Université de Lille 1 SCIENCES ET TECHNOLOGIES

L2 Info - M32
2018/2019

Chapitre 2
–
DÉTERMINANTS

Dans tout ce chapitre, $\mathbb{K}$ désignera le corps des nombres réels $\mathbb{R}$ ou le corps des nombres complexes $\mathbb{C}$ et E un espace vectoriel sur $\mathbb{K}$.

1 Le groupe symétrique

1.1 Groupe symétrique

Pour $n \in \mathbb{N}$, on note $[\![1\ ;\ n]\!]$ l'ensemble $\{1, 2, \ldots, n\}$

Définition 1.1.1 On appelle *permutation* de $[\![1\ ;\ n]\!]$ toute bijection p de $[\![1\ ;\ n]\!]$ dans $[\![1\ ;\ n]\!]$. Le *support* d'une permutation p est l'ensemble des éléments a de $[\![1\ ;\ n]\!]$ tel que $p(a) \neq a$. On note $\mathcal{S}_n$ l'ensemble des permutations de $[\![1\ ;\ n]\!]$.
L'ensemble de toutes les permutations de $[\![1\ ;\ n]\!]$ muni de la loi de composition des applications "$\circ$" est muni d'une structure de groupe

1. pour tout p, q et r dans $\mathcal{S}_n$, $(p \circ q) \circ r = p \circ (q \circ r)$,
2. l'application identité $Id : [\![1\ ;\ n]\!] \to [\![1\ ;\ n]\!]$ ($Id(k) = k$ pour tout $k \in [\![1\ ;\ n]\!]$) est l'élément neutre pour la composition : pour tout $p \in \mathcal{S}_n$, $p \circ Id = Id \circ p = p$,
3. pour tout $p \in \mathcal{S}_n$, il existe un unique élément $q \in \mathcal{S}_n$ tel que $p \circ q = q \circ p = Id$, $q = p^{-1}$ est la bijection réciproque de p.

$(\mathcal{S}_n, \circ)$ est appelé groupe des permutations de $[\![1\ ;\ n]\!]$ ou groupe symétrique de $[\![1\ ;\ n]\!]$.

Remarque 1.1.2 Si A est un ensemble à n éléments, il existe une bijection de A dans $[\![1\ ;\ n]\!]$ et il existe alors une bijection de $\mathcal{S}_n$ dans le groupe des permutations de A, i.e. le groupe des bijections de A dans lui-même. L'étude du groupe des permutations de A est alors équivalente à celle de $\mathcal{S}_n$ et nous nous intéresserons uniquement à ce dernier.

On représentera une permutation p de la manière suivante :

$$\begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ p(1) & p(2) & \ldots & p(i) & \ldots & p(n) \end{pmatrix}.$$

Remarquons que p s'écrit aussi

$$\begin{pmatrix} 2 & 5 & \ldots & k \\ p(2) & p(5) & \ldots & p(k) \end{pmatrix}$$

pourvu que tous les éléments de $[\![1\ ;\ n]\!]$ apparaissent !

Exemple 1.1.3 Si τ est donné par

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 4 & 3 & 5 & 2 \end{pmatrix}$$

alors $\tau(1) = 6, \tau(2) = 1, \tau(3) = 4, \tau(4) = 3, \tau(5) = 5$ et $\tau(6) = 2$. Le support de τ est $\{1, 2, 3, 4, 6\}$.

Proposition 1.1.4 Le groupe $\mathcal{S}_n$ a $n!$ éléments.

Preuve : voir TD. □

De manière abusive, si p et q sont deux permutations de $\mathcal{S}_n$, on parle du produit pq plutôt que de la composée $p \circ q$. En particulier, p^k désigne $\underbrace{p \circ p \circ p \circ \ldots \circ p}_{k \text{ fois}}$.

Propriété 1.1.5 Le groupe $\mathcal{S}_n$ n'est pas commutatif lorsque $n \geq 3$.

Preuve : Soit p et q définie par :

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 2 & 3 & 1 & 4 & \ldots & n \end{pmatrix}$$
$$q = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 3 & 2 & 1 & 4 & \ldots & n \end{pmatrix}$$

Alors

$$qp = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 2 & 1 & 3 & 4 & \ldots & n \end{pmatrix}$$

et

$$pq = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 1 & 3 & 2 & 4 & \ldots & n \end{pmatrix}$$

donc $pq \neq qp$.

Définition 1.1.6 On appelle *transposition* une permutation dont le support ne comporte que 2 éléments (*t* est une permutation si $\exists i \neq j$ tels que $t(i) = j$, $t(j) = i$ et $t(k) = k$ pour tout $k \neq i, j$).
On appelle *cycle* une transposition c pour laquelle il existe $p \in [\![1\ ;\ n]\!]$ et des éléments $a_1, \ldots, a_p \in [\![1\ ;\ n]\!]$ tels que $c(a_1) = a_2$, $c(a_2) = a_3$,..., $c(a_{p-1}) = c(a_p)$, $c(a_p) = c(a_1)$ et $c(a) = a$ pour tout $a \notin \{a_1, \ldots, a_p\}$. Le nombre p est appelé longueur du cycle et on notera un tel cycle $c = (a_1 a_2 \ldots a_p)$. L'ensemble $\{a_1, \ldots, a_p\}$ est le support de c.

Remarquons que pour tout k, $c(a_{k \mod p}) = a_{(k+1) \mod p}$.

Proposition 1.1.7 Soit $c = (a_1 a_2 \ldots a_p)$ un cycle. Alors pour tout $k \in \mathbb{N}$, $c^k(a_j) = c(a_{j+k \mod p})$.
En particuier, $c^p = Id$.

