{a}{1} = \{(c,d) \in A \times A^* \,;\, c = ad\} = \tfrac{ad}{d} \;\text{ pour tout } d \in A^*.$$

En particulier : $0 = \frac{0}{1} = \frac{0}{b}$ pour tout $b \in A^*$ et $1 = \frac{1}{1} = \frac{b}{b}$ pour tout $b \in A^*$.

▶ Etape 3. – *Les lois de composition internes dans K définies par :*

$$\tfrac{a}{b} + \tfrac{c}{d} = \tfrac{ad+bc}{bd} \qquad \text{et} \qquad \tfrac{a}{b} \times \tfrac{c}{d} = \tfrac{ac}{bd}$$

sont bien définies (indépendamment des représentants choisis), munissent K d'une structure d'anneau commutatif unitaire, et prolongent celles de A (ce qui signifie que l'injection canonique est un morphisme d'anneaux unitaires, ou encore que A peut être considéré, en l'identifiant avec son image par ϕ, comme un sous-anneau unitaire de K).

Preuve. Supposons que $\frac{a}{b} = \frac{a'}{b'}$ et $\frac{c}{d} = \frac{c'}{d'}$. Un calcul évident montre que $ab' = a'b$ et $cd' = c'd$ impliquent d'une part $(ad + bc)b'd' = (a'd' + b'c')bd$, et donc $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$, et d'autre part $(ac)(b'd') = (a'c')(bd)$, et donc $\frac{ac}{bd} = \frac{a'c'}{b'd'}$. Ceci prouve que les deux lois sont bien définies. Qu'elles satisfont alors tous les axiomes de la structure d'anneau commutatif unitaire (avec $0 = \frac{0}{1}$ pour neutre additif et $1 = \frac{1}{1}$ pour neutre multiplicatif) est une simple vérification laissée au lecteur. Enfin quels que soient deux éléments $a, c \in A$, on a : $\phi(a + c) = \frac{a+c}{1} = \frac{a}{1} + \frac{c}{1} = \phi(a) + \phi(c)$ et $\phi(ac) = \frac{ac}{1} = \frac{a}{1}.\frac{c}{1} = \phi(a).\phi(c)$, ce qui achève la preuve. □

► Etape 4. – *Tout élément non nul de K est inversible dans K. Plus précisément, tout élément $\frac{a}{b} \in K$ avec $(a, b) \in A^* \times A^*$ admet $\frac{b}{a}$ pour inverse.*

Preuve. Evident puisque $\frac{a}{b}.\frac{b}{a} = \frac{ab}{ba} = 1$. □

En particulier, tout élément non nul $a \in A$ admet dans K l'inverse $\frac{1}{a}$.

1.2 - Conclusion

On a démontré par cette construction et les vérifications faites aux différentes étapes :

Théorème. Soit A un anneau commutatif unitaire intègre.
L'ensemble $K = (A \times A^*)/\sim$ des fractions sur A, muni des lois construites ci-dessus, est un corps commutatif, qui contient A comme sous-anneau unitaire.

1.3 - Caractère canonique et minimal de la construction

La proposition suivante explicite le caractère minimal du corps de fractions.

Proposition. Soit A un anneau commutatif unitaire intègre. Soit K son corps de fractions.

(i) Si K' est un sous-corps de K tel que A est un sous-anneau de K', alors $K' = K$.

(ii) Si L est un corps tel que A est un sous-anneau de L, alors il existe dans L un sous-corps K' isomorphe à K, ce qui permet par identification de considérer K comme un sous-corps de L.

Preuve. Pour (i), on a $A \subseteq K' \subseteq K$ avec K' un corps. Soit $x \in K$. Par définition, il existe $a \in A$ et $b \in A^*$ tel que $x = \frac{a}{b} = a.\frac{1}{b}$. On a $b \in A$ donc $b \in K'$, avec $b \neq 0$; comme l'inverse de b dans K est $\frac{1}{b} \in K$, et que cet inverse doit appartenir à K' puisque K' est un sous-corps, on a $\frac{1}{b} \in K'$. Par ailleurs $a \in A$ donc $a \in K'$. Le sous-corps K' est stable par produit, donc $a.\frac{1}{b} \in K'$, c'est-à-dire $\frac{a}{b} = x \in K'$. Cela prouve que $K \subseteq K'$, donc $K = K'$.