Preuve : C'est vrai pour $k = 1$: $c(a_1) = a_2$,..., $c(a_{p-1}) = a_p$ et $c(a_p) = a_1 = a_{1+p \mod p}$.
Supposons le résultat vrai au rang k. Alors $c^{k+1}(a_j) = c(c^k(a_j)) = c(a_{j+k \mod p}) = a_{k+j+1 \mod p}$.
Ainsi, l'égalité est encore vraie au rang $k+1$ et donc par récurrence, pour tout k. □

Exemple 1.1.8

$$(1562)^2 = (1652)$$
$$(1562)^3 = (1265)$$
$$(1562)^4 = Id.$$

Proposition 1.1.9 Soient $c = (a_1 \dots a_p)$ et $d = (b_1 \dots b_q)$ deux cycles à supports disjoints (autrement dit $\{a_1, \dots, a_p\} \cap \{b_1, \dots, b_q\} = \emptyset$). Alors $cd = dc$.

Preuve : Soit $a \notin \{a_1, \dots, a_p\} \cup \{b_1, \dots, b_q\}$. Alors $c(a) = a$ et $d(a) = a$ donc $cd(a) = a$ et $dc(a) = a$.
Pour tout j, on $d(a_j) = a_j$ car a_j n'appartient pas au support de d. Pour tout $1 \leq k \leq p$, on a alors $c(a_k) = a_{k+1 \mod p}$ et donc $cd(a_k) = a_{k+1 \mod p}$ et $dc(a_k) = a_{k+1 \mod p}$. De même $dc(b_k) = cd(b_k)$ pour tout k.
Ainsi $cd(a) = dc(a)$ pour tout $a \in [\![1 \ ; \ n]\!]$. □

Exemple 1.1.10 Si $c = (1562)$ et $d = (37)$ sont des éléments de $\mathcal{S}_7$, alors

$$\begin{aligned} cd(1) &= 5 & dc(1) &= 5 \\ cd(2) &= 1 & dc(2) &= 1 \\ cd(3) &= 7 & dc(3) &= 7 \\ cd(4) &= 4 & dc(4) &= 4 \\ cd(5) &= 6 & dc(5) &= 6 \\ cd(6) &= 2 & dc(6) &= 2 \\ cd(7) &= 3 & dc(7) &= 3 \end{aligned}$$

Théorème 1.1.11 Toute permutation de $\mathcal{S}_n$ est décomposable en produit de cycles à support disjoints.

Preuve : Soit p une permutation de $\mathcal{S}_n$. Si p est l'identité, il n'y a rien à faire.
Sinon, soit $a_1 \in [\![1 \ ; \ n]\!]$ tel que $p(a_1) \neq a_1$. On pose $a_2 = p(a_1)$ et tant que a_i n'appartient pas à $\{a_1, \dots, a_{i-1}\}$, on pose $a_i = p(a_{i-1})$.
Soit k le plus petit indice tel que $p(a_k)$ appartienne à $\{a_1, \dots, a_{k-1}\}$. Soit $i \in \{1, \dots, k-1\}$ tel que $p(a_k) = a_i$. Alors, si $i > 1$, $p(a_k) = a_i = p(a_{i-1})$ donc, puisque p est bijective, $a_{i-1} = a_k$ ce qui est absurde ! Donc $p(a_k) = a_1$ et la restriction de p à $\{a_1, \dots, a_k\}$ est un cycle de longueur i. Soit c ce cycle.
Alors $q = c^{-1} \circ p$ est une permutation dont le support est strictement plus petit que celui de p car $q(a_1) = a_1, \dots q(a_p) = a_p$. □

Théorème 1.1.12 Toute permutation est décomposable en cycle de transposition.

Preuve : Il suffit de prouver le théorème pour tout cycle. Soit $c = (a_1 \dots a_k)$ un cycle. Alors

$$c = (a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k).$$

En effet, posons $d = (a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k)$ et montrons que $c = d$. Si $a \notin \{a_1, \dots, a_k\}$, $c(a) = a$ et $d(a) = a$ et pour tout $j \in \{1, \dots, k-1\}$, on $c(a_j) = a_{j+1}$ et :

$$\begin{aligned} d(a_j) &= (a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k)(a_j) \\ &= (a_1 a_2) \dots (a_j a_{j+1})(a_j) \\ &= (a_1 a_2) \dots (a_{j-1} a_j)(a_{j+1}) \\ &= a_{j+1} \end{aligned}$$

et si $j = k$, $c(a_k) = a_1$:

$$\begin{aligned} d(a_k) &= (a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k)(a_k) \\ &= (a_1 a_2)(a_2 a_3) \dots (a_{k-2} a_{k-1}(a_{k-1}) \\ &= (a_1 a_2)(a_2 a_3) \dots (a_{k-3} a_{k-2})(a_{k-2}) \\ &\vdots \\ &= a_1. \end{aligned}$$

Ainsi, $c = d$. $\square$

Exemple 1.1.13 Soit τ est donné par

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 4 & 3 & 5 & 2 \end{pmatrix}$$

Alors

$$\tau = (162)(34)$$

et

$$\tau = (16)(62)(34).$$

En effet, notons $p = (162)(34)$ et $q = (16)(62)(34)$. Alors

$\tau(1) = 6$	$p(1) = 6$	$q(1) = 6$
$\tau(2) = 1$	$p(2) = 1$	$q(2) = 1$
$\tau(3) = 4$	$p(3) = 4$	$q(3) = 4$
$\tau(4) = 3$	$p(4) = 3$	$q(4) = 3$
$\tau(5) = 5$	$p(5) = 5$	$q(5) = 5$
$\tau(6) = 2$	$p(6) = 2$	$q(6) = 2$

1.2 Signature d'une permutation

Définition 1.2.1 Soient $p \in \mathcal{S}_n$ et un couple (i, j) avec $1 \leq i < j \leq n$. On dit que p réalise une inversion du couple (i, j) si $p(i) > p(j)$. On note $I(p)$ le nombre de couples (i, j) (avec $1 \leq i < j \leq n$) sur lesquels p réalise une inversion.
Soit $p \in \mathcal{S}_n$. On appelle signature de p et on note $\varepsilon(p)$ le nombre

$$\varepsilon(p) = (-1)^{I(p)}.$$

Exemple 1.2.2 Dans $\mathcal{S}_4$, la permutation $p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ inverse (1,4), (2,3) (2,4) et (3,4) donc $I(p) = 4$ et $\varepsilon(p) = 1$.

Exemple 1.2.3 Soit t une transposition. Alors $I(t) = 1$ et donc $\varepsilon(t) = -1$.

Théorème 1.2.4 L'application $\varepsilon : \mathcal{S}_n \to \{-1, 1\}$ définit un morphisme du groupe $(\mathcal{S}_n, \circ)$ dans le groupe $(\{-1, 1\}, \cdot)$ (i.e. $\varepsilon(pq) = \varepsilon(q)\varepsilon(q)$ pour toutes permutations p et q).

Preuve : Nous montrons que pour tout $p, q \in \mathcal{S}_n$, $\varepsilon(pq) = \varepsilon(p)\varepsilon(q)$. Soit un couple (i, j) tel que $1 \leq i < j \leq n$. Alors pq réalise une inversion sur le couple (i, j) si et seulement si $p(q(i)) > p(q(j))$. Examinons les différents cas :

- Si q n'inverse pas (i, j) (i.e. $1 \leq q(i) < q(j) \leq n$) et si p réalise une inversion sur le couple $(q(i), q(j))$ alors $p(q(i)) < p(q(j))$.
- Si q réalise une inversion de (i, j) (i.e. $q(i) > q(j)$) et si p n'inverse pas $(q(i), q(j))$ alors $pq(i) > pq(j)$.
- Si q ne réalise pas une inversion de (i, j) (i.e. $q(i) < q(j)$) et si p n'inverse pas $(q(i), q(j))$ alors $pq(i) < pq(j)$.
- Si q réalise une inversion de (i, j) (i.e. $q(i) > q(j)$) et si p inverse $(q(i), q(j))$ alors $pq(i) < pq(j)$.

Ainsi, à chaque inversion réalisé par pq correspond une inversion de p ou de q mais pas aux deux en même temps et réciproquement. On en déduit que $I(pq) = I(p)+I(q) \mod 2$ et $\varepsilon(pq) = (-1)^{I(p)+I(q)} = (-1)^{I(p)}(-1)^{I(q)} = \varepsilon(p)\varepsilon(q)$. $\square$

Exemple 1.2.5 Soit $c = (162)$ un cycle. Alors $\varepsilon(c) = (-1)^2$ car $c = (16)(62)$. Plus généralement, si c est un cycle de longueur k, c se décompose en produit de $k-1$ permutations et $\varepsilon(c) = (-1)^{k-1}$.

Soit $\mathcal{A}_n = \{p \in \mathcal{S}_n / \ \varepsilon(p) = 1\} = \ker \varepsilon$. L'ensemble $\mathcal{A}_n$ est appelé ensemble des permutations paires. Une permutation qui n'est pas paire est dite impair.
Soit t une transposition et $\varphi_t : \mathcal{A}_n \to \mathcal{S}_n \setminus \mathcal{A}_n$ définie pour tout p par $\varphi_t(p) = p \circ t$. Alors φ_t est bien définie au sens où si p est une permutation paire, $p \circ t$ est impair. De plus φ_t est une bijection. En effet, si $\varphi_t(p) = \varphi_t(q)$ alors $p \circ t = q \circ t$ et donc $p \circ t \circ t = q \circ t \circ t$, i.e. $p = q$ car $t^{-1} = t$: l'application φ_t est donc injective. Si p est impair, $p \circ t$ est pair et $\varphi_t(p \circ t) = p$ donc φ_t est surjective et donc bijective.

2 Déterminants

2.1 Formes n-linéaires et formes alternées

Définition 2.1.1 Soit $n \in \mathbb{N}^*$. On dit que $f : E^n \to \mathbb{K}$ est n-linéaire si pour tout j et tous vecteurs $v_1, \ldots, v_{j-1}, v_{j+1}, \ldots, v_n$, l'application $f_j : \left\{ \begin{array}{ccc} E & \longrightarrow & E \\ v & \longmapsto & f_j(v) = f(v_1, \ldots, v_{j-1}, v, v_{j+1}, \ldots v_n) \end{array} \right.$ est linéaire. Lorsque $n \geq 2$, on parle de forme multi-linéaire.

Autrement dit, si on fixe $n-1$ composantes, f est linéaire par rapport à la n-ième : Pour tout j, tout $u_1, \ldots, u_n, v, w \in E$, tout $\lambda \in \mathbb{K}$:

$$\begin{aligned} &f(u_1, \ldots, u_{j-1}, v + \lambda w, u_{j+1}, \ldots u_n) \\ &= f(u_1, \ldots, u_{j-1}, v, u_{j+1}, \ldots u_n) + \lambda f(u_1, \ldots, u_{j-1}, w, u_{j+1}, \ldots u_n). \end{aligned}$$

Définition 2.1.2 Une application $f : E^n \to \mathbb{K}$ est dite anti-symétrique si pour tout $i \neq j$ et tout $v_1, \ldots, v_n \in E$, on a :

$$f(v_1, \ldots, v_{i-1}, v_i, v_{i+1}, \ldots, v_{k-1}, v_k, v_{k+1}, \ldots, v_n) = -f(v_1, \ldots, v_{i-1}, v_k, v_{i+1}, \ldots, v_{k-1}, v_i, v_{k+1}, \ldots, v_n).$$

On peut reformuler la définition précédente de la manière suivante :

Définition 2.1.3 Une application $f : E^n \to \mathbb{K}$ est dite anti-symétrique si pour tout transposition t de $\mathcal{S}_n$ et tout $v_1, \ldots, v_n \in E$, on a :

$$f(v_{t(1)}, \ldots, v_{t(n)}) = -f(v_1, \ldots, v_n).$$

Proposition 2.1.4 Soit $f : E^n \to E$ une application n anti-symétrique. Alors pour toute permutation p de $\mathcal{S}_n$ et tout vecteur $v_1, \ldots, v_n \in E$, on a :

$$f(v_{p(1)}, \ldots, v_{p(n)}) = \varepsilon(p) f(v_1, \ldots, v_n).$$

Preuve : Si p est une permutation, elle est décomposable en produit de k transpositions : $p = t_1 t_2 \ldots t_k$. On en déduit alors que

$$\begin{aligned} f(v_{p(1)}, \ldots, v_{p(n)}) &= f(v_{t_1 t_2 \ldots t_k(1)}, \ldots, v_{t_1 t_2 \ldots t_k(n)}) \\ &= f(v_{t_1(t_2 \ldots t_k(1))}, \ldots, v_{t_1(t_2 \ldots t_k(n))}) \\ &= -f(v_{t_2 \ldots t_k(1)}, \ldots, v_{t_2 \ldots t_k(n)}) \\ &\vdots \\ &= (-1)^k f(v_1, \ldots, v_n). \end{aligned}$$