Pour (ii), on a $A \subseteq L$ avec L un corps. Considérons l'application $j : K \to L$ qui à toute fraction $\frac{a}{b} \in K$ associe ab^{-1}, c'est-à-dire le produit dans L de a (qui est un élément de A donc de L) et de l'inverse de b (car b est un élément non-nul de A donc inversible dans L). Il est immédiat de vérifier que j est bien défini, que c'est un morphisme d'anneaux unitaires, et que j est injective. Par ce plongement, on identifie K au sous-corps $j(K)$ de L. □

1.4 - Exemples

- ► Le corps de fractions de l'anneau intègre $\mathbb{Z}$ est appelé *corps des rationnels* et est noté $\mathbb{Q}$.
- ► On considère dans $\mathbb{C}$ le sous-anneau $A = \mathbb{Z}[i] = \{a + bi\,;\, a \in \mathbb{Z}, b \in \mathbb{Z}\}$ des entiers de Gauss. Le sous-ensemble $\mathbb{Q}(i) = \{p + qi\,;\, p \in \mathbb{Q}, q \in \mathbb{Q}\}$ de $\mathbb{C}$ est un sous-corps de $\mathbb{C}$ isomorphe au corps des fractions de A.

2. Corps de fractions rationnelles

2.1 - Notion de fraction rationnelle

Lemme. Soient A un anneau commutatif unitaire et $A[X]$ l'anneau des polynômes en une indéterminée à coefficients dans A. Si A est intègre, alors $A[X]$ est intègre.

Preuve. Soient P, Q deux polynômes non-nuls de $A[X]$, de degrés respectifs $n, m \in \mathbb{N}$. Notons $P = \sum_{i=0}^{n} a_i X^i$ et $Q = \sum_{i=0}^{m} b_i X^i$ avec $a_i, b_i \in A, a_n \neq 0, b_m \neq 0$. On a alors $PQ = a_n b_m X^{n+m} + \cdots$. L'intégrité de A implique que $a_n b_m \neq 0$ dans A, donc $PQ \neq 0$ dans $A[X]$. □

En particulier, si K est un corps, alors l'anneau $K[X]$ est intègre. D'où la définition suivante.

Définition. Pour tout corps K, le corps de fractions de l'anneau intègre $K[X]$ est appelé *corps des fractions rationnelles à coefficients dans* K, noté $K(X)$. Ses éléments sont de la forme :

$$F = \frac{P}{Q} \quad \text{où } (P, Q) \in K[X] \times K[X] \text{ avec } Q \neq 0 \text{ est un représentant de } F.$$

Considérer les corps de fractions rationnelles à coefficients dans un corps est suffisant pour rendre compte des corps de fractions des anneaux de polynômes à coefficients dans un anneau intègre.

Proposition Soit A un anneau commutatif unitaire intègre. Soit K le corps de fractions de A. Alors le corps de fractions de l'anneau intègre $A[X]$ est égal à $K(X)$. Ses éléments sont de la forme :

$$F = \frac{P}{Q} \quad \text{avec } P, Q \in A[X],\ Q \neq 0.$$

Preuve. Comme A est un sous-anneau de K, l'anneau $A[X]$ est un sous-anneau de $K[X]$, donc un sous-anneau du corps $K(X)$. D'après le point (ii) de la proposition 1.3, le corps de fractions F de $A[X]$ est un sous-corps de $K(X)$. Puisque que $A \subset A[X]$, on a $K \subset F$, et comme par ailleurs $A[X] \subset F$, on en déduit que $K[X] \subset F$. Finalement $K[X] \subset F \subset K(X)$, et comme $K(X)$ est le corps de fractions de $K[X]$, on conclut avec le point (i) de la proposition 1.3 que $F = K(X)$. □

► *Exemple.* Le corps de fractions de $\mathbb{Z}[X]$ est $\mathbb{Q}(X)$.

► *Remarque : cas de plusieurs variables.* En utilisant l'isomorphisme canonique $K[X_1, X_2] \simeq K[X_1][X_2]$, il résulte du lemme ci-dessus que $K[X_1, X_2]$ est intègre ; on peut donc considérer son corps de fractions $K(X_1, X_2) \simeq K(X_1)(X_2)$ et, par une itération évidente, le corps de fractions rationnelles $K(X_1, \ldots, X_n)$ en un nombre fini quelconque n d'indéterminés.

2.2 - Dérivée d'une fraction rationnelle

Proposition et définition. Soit K un corps.

(i) Pour toute fraction rationnelle $F = \frac{P}{Q} \in K(X)$ avec $P, Q \in K[X], Q \neq 0$, la fraction rationnelle $F' = \frac{P'Q - PQ'}{Q^2}$ est indépendante du couple de représentants (P, Q) choisi. On l'appelle la *fraction rationnelle dérivée* de F.

(ii) L'application $F \mapsto F'$ est un endomorphisme de K-espace vectoriel de $K(X)$ vérifiant de plus $(FG)' = F'G + FG'$ pour toutes $F, G \in K(X)$.

Preuve. Vérification évidente. □

2.3 - Formes irréductibles, zéros et pôles d'une fraction rationnelle

Proposition et définition Soit K un corps.

Pour toute $F \in K(X)$, on appelle *représentant irréductible* de F tout couple de polynômes $P, Q \in K[X]$ avec $Q \neq 0$ tels que $F = \frac{P}{Q}$ avec P et Q sont premiers entre eux. On dit aussi dans ce cas que $F = \frac{P}{Q}$ est *sous forme réduite.*

Pour toute $F \in K(X)$, il existe un unique représentant irréductible P, Q tel que Q est unitaire.

Preuve. Soit $F = \frac{A}{B} \in K(X)$ avec $A, B \in K[X], B \neq 0$. Parce que K est un corps, l'anneau $K[X]$ est principal. On peut donc considérer un pgcd $D \in K[X]$ de A et B ; rappelons que D n'est pas défini de façon unique, mais au produit près par un élément de K^*. On a $A = DP$ et $B = DQ$ avec P et Q premiers entre eux. Donc $F = \frac{P}{Q}$, et le couple P, Q est un représentant irréductible de F.

Désignons par $c \in K^*$ le coefficient dominant de Q et notons $Q_1 = \frac{1}{c}Q$, qui est unitaire dans $K[X]$. Si l'on pose $P_1 = \frac{1}{c}P$, on a $F = \frac{P}{Q} = \frac{P_1}{Q_1}$, avec toujours P_1 et Q_1 premier entre eux. La preuve de l'unicité est évidente et laissée au lecteur. □

Définition Soit K un corps. Soit $F = \frac{P}{Q} \in K(X)$ supposée écrite sous forme irréductible.

On appelle *zéro* de F dans K tout zéro dans K du polynôme $P \in K[X]$.

On appelle *pôle* de F dans K tout zéro dans K du polynôme non-nul $Q \in K[X]$.

▶ *Remarques.*

1. Ces notions ne sont définies qu'en partant d'une forme irréductible de F, et dépendent du corps K où on les considère.

   Exemple. Considérons $F(X) = \frac{X^3-1}{X^2-1} \in \mathbb{R}(X)$. Sous cette forme, les zéros réels du dénominateur sont 1 et -1. Mais il faut réécrire F sous forme irréductibe $F(X) = \frac{X^2+X+1}{X+1}$ pour conclure que F admet -1 comme unique pôle dans $\mathbb{R}$ et n'admet pas de zéros dans $\mathbb{R}$. Pour la même fraction vue dans $\mathbb{C}(X)$, on a toujours -1 comme unique pôle dans $\mathbb{C}$, mais on a aussi deux zéros j et j^2 dans $\mathbb{C}$.

2. L'ordre d'un zéro (respectivement d'un pôle) de F est naturellement défini comme son ordre en tant que zéro de P (respectivement de Q).