Comme $\varepsilon(p) = (-1)^k$, le théorème est montré. □

Définition 2.1.5 Une n-forme linéaire f est dite alternée si pour tout vecteur $u_1, \ldots, u_n$, tels qu'il existe $i \neq j$ tel que $u_i = u_j$, alors $f(u_1, \ldots, u_n) = 0$

Proposition 2.1.6 Soit f une forme n-linéaire alternée sur E. Alors f est anti-symétrique.

Preuve : Afin de simplifier l'écriture, nous montrons seulement que pour tous vecteurs $u_1, \ldots, u_n$, $f(u_1, u_2, u_3, \ldots, u_n) = -f(u_2, u_1, u_3, \ldots, u_n)$. Alors comme f est n-linéaire :

$$\begin{aligned} &f(u_1 + u_2, u_1 + u_2, \ldots u_n) \\ &= f(u_1, u_1, \ldots, u_n) + f(u_1, u_2, \ldots, u_n) + f(u_2, u_1, \ldots, u_n) + f(u_2, u_2, \ldots, u_n). \end{aligned}$$

Comme f est alternée, il vient $f(u_1, u_2, \ldots, u_n) + f(u_2, u_1, \ldots, u_n) = 0$. □

Proposition 2.1.7 Soit f une forme n-linéaire alternée sur E. Alors pour tous vecteurs $x_1, \ldots, x_n$ liés $f(x_1, \ldots, x_n) = 0$.

Preuve : Puisque les vecteurs $x_1, \ldots, x_n$ sont liés, il existe j et $\lambda_1, \ldots, \lambda_{j-1}, \lambda_{j+1}, \ldots, \lambda_n$ tels que $x_j = \sum_{\substack{i=1 \\ i \neq j}}^{n} \lambda_i x_i$. Comme f est n-linéaire, il vient alors

$$\begin{aligned} f(x_1, \ldots, x_n) &= f(x_1, \ldots, x_{j-1}, \sum_{\substack{i=1 \\ i \neq j}}^{n} \lambda_i x_i, x_{j+1}, \ldots, x_n) \\ &= \sum_{\substack{i=1 \\ i \neq j}}^{n} \lambda_i f(x_1, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_n). \end{aligned}$$

Puisque f est alternée, pour tout $i \neq j$, $f(x_1, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_n) = 0$ d'où $f(x_1, \ldots, x_n) = 0$. □

2.2 Déterminants d'une famille de vecteurs

Définition 2.2.1 Soit E un $\mathbb{K}$-espace vectoriel de dimension n et $(e_1, \ldots, e_n)$ une base de E. L'ensemble des formes n-linéaires alternées sur E est un $\mathbb{K}$-espace vectoriel de dimension 1. Il existe une unique forme n-linéaire alternée qui prend la valeur 1 en $(e_1, \ldots, e_n)$. On l'appelle déterminant relatif à la base $e_1, \ldots, e_n$ et on la note $\det_{(e_i)}$ ou simplement det si aucune confusion n'est à craindre. De plus, pour tout $(x_1, \ldots, x_n) \in E^n$, si $(x_{i1}, \ldots, x_{i,n})$ sont les coordonnées de x_i dans la base $e_1, \ldots, e_n$, on a :

$$\det_{(e_i)}(x_1, \ldots, x_n) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) x_{1\sigma(1)} \ldots x_{n\sigma(n)}.$$

En particulier, pour toute forme n-linéaire alternée ϕ, il existe $\lambda \in \mathbb{K}$ tel que $\phi = \lambda \det_{(e_i)}$.

Preuve : Soit f une forme n-linéaire alternée sur E. Soit $(e_1, \ldots, e_n)$ une base de E et soient donnés n vecteurs $x_1, \ldots, x_n$ de E. On note $(x_{1,1}, \ldots, x_{1n})$ les coordonnées de x_1, ..., $(x_{n,1}, \ldots, x_{nn})$ celle de x_n. Alors nous avons

$$\begin{aligned} f(x_1, \ldots, x_n) &= f\left(\sum_{j_1=1}^{n} x_{1,j_1} e_{j_1}, \ldots, \sum_{j_n=1}^{n} x_{1,j_n} e_{j_n}, \right) \\ &= \sum_{j_1, \ldots, j_n = 1}^{n} x_{1,j_1} \ldots x_{n,j_n} f(e_{j_1}, \ldots, e_{j_n}). \end{aligned}$$

Mais si $j_k = j_l$ pour un couple (k, l), $l \neq k$, alors $f(e_{j_1}, \ldots, e_{j_n}) = 0$. Cela implique que $k \mapsto j_k$ est une bijection (puisque c'est une application injective de $[\![1\ ;\ n]\!]$ dans lui-même). Autrement dit, on somme

sur toutes les permutations de $[\![1\ ;\ n]\!]$:

$$\begin{aligned} f(x_1,\dots,x_n) &= \sum_{p\in\mathcal{S}_n} x_{1,p(1)}\dots x_{n,p(n)} f(e_{p(1)},\dots,e_{p(n)}) \\ &= \sum_{p\in\mathcal{S}_n}^{n} \varepsilon(p) x_{1,p(1)}\dots x_{n,p(n)} f(e_1,\dots,e_n) \\ &= f(e_1,\dots,e_n) \sum_{p\in\mathcal{S}_n} \varepsilon(p) x_{1,p(1)}\dots x_{n,p(n)}. \end{aligned}$$