3. Soit $F \in K(X)$ une fraction rationnelle. Comme le polynôme Q n'a qu'un nombre fini de zéros dans K, la fraction n'a qu'un nombre fini de pôles. Notons D l'ensemble K privé de l'ensemble fini des pôles de F. Pour tout élément $x \in K$, on peut considérer par évaluation des polynômes P et Q en x les éléments $P(x) \in K$ et $Q(x) \in K^*$. D'où l'application :
   $$\widetilde{F} : D \to K, \quad x \mapsto \widetilde{F}(x) = \frac{P(x)}{Q(x)}.$$
   On appelle $\widetilde{F}$ la *fonction rationnelle* associée à F, et l'on note généralement $\widetilde{F} = F$.
   On montre facilement (la preuve est laissé en exercice au lecteur) que, lorsque le corps K n'est pas fini, deux fractions rationnelles sont égales si et seulement leur fonctions rationelles associées coïncident en tout $x \in K$ qui n'est un pôle ni de l'une ni de l'autre.

2.5 - Degré d'une fraction rationnelle

Définition Soit K un corps. Soit $F = \frac{P}{Q} \in K(X)$ non-nulle supposée écrite sous forme irréductible. On appelle *degré* de F l'entier relatif $\deg F = \deg P - \deg Q \in \mathbb{Z}$.

— On pose par convention $\deg F = -\infty$ lorsque $F = 0$, et l'on obtient les propriétés usuelles : $\deg(F+G) \leq \max(\deg F, \deg G)$ et $\deg(FG) = \deg F + \deg G$ pour toutes $F, G \in K(X)$.
— Attention : $\deg F \geq 0$ ne signifie pas que F est un polynôme (par exemple $F(X) = \frac{X^2}{X+1}$).
— En utilisant 2.2, calculer à titre d'exercice $\deg F'$ en fonction de $\deg F$ pour toute $F \in K(X)$.

3. Décomposition en éléments simples

3.1 - Principe général

▶ *Partie entière*

Lemme et définition. Soit K un corps. Toute fraction rationnelle $F \in K(X)$ s'écrit de façon unique sous la forme $F = E + S$ où E est un polynôme de $K[X]$ et S est une fraction rationnelle dans $K(X)$ vérifiant $\deg S < 0$. Le polynôme E est appelé la *partie entière* de F.

Preuve. Comme K est un corps, l'anneau $K[X]$ est euclidien. En effectuant la division euclidienne de P par Q, il existe deux polynômes $E, R \in K[X]$ telle que $P = QE + R$ avec $\deg R < \deg Q$, d'où $F = \frac{P}{Q} = E + \frac{R}{Q}$ avec $S := \frac{R}{Q} \in K(X)$ de degré strictement négatif, ce qui montre l'existence de la décomposition. Pour l'unicité, supposons que $F = E_1 + S_1 = E_2 + S_2$ avec $E_1, E_2 \in K[X]$ et $S_1, S_2 \in K(X)$ de degrés strictement négatifs. On a alors $E_1 - E_2 = S_2 - S_1$ avec $E_1 - E_2$ un polynôme et $S_2 - S_1$ une fraction de degré strictement négatif, ce qui n'est possible que si $E_1 = E_2$ et $S_1 = S_2$. □

▶ *Le théorème fondamental*

Théorème. Soit K un corps. Toute fraction rationnelle $F \in K(X)$ s'écrit de façon unique sous la forme :

$$F = E + S_1 + S_2 + \cdots + S_p$$

avec $E \in K[X]$ la partie entière de F et, pour tout $1 \leq i \leq p$, $S_i \in K(X)$ de la forme :

$$S_i = \sum_{k=1}^{n_i} \frac{P_{i,k}}{Q_i^k}$$

où les Q_i sont des polynômes irréductibles dans $K[X]$ deux à deux non associés, les n_i sont des entiers naturels non-nuls, et les $P_{i,k}$ sont des polynômes dans $K[X]$ vérifiant :

$$\deg P_{i,k} < \deg Q_i \quad \text{pour tout } 1 \leq i \leq p \text{ et tout } 1 \leq k \leq n_i.$$

Cette écriture unique s'appelle la décomposition en éléments simples de F.

Dans cette écriture, les polynômes $Q_1, Q_2, \ldots, Q_p$ sont les facteurs distincts de la décomposition en polynômes irréductibles dans $K[X]$ du dénominateur de F écrite sous forme réduite, et l'entier n_i est la plus grand puissance avec laquelle Q_i intervient dans cette décomposition.