Soit Δ l'application définie sur E par $\Delta(x_1,\dots,x_n) = \sum_{p\in\mathcal{S}_n}^{n} \varepsilon(p) x_{1,p(1)}\dots x_{n,p(n)}$.
Si nous démontrons que Δ est n-linéaire alternée, alors toute forme n-linéaire alternée f s'écrira

$$f = \lambda\Delta$$

où $\lambda = f(e_1,\dots,e_n)$ et si $f(e_1,\dots,e_n) = 1$, alors $f = \Delta$ ce qui prouvera le théorème.
Soit $x_1,\dots,x_n$, n vecteurs de E, $u,v \in E$, $\lambda \in \mathbb{K}$ et $i \in [\![1\ ;\ n]\!]$. Alors

$$\begin{aligned} &\Delta(x_1,\dots,x_{i-1},u+\lambda v,,x_{i+1},\dots,x_n) \\ &= \sum_{p\in\mathcal{S}_n} \varepsilon(p) x_{1p(1)}\dots x_{ip(i+1)}(u_{p(i)}+\lambda v_{p(i)}) x_{i+1p(i+1)}\dots x_{np(n)} \\ &= \sum_{p\in\mathcal{S}_n} \varepsilon(p) x_{1p(1)}\dots x_{ip(i+1)} u_{p(i)} x_{i+1p(i+1)}\dots x_{np(n)} + \lambda \sum_{p\in\mathcal{S}_n} \varepsilon(p) x_{1p(1)}\dots x_{ip(i+1)} v_{p(i)} x_{i+1p(i+1)}\dots x_{np(n)} \\ &= \Delta(x_1,\dots,x_{i-1},u,x_{i+1},\dots,x_n) + \lambda\Delta(x_1,\dots,x_{i-1},v,,x_{i+1},\dots,x_n). \end{aligned}$$

Par conséquent, Δ est n-linéaire. montrons qu'elle est alternée.
Soit $x_1,\dots,x_n$, n vecteurs de E telle que $x_1 = x_2$ par exemple. On considère $t = (12)$. Alors

$$\begin{aligned} \Delta(x_1,\dots,x_n) &= \sum_{p\in\mathcal{S}_n} \varepsilon(p) x_{1p(1)}\dots x_{np(n)} \\ &= \sum_{p\in\mathcal{A}_n} \varepsilon(p) x_{1p(1)}\dots x_{np(n)} + \sum_{p\in\mathcal{S}_n\setminus\mathcal{A}_n} \varepsilon(p) x_{1p(1)}\dots x_{np(n)} \\ &= \sum_{p\in\mathcal{A}_n} \varepsilon(p) x_{1p(1)}\dots x_{np(n)} + \sum_{p\in\mathcal{A}_n} \varepsilon(pt) x_{1pt(1)} x_{2pt(2)}\dots x_{npt(n)} \text{ car } \varphi_t \text{ est une bijection} \\ &= \sum_{p\in\mathcal{A}_n} \varepsilon(p) x_{1p(1)}\dots x_{np(n)} + \sum_{p\in\mathcal{A}_n} -\varepsilon(p) x_{1p(2)} x_{2p(1)}\dots x_{npt(n)} \\ &= \sum_{p\in\mathcal{A}_n} \varepsilon(p) x_{1p(1)}\dots x_{np(n)} + \sum_{p\in\mathcal{A}_n} -\varepsilon(p) x_{2p(2)} x_{1p(1)}\dots x_{npt(n)} \text{ car } x_1 = x_2 \\ &= 0 \end{aligned}$$

Ainsi Δ est alternée. □

Théorème 2.2.2 Soit $x_1,\dots,x_n$ des vecteurs de E. Les assertions suivantes sont équivalentes :

(i) Les vecteurs $x_1,\dots,x_n$ sont liés,

(ii) Pour toute base $e_1,\dots,e_n$ de E, $\det_{e_i}(x_1,\dots,x_n) = 0$.

(iii) Il existe une base $e_1,\dots,e_n$ de E, telle que $\det_{e_i}(x_1,\dots,x_n) = 0$.

Preuve : L'implication $(i) \Rightarrow (ii)$ est immédiate d'après la proposition 2.1.7.
L'implication $(ii) \Rightarrow (iii)$ est évidente.
Nous démontrons maintenant l'implication $(iii) \Rightarrow (i)$ en montrant la contraposée : non (i) implique non (iii), autrement dit que si $x_1,\dots,x_n$ est une famille libre, alors pour toute base $e_1,\dots,e_n$ de E, telle que $\det_{e_i}(x_1,\dots,x_n) \neq 0$.

Comme $x_1, \dots, x_n$ est une famille libre et comme $\dim E = n$, $x_1, \dots, x_n$ est une base de E. Par conséquent $\det_{(x_i)}(x_1, \dots, x_n) = 1 \neq 0$.
Si maintenant $e_1, \dots, e_n$ est une base de E, comme $\det_{(e_i)}$ est une application multi linéaire alternée que l'ensemble des formes multi linéaires alternées est un espace vectoriel de dimension 1, il existe $\lambda \in \mathbb{K}$ tel que $\det_{(e_i)} = \lambda \det_{(x_i)}$. De plus, $\lambda \neq 0$ car $\det_{(e_i)}(e_1, \dots, e_n) = 1 = \lambda \det_{(x_i)}(e_1, \dots, e_n)$ et $\lambda = \lambda \det_{(x_i)}(x_1, \dots, x_n) = \det_{(e_i)}(x_1, \dots, x_n)$, d'où $\det_{(e_i)}(x_1, \dots, x_n) \neq 0$. □

Corollaire 2.2.3 Une famille $x_1, \dots, x_n \in E$ est une base de E si et seulement si il existe une base $e_1, \dots, e_n$ de E telle que $\det_{(e_j)}(x_1, \dots, x_n) \neq 0$.