Nous ne reprenons pas ici la preuve de ce théorème, qui est classique et figure dans tous les ouvrages d'algèbre élémentaire.

3.2 - Mise en œuvre sur $\mathbb{C}$ et $\mathbb{R}$

Les polynômes irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1, et les polynômes irréductibles de $\mathbb{R}[X]$ sont les polynômes de degré 1 et ceux de degré 2 dont le discriminant est strictement négatif ; on en déduit immédiatement la forme de la décomposition en éléments simples dans $\mathbb{C}(X)$ et dans $\mathbb{R}(X)$.

Corollaire 1. Toute fraction rationnelle $F \in \mathbb{C}(X)$ s'écrit de façon unique sous la forme :

$$F = E + \sum_{i=1}^{p} \sum_{k=1}^{n_i} \frac{\lambda_{i,k}}{(X-a_i)^k}$$

où :
$E \in \mathbb{C}[X]$ est la partie entière de F,
$a_1, \ldots, a_p \in \mathbb{C}$ sont les pôles deux à deux distincts de F d'ordres respectifs $n_1, \ldots, n_p$,
les coefficients $\lambda_{i,k}$ appartiennent à $\mathbb{C}$.

Corollaire 2. Toute fraction rationnelle $F \in \mathbb{R}(X)$ s'écrit de façon unique sous la forme :

$$F = E + \sum_{i=1}^{p} \sum_{k=1}^{n_i} \frac{\lambda_{i,k}}{(X-a_i)^k} + \sum_{i=1}^{q} \sum_{k=1}^{m_i} \frac{\alpha_{i,k}X+\beta_{i,k}}{(X^2+b_iX+c_i)^k}$$

où :
$E \in \mathbb{R}[X]$ est la partie entière de F,
$a_1, \ldots, a_p \in \mathbb{R}$ sont les pôles de F deux à deux disctincts d'ordres respectifs $n_1, \ldots, n_p$,
les coefficients $\lambda_{i,k}$ appartiennent à $\mathbb{R}$,
les polynômes $X^2 + b_iX + c_i$ pour $1 \leq i \leq q$ sont les diviseurs irréductibles de degré 2 du dénominateur de la forme réduite de F,
les coefficients $\alpha_{i,k}, \beta_{i,k}$ appartiennent à $\mathbb{R}$.

Les méthodes classiques de calcul des coefficients figurent dans la plupart des livres usuels ; on ne les reprend pas ici.

3.3 - Quelques applications usuelles

▶ *Calcul des primitives des fonctions rationnelles réelles.*

La décomposition en éléments simples dans $R(X)$ permet par linéarité de ramener le calcul des primitives de toute fonction rationnelle réelle au calcul des primitives des fonctions rationnelles du type correspondant aux deux types déléments simples $\frac{\lambda}{(X-a)^k}$ ou $\frac{\alpha X+\beta}{(X^2+bX+c)^k}$, pour lesquels des méthodes d'intégration adhoc peuvent être mises en œuvre. C'est une des applications majeures de la décomposition, mais là encore, nous renvoyons aux livres d'enseignement classiques.

▶ *Calcul de sommes de séries "téléscopiques".*

Exemple : la série $\sum_{n=1}^{+\infty} \frac{1}{n(n+1)(n+2)}$ est convergente (équivalente à la série de Riemann de terme général $\frac{1}{n^3}$. Pour calculer sa somme, on introduit la décomposition en éléments simples du terme général $F(n) = \frac{1}{n(n+1)(n+2)} = \frac{1}{2n} - \frac{1}{(n+1)} + \frac{1}{2(n+2)}$ donc $2F(n) = (\frac{1}{n} - \frac{1}{n+1}) - (\frac{1}{n+1} - \frac{1}{n+2})$. D'où $2\sum_{n=1}^{N} F(n) = (1 - \frac{1}{2}) - (\frac{1}{N+1} - \frac{1}{N+2})$, puis $\sum_{n=1}^{+\infty} F(n) = \frac{1}{4}$.