Puisque le déterminant est une forme n-linéaire alternée, nous avons :

Proposition 2.2.4 Soient $x_1, \dots, x_n, x_i' \in E$, $\lambda \in \mathbb{K}$. Alors

1.
$$\det(x_1, \dots, x_i + x_i', \dots, x_n) = \det(x_1, \dots, x_i, \dots, x_n) + \det(x_1, \dots, x_i', \dots, x_n),$$
$$\det(x_1, \dots, \lambda x_i, \dots, x_n) = \lambda \det(x_1, \dots, x_i, \dots, x_n).$$

2. Si les vecteurs $x_1, \dots, x_n$ sont liés (en particulier si l'un des vecteurs est nul) :
$$\det(x_1, \dots, x_n) = 0.$$

3. Pour tout $\lambda_1, \dots, \lambda_n \in \mathbb{K}$:
$$\det(x_1, \dots, x_{i-1}, \sum_{j=1}^{n} \lambda_j x_j, x_{i+1}, \dots, x_n) = \lambda_i \det(x_1, \dots, x_n).$$

4. Pour toute permutation p, on a
$$\det(x_{p(1)}, \dots, x_{p(n)}) = \varepsilon(p) \det(x_1, \dots, x_n).$$
En particulier, si on échange deux colonnes, on multiplie le déterminant par -1.

Exemple 2.2.5

$$\begin{vmatrix} 5 & -1 & -3 \\ 2 & 1 & -4 \\ 3 & -2 & 1 \end{vmatrix} = 0, \qquad \begin{vmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 7 \end{vmatrix} = 0.$$

3 Déterminant d'une matrice et d'un endomorphisme

Définition 3.0.1 Soit $A = (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{K})$, soit $e_1, \dots, e_n$ la base canonique de $\mathbb{K}^n$, soit $c_j = \sum_{i=1}^{n} a_{ij} e_j$ pour $j = 1, \dots, n$ les vecteurs colonnes de A. On appelle déterminant de A le déterminant des vecteurs colonnes c_j de A :

$$\det A = \det_{(e_j)}(c_1, \dots, c_n) = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \sum_{p \in \mathcal{S}_n} \varepsilon(p) a_{p(1)1} \dots a_{p(n)n}.$$

Proposition 3.0.2 Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors $\det A = \det A^t$.

Preuve : Nous avons

$$\det A = \sum_{p\in\mathcal{S}_n} \varepsilon(p) a_{p(1)1}\dots a_{p(n)n}, \qquad \det A^t = \sum_{q\in\mathcal{S}_n} \varepsilon(p) a_{1q(1)}\dots a_{nq(n)}.$$

Le produit $a_{1q(1)}\dots a_{nq(n)}$ est invariant si on fait subir aux facteurs une permutation, donc pour tout $t \in \mathcal{S}_n$, on a

$$a_{1q(1)}\dots a_{nq(n)} = a_{t(1)qt(1)}\dots a_{t(n)qt(n)}.$$

En particulier si $t = q^{-1}$:

$$a_{1q(1)}\dots a_{nq(n)} = a_{q^{-1}(1)1}\dots a_{q^{-1}(n)n}$$

et puisque $\varepsilon(q^{-1}) = \varepsilon(q)$

$$\varepsilon(q) a_{1q(1)}\dots a_{nq(n)} = \varepsilon(q^{-1}) a_{q^{-1}(1)1}\dots a_{q^{-1}(n)n}.$$

On en déduit :

$$\det A^t = \sum_{q\in\mathcal{S}_n} \varepsilon(q^{-1}) a_{q^{-1}(1)1}\dots a_{q^{-1}(n)n}.$$

Mais l'application $q \mapsto q^{-1}$ de $\mathcal{S}_n$ dans lui-même est bijective et donc

$$\det A^t = \sum_{q\in\mathcal{S}_n} \varepsilon(q) a_{q(1)1}\dots a_{q(n)n}.$$

□
Puisque $\det A = \det A^t$, toute propriété vraie sur les colonnes, le sera également sur les lignes.

Théorème 3.0.3 Soient A et B deux matrices. Alors

$$\det(AB) = \det(BA) = \det A \det B.$$

Preuve : Soit $e_1, \dots, e_n$ une base de $\mathbb{K}^n$. On considère les endomorphismes f et g de $\mathbb{K}^n$ dont les matrices dans la base $e_1, \dots, e_n$ sont respectivement A et B.
Soit φ la forme définie sur $\mathbb{K}^n$ par

$$\varphi(x_1, \dots, x_n) = \det{}_{(e_i)}(g(x_1), \dots, g(x_n)).$$

L'application g étant linéaire et le déterminant étant n-linéaire, φ est n-linéaire et puisque le déterminant est alterné, φ est aussi alterné car si $x_i = x_j$, $g(x_i) = g(x_j)$ et $det_{(e_i)}(g(x_1), \dots, g(x_n)) = 0$ puisque deux vecteurs parmi $g(x_1), \dots, g(x_n)$ sont égaux.
D'après la défintion 2.1.1, il existe donc $\lambda = \det(g(e_1), \dots, g(e_n)) \in \mathbb{K}$ tel que $\varphi = \lambda \det_{(e_i)}$. On en déduit que

$$\varphi(f(x_1), \dots, f(x_n)) = \lambda \det{}_{(e_i)}(f(x_1), \dots, f(x_n)).$$

Par conséquent :

$$\det{}_{(e_i)}(g \circ f(e_1), \dots, g \circ f(e_n)) = \det(g(e_1), \dots, g(e_n)) \cdot \det{}_{(e_i)}(fe_1), \dots, f(e_n)).$$

Mais $g(e_1), \dots, g(e_n)$ sont les colonnes de B, de même $f(e_1), \dots, f(e_n)$ sont les colonnes de A et $g \circ f(e_1), \dots, g \circ f(e_n)$ sont les colonnes de la matrice de $g \circ f$ dans la base $e_1, \dots, e_n$ qui est égale à BA. Ainsi

$$\det(BA) = \det(A) \det(B).$$

De même on montre que $\det(AB) = \det A \det B$. □

Corollaire 3.0.4 Soit A une matrice. Alors A est inversible si et seulement si $\det A \neq 0$ et dans ce cas :

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

Preuve : Si A est inversible, on a $\det(AA^{-1}) = \det(I_n) = 1$ et $\det(AA^{-1}) = \det A \det(A^{-1})$ donc $\det(A)\det(A^{-1}) = 1$. Par conséquent, $\det A \neq 0$ et $\det(A^{-1}) = \frac{1}{\det A}$.
Réciproquement, si $\det A \neq 0$, A représente un endomorphisme inversible puisque les colonnes de A sont libres donc A est inversible. □

Ces corollaires impliquent que pour toute matrice inversible P et toute matrice A, on a

$$\begin{aligned}\det(P^{-1}AP) &= \det(P^{-1})\det(A)\det P \\ &= \det A.\end{aligned}$$

Ainsi, si f est un endomorphisme d'un espace vectoriel E, $e_1, \ldots, e_n$ et $e'_1, \ldots, e'_n$ deux bases de E, A la matrice de f dans la base $e_1, \ldots, e_n$, A' la matrice de f dans la base $e'_1, \ldots, e'_n$, et P la matrice de passage de la base $e_1, \ldots, e_n$ à la base $e'_1, \ldots, e'_n$. Alors $A = PA'P^{-1}$ et $\det A = \det A'$. Autrement dit, toutes les matrices représentant un même endomorphisme ont le même déterminant. Cela nous autorise à poser la définition suivante :

Définition 3.0.5 Soit f un endomorphisme d'un espace vectoriel E. On appelle déterminant de f et on note $\det f$ le déterminant de la matrice de f dans une base quelconque $e_1, \ldots, e_n$ de E.

Proposition 3.0.6 Soient f et g deux endomorphismes de E. On a

$$\det(f \circ g) = \det f \cdot \det g.$$

4 Méthode de calcul des déterminants

Théorème 4.0.1 (Développement par blocs) Soit $M = (m_{ij})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{K})$ et $p \in [\![1\ ;\ n]\!]$ tels que pour tout $i > p$ et tout $j < p+1$, $m_{ij} = 0$:

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

où $A \in \mathcal{M}_p(\mathbb{K})$, $B \in \mathcal{M}_{n-p}(\mathbb{K})$, $C \in \mathcal{M}_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n-p}}(\mathbb{K})$ et O est la matrice nulle à $n-p$ lignes et p colonnes.
Alors

$$\det M = \det A \det B.$$

Preuve : Nous avons

$$\det M = \sum_{t \in \mathcal{S}_n} \varepsilon(t) m_{t(1)1} \ldots m_{t(n)n}.$$

Mais si $t(1)$ ou $t(2)$ ou $\ldots t(p)$ appartient à $[\![p+1;\ n]\!]$, le produit $m_{t(1)1} \ldots m_{t(n)n}$ est nul. Ainsi le terme $m_{t(1)1} \ldots m_{t(n)n} = 0$ dès que $t([\![1,p]\!])$ n'est pas inclus dans $t([\![1,p]\!])$. Donc seules les permutations t telles que $t([\![1,p]\!]) \subset [\![1,p]\!]$ nous intéressent donc

$$\det M = \sum_{\substack{t \in \mathcal{S}_n \\ t([\![1;\ p]\!]) \subset [\![1;\ p]\!]}} \varepsilon(t) m_{t(1)1} \ldots m_{t(n)n}.$$

De plus, si $t([\![1;p]\!])$ est inclus dans $[\![1;\ p]\!]$, nécessairement $t([\![p+1;\ n]\!])$ est inclus dans $[\![p+1;\ n]\!]$.
Ainsi $t' : [\![1;\ p]\!] \to [\![1;\ p]\!]$ définie par $t'(i) = t(i)$ appartient à $\mathcal{S}_p$ et $t'' : [\![1;\ n-p]\!] \to [\![1; n-p]\!]$ définie par $t''(i) = t(i+p) - p$ appartient à $\mathcal{S}_{n-p}$. Réciproquement si t' appartient à $\mathcal{S}_p$ et t'' appartient à

$\mathcal{S}_{n-p}$, alors $t : [\![1\ ;\ n]\!] \to [\![1\ ;\ n]\!]$ définie par $t(i) = t'(i)$ si $i \leq p$ et $t(i) = t''(i-p)+p$ si $i > p$ est une permutation de $\mathcal{S}_n$ telle que $t([\![1;p]\!])$ est inclus dans $[\![1;\ p]\!]$ et $t([\![p+1;\ n]\!])$ est inclus dans $[\![p+1;\ n]\!]$. Enfin pour une telle permutation t, le nombre d'inversions de t est égal au nombre d'inversions de t' ajouté au nombre d'inversions de t'' et on a donc $\varepsilon(t) = \varepsilon(t')\varepsilon(t'')$.
On en déduit que

$$\begin{aligned}\det M &= \sum_{\substack{t'\in\mathcal{S}_p\\ t''\in\mathcal{S}_{n-p}}} \varepsilon(t')\varepsilon(t'')m_{t'(1)1}\dots m_{t'(p)p}m_{p+t''(1)p+1}m_{t''(n-p)+pn-p+p}\\ &= \left(\sum_{t'\in\mathcal{S}_p}\varepsilon(t')m_{t'(1)1}\dots m_{t'(p)p}\right)\left(\sum_{t''\in\mathcal{S}_{n-p}}\varepsilon(t'')m_{p+t''(1)p+1}m_{t''(n-p)+pn-p+p}\right)\\ &= \det A\det B.\end{aligned}$$

car $B = \begin{pmatrix} m_{p+1,p+1} & \dots & m_{p+1,p+(n-p)} \\ \vdots & \vdots & \\ m_{p+(n-p),p+1} & \dots & m_{p+(n-p),p+(n-p)}\end{pmatrix}$ ce qui implique que

$$\det B = \sum_{t''\in\mathcal{S}_{n-p}}\varepsilon(t'')m_{p+t''(1)p+1}m_{p+t''(n-p),p+n-p}.$$

□

Corollaire 4.0.2 Soit $M \in \mathcal{M}_n(\mathbb{K})$ une matrice triangulaire par bloc, i.e.

$$M = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1p} \\ O & A_{22} & \dots & A_{2p} \\ \vdots & \ddots & \ddots & \vdots \\ O & \dots & O & A_{pp}\end{pmatrix},$$

où pour tout i, A_{ii} est une matrice carrée et où O représente une matrice dont tous les coefficients sont nuls.
Alors

$$\det M = \det(A_{11})\dots\det(A_{pp}).$$

Preuve : il suffit de raisonner par récurrence en utilisant le théorème précédent. □
On en déduit immédiatement le corollaire suivant.