4. Divers prolongements et développements

4.1 - Développement en série entières d'une fonction rationnelle complexe

On considère ici une fraction rationnelle $F \in \mathbb{C}(X)$ et l'on note f la fonction d'une variable complexe à valeurs complexes associée (au sens de 2.3.3) ; une telle fonction est appelée une fonction rationnelle complexe.

Proposition. Toute fonction rationnelle complexe f n'admettant pas 0 pour pôle est développable en série entière au voisinage de 0, et le rayon de convergence de cette série entière est égal au minimum des modules des pôles de f.

Preuve. La décomposition en éléments simples de la fraction rationnelle $F \in \mathbb{C}(X)$ associée est de la forme :

$$F(X) = E(X) + \sum_{i=1}^{p} \sum_{k=1}^{n_i} \frac{\lambda_{i,k}}{(X-z_i)^k} \quad \text{avec } z_i, \lambda_{i,k} \in \mathbb{C}.$$

Par hypothèse $z_i \neq 0$ pour tout $1 \leq i \leq p$. Pour tout $1 \leq i \leq p$, $1 \leq k \leq n_i$ et $z \in \mathbb{C}$, on a :

$$f_{i,k}(z) := \frac{\lambda_{i,k}}{(z-z_i)^k} = \frac{\lambda_{i,k}}{(-z_i)^k} \left(1 - \frac{z}{z_i}\right)^{-k}.$$

Il est clair alors, puisque $|z| < |z_i|$ équivaut à $|\frac{z}{z_i}| < 1$, que $f_{k,i}$ est développable en série entière sur $D(0, |z_i|)$, et que le rayon de convergence correspondant est égal à $|z_i|$. Il en résulte pour la somme des $f_{i,k}$, en notant $\rho = \min\{z_1, \ldots, z_p\}$, que f est développable en série entière sur $D(0, \rho)$, et que le rayon de convergence correspondant est égal à ρ. □

4.2 - Fonction rationnelle réelle à valeurs entières

• Rappelons d'abord que l'on sait caractériser les polynômes $P \in \mathbb{R}[X]$ tels que $P(n) \in \mathbb{Z}$ pour tout $n \in \mathbb{Z}$. Ce sont les polynômes de la forme $\sum_{i=0}^{n} a_i H_i$ avec $a_i \in \mathbb{Z}$, où H_i désigne pour tout $i \in \mathbb{N}$ le polynôme de Hermite $H_i = \frac{1}{i!} X(X-1)\cdots(X-i+1)$ de degré i, avec $H_0 = 1$. Ces polynômes vérifient : $H_{i+1}(X+1) = H_{i+1}(X) + H_i(X)$, avec $H_i(0) = 0$. Il est clair que $H_i(n) = \binom{n}{i} \in \mathbb{N}$ pour tout $n \in \mathbb{N}$, d'où $H_i(n) \in \mathbb{Z}$ pour tout $n \in \mathbb{Z}$. La famille $(H_i)_{i \geq 0}$ est une famille étagée qui constitue donc une base de $\mathbb{R}[X]$, et l'on montre par récurrence sur le degré que, parmi les combinaisons linéaires réelles des H_i, celles dont les coefficients sont des entiers sont exactement les polynômes qui ne prennent que des valeurs entières sur $\mathbb{Z}$.

• On considère ici une fraction rationnelle $F \in \mathbb{R}(X)$ et l'on note f la fonction réelle d'une variable réelle associée ; une telle fonction est appelée une fonction rationnelle réelle.

Proposition. Toute fonction rationnelle réelle qui ne prend que des valeurs entières sur $\mathbb{Z}$ est une fonction polynomiale.

Preuve. On raisonne par récurrence sur le degré de la partie entière de F (voir 3.1).
Supposons d'abord que la partie entière de F est de degré nul. On a donc $F = c + S$ avec $c \in \mathbb{R}$ et $S \in \mathbb{R}(X)$ tel que $\deg S < 0$. La fonction rationnelle réelle s associée à S vérifie $\lim_{n\to\infty} s(n) = 0$, donc la suite $(f(n))_{n\geq 0}$ est une suite d'entiers qui converge dans $\mathbb{R}$ vers le réel c. Il en résulte que $c \in \mathbb{Z}$ et $f(n) = c$ pour n assez grand, donc $s(n) = 0$ pour tout entier n assez grand. Si s n'était pas identiquement nulle, elle n'admettrait qu'un nombre fini de zéros (ceux du numérateur d'une forme réduite de S), donc ici s est nécessairement la fonction nulle. On conclut que $F = c \in \mathbb{Z}$.

Supposons ensuite que la proposition soit vraie pour toute fraction rationnelle de partie entière de degré $\leq k$. Soit $F \in \mathbb{R}(X)$, décomposée suivant 3.1 en $F = E + S$, avec $E \in \mathbb{R}[X]$ tel que $\deg E \leq k+1$ et $S \in \mathbb{R}(X)$ telle que $\deg S < 0$. On considère la fraction rationnelle $G(X) = F(X+1) - F(X)$; comme F elle vérifie $G(n) \in \mathbb{Z}$ pour tout $n \in \mathbb{Z}$ et sa partie entière $E(X+1) - E(X)$ est de degré $\leq k$. On applique hypothèse de récurrence pour conclure que $F(X+1) - F(X)$ est un polynôme, et donc que $S(X) = S(X+1)$ dans $\mathbb{R}(X)$. En comparant l'ensemble fini des pôles complexes de $S(X)$ et de $S(X+1)$, on en déduit que $S = 0$, et donc que $F \in \mathbb{R}[X]$. □

4.3 - Décomposition en éléments simples de P'/P et théorème de Lucas

Proposition. Soient P un polynôme non constant de $\mathbb{C}[X]$, $r_1, \ldots, r_m$ ses zéros dans $\mathbb{C}$ et $\alpha_1, \ldots, \alpha_m$ leurs multiplicités respectives ; on a alors dans $\mathbb{C}(X)$ l'égalité :

$$\frac{P'(X)}{P(X)} = \sum_{j=1}^{m} \frac{\alpha_j}{X - r_j}.$$

Preuve. Notons $P(X) = a_n(X-r_1)^{\alpha_1}(X-r_2)^{\alpha_2}\cdots(X-r_m)^{\alpha_m}$. On calcule $P'(X) = \sum_{j=1}^{m} \frac{\alpha_j P(X)}{X-r_j}$, et le résultat voulu s'en déduit. □

Une conséquence classique mais intéressante de ce simple calcul est le théorème de Lucas qui établit que, si P est un polynôme de degré $n \geq 2$ dans $\mathbb{C}[X]$, l'ensemble des points du plan dont les affixes sont les zéros de P' est inclus dans l'enveloppe convexe de l'ensemble des points du plan dont les affixes sont les zéros de P (voir page 77 de ce document, dans la section consacrée aux racines d'un polynôme).

4.4 - Déterminant de Cauchy

Proposition. Soient $a_1, \ldots, a_n, b_1, \ldots, b_n$ des nombres complexes tels quel $a_i + b_j \neq 0$ pour tous $1 \leq i, j \leq n$. Le déterminant de la matrice :

$$A_n = \left(\frac{1}{a_i + b_j}\right)_{1 \leq i,j \leq n}$$

est égal à :

$$\det A_n = \frac{\displaystyle\prod_{1 \leq i < j \leq n} (a_j - a_i) \prod_{1 \leq i < j \leq n} (b_j - b_i)}{\displaystyle\prod_{1 \leq i,j \leq n} (a_i + b_j)}.$$

Preuve. C'est un calcul classique dont on trouvera le détail dans de nombreux ouvrages ; nous ne le reprenons pas ici. L'idée est que, si F est une fraction rationnelle admettant n pôles simples (à savoir $a_1, \ldots, a_n$) qui prend des valeurs données en n points distincts des a_i (à savoir $-b_1, \ldots, -b_n$), alors, dans la décomposition en éléments simples $F(X) = \sum_{i=1}^{n} \frac{\lambda_i}{X - a_i}$, les numérateurs $\lambda_1, \ldots, \lambda_n$ sont solutions d'un système de n équations à n inconnues dont le déterminant est le détermiant de Cauchy. □

4.5 - Automorphismes de $K(X)$

Théorème. Le groupe des K-automorphismes d'anneau de $K(X)$ est isomorphe au groupe linéaire projectif $\mathrm{PGL}(2, \mathbb{K})$.

Preuve. Notons $\mathrm{Aut}_K K(X)$ le groupe des K-automorphisme de $K(X)$ c'est-à-dire le groupe des automorphismes d'anneaux de $K(X)$ vérifiant $\sigma(a) = a$ pour tout $a \in K$. Tout $\sigma \in \mathrm{Aut}_K K(X)$ est entièrement

déterminé par la valeur de $\sigma(X)$. En particulier, pour toute matrice $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,K)$, on peut considérer $\sigma_M \in \mathrm{Aut}_K\, K(X)$ défini par $\sigma_M(X) = \frac{aX+b}{cX+d}$. On vérifie aisément que :

$$\Phi : \mathrm{GL}(2,K) \to \mathrm{Aut}_K\, K(X),\ M \mapsto \sigma_M$$

est un morphisme de groupes. Son noyau est le sous-groupe des matrices scalaires dans $\mathrm{GL}(2,K)$, que l'on identifie à K^*, de sorte que $\mathrm{Im}\,\Phi \simeq \mathrm{GL}(2,K)/\mathrm{Ker}\,\Phi = \mathrm{GL}(2,K)/K^* = \mathrm{PGL}(2,K)$. Il suffit donc pour montrer le théorème de vérifier que Φ est surjective.

Fixons $\sigma \in \mathrm{Aut}_K\, K(X)$ quelconque. Posons $Y = \sigma(X)$, que l'on peut écrire sous la forme $Y = \frac{P}{Q}$ avec $P, Q \in K[X]$ premiers entre eux, $Q \neq 0$. Il est clair que l'on a aussi $P \neq 0$, et la surjectivité de σ équivaut à l'existence de deux polynômes $R, S \in K[Y]$ premiers entre eux tels que $X = \frac{R}{S}$. On note :

$$R = a_n Y^n + \cdots + a_1 Y + a_0 \text{ et } S = b_n Y^n + \cdots + b_1 Y + b_0 \text{ avec } a_i, b_i \in K,\ \ (a_0, b_0) \neq (0,0) \neq (a_n, b_n).$$

Donc :

$$X = \frac{a_n P^n Q^{-n} + \cdots + a_1 P Q^{-1} + a_0}{b_n P^n Q^{-n} + \cdots + b_1 P Q^{-1} + b_0} = \frac{a_n P^n + \cdots + a_1 P Q^{n-1} + a_0 Q^n}{b_n P^n + \cdots + b_1 P Q^{n-1} + b_0 Q^n},$$

ou encore :

$$X(b_n P^n + \cdots + b_1 P Q^{n-1} + b_0 Q^n) = a_n P^n + \cdots + a_1 P Q^{n-1} + a_0 Q^n,$$

que l'on écrit sous la forme $(b_0 X - a_0) Q^n = PT$ avec $T \in \mathbb{K}[X]$. Puisque P et Q sont premiers entre eux dans l'anneau principal $K[X]$, on en déduit avec le lemme de Gauss que P divise $(b_0 X - a_0)$. Comme $(a_0, b_0) \neq (0,0)$, il en résulte que P est de degré inférieur ou égal à 1. De manière symétrique, on montre que Q divise $(b_n X - a_n) P^n$ pour en déduire que Q est de degré inférieur ou égal à 1. Ainsi P est de la forme $aX + b$ et Q de la forem $cX + d$, donc $\sigma(X) = \frac{aX+b}{cX+d}$, et la bijectivité de σ implique $ad - bc \neq 0$. Ceci prouve que $\sigma = \sigma_M$ pour $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2,K)$, ce qui établit la surjectivité de Φ.. □

Commentaire. Ce résultat est connu sous le nom de théorème de Lüroth. Un théorème comparable, connu sous le nom de théorème de Castelnuovo, nettement plus profond et compliqué, décrit explicitement le groupe des K-automorphismes de $K(X,Y)$. D'une façon générale, le groupe $\mathrm{Aut}_K\, K(X_1, \ldots, X_n)$ est appelé le groupe de Cremona, et constitue un objet fondamental de géométrie algébrique.