Corollaire 4.0.3 Soit $T = (t_{i,j})_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{K})$ une matrice triangulaire ou une matrice diagonale. Alors $\det T = t_{11}t_{22}\dots t_{nn}$.

Définition 4.0.4 Soit $A = (a_{i,j})_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{K})$. Pour tout (i,j), on appelle mineur de l'entrée $a_{i,j}$ de déterminant $\Delta_{i,j}$ de la matrice carrée de taille $n-1$ obtenue en supprimant la i-ième ligne et la j-ième colonne de A.
Le nombre $A_{i,j} = (-1)^{i+j}\Delta_{i,j}$ est appelé cofacteur de $a_{i,j}$.

Corollaire 4.0.5 Soit $A = (a_{i,j})_{1\leq i,j\leq n} \in \mathcal{M}_n(\mathbb{K})$, $A_{i,j}$ les cofacteurs de A. Alors pour tout (i,j) :

$$\det A = \sum_{k=1} a_{k,j}A_{k,j} = \sum_{k=1} a_{j,k}A_{j,k}.$$

Preuve : Soit $e_1, \dots, e_n$ la base canonique de $\mathbb{K}^n$ et pour tout j, soit $a_j = \sum_{i=1} a_{ij} e_j$. Alors

$$\begin{aligned}\det A &= \det(a_1, \dots, a_j, \dots, a_n) \\ &= \det(a_1, \dots, \sum_{k=1}^{n} a_{kj} e_k, \dots, a_n) \\ &= \sum_{j=1}^{n} a_{kj} \det(a_1, \dots, a_{j-1}, e_k, a_{j+1}, \dots, a_n).\end{aligned}$$

Il reste donc à démontrer que

$$A_{k,j} = \det(a_1, \dots, a_{j-1}, e_k, a_{j+1}, \dots, a_n).$$

Or

$$\begin{aligned}\det(a_1, \dots, e_k, \dots, a_n) &= (-1)^{j+1} \det(e_k, a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_n) \\ &= (-1)^{j+1} \begin{vmatrix} 0 & a_{11} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 1 & a_{k1} & \dots & a_{k,j-1} & a_{k,j+1} & \dots & a_{kn} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & a_{n1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{nn} \end{vmatrix} \\ &= (-1)^{j+1}(-1)^{k+1} \begin{vmatrix} 1 & a_{k1} & \dots & a_{k,j-1} & a_{k,j+1} & \dots & a_{kn} \\ 0 & a_{11} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & a_{k-1,1} & \dots & a_{k-1,j-1} & a_{k-1,j+1} & \dots & a_{k-1n} \\ 0 & a_{k+1,1} & \dots & a_{k+1,j-1} & a_{k+1,j+1} & \dots & a_{k+1,n} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & a_{n1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{nn} \end{vmatrix}.\end{aligned}$$

On en déduit grâce au déterminant par bloc que

$$\begin{aligned}\det(a_1, \dots, e_k, \dots, a_n) &= (-1)^{j+k} \begin{vmatrix} a_{11} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{k-1,1} & \dots & a_{k-1,j-1} & a_{k-1,j+1} & \dots & a_{k-1n} \\ a_{k+1,1} & \dots & a_{k+1,j-1} & a_{k+1,j+1} & \dots & a_{k+1,n} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{n1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{nn} \end{vmatrix} \\ &= A_{k,j}.\end{aligned}$$

□

Exemple 4.0.6

$$\begin{vmatrix} 1 & 2 & -1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{vmatrix} = 3$$

5 Applications des déterminants

5.1 Calcul de l'inverse d'une matrice

Définition 5.1.1 Soit $A = (a_{i,j})_{1 \le i,j \le n} \in \mathcal{M}_n(\mathbb{K})$. On appelle comatrice de A la matrice $\mathrm{com}(A) = (A_{i,j})_{1 \le i,j \le n}$ où les $A_{i,j}$ sont les cofacteurs de A.

Proposition 5.1.2 Soit $A \in \mathcal{M}_n(\mathbb{K})$. Alors

$$\mathrm{com}(A)^t \cdot A = A \cdot \mathrm{com}(A)^t = (\det A) I_n.$$

Preuve : Soit $b_1, \ldots, b_n \in \mathbb{K}$ et $j \in [\![1\ ;\ n]\!]$. Notons M la matrice obtenue à partir de A en remplaçant la j-ième ligne par $(b_1, \ldots, b_n)$. Alors, en développant le déterminant de M par rapport à la j-ième ligne, il vient

$$\det M = \sum_{k=1}^{n} b_k A_{jk}.$$

En particulier, si $(b_1, \ldots, b_n) = (a_{j,1}, \ldots, a_{j,n})$, on a $\det M = \det A$ d'où

$$\sum_{k=1}^{n} a_{j,k} A_{j,k} = \det A.$$

Si $(b_1, \ldots, b_n) = (a_{i,1}, \ldots, a_{i,n})$ avec $i \neq j$, alors $\det M = 0$ d'où

$$\sum_{k=1}^{n} a_{j,k} A_{j,k} = 0.$$

D'autre part, les coefficients de $A \cdot \mathrm{com}(A)^t$ sont

$$c_{ij} = \sum_{k=1}^{n} a_{ik} A_{jk},$$

d'où $A \cdot \mathrm{com}(A)^t = (\det A) I_n$. □

Corollaire 5.1.3 (Formules de Cramer) Soient $A = (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{K})$ et $b \in \mathbb{K}^n$. Si A est inversible, l'équation $Ax = b$ admet une unique solution $(x_1, \ldots, x_n)$ où pour tout $j \in [\![1\ ;\ n]\!]$

$$x_j = \frac{\begin{vmatrix} a_{1,1} & \ldots & a_{1,j-1} & b_1 & a_{1,j+1} & \ldots & a_{1,n} \\ a_{2,1} & \ldots & a_{2,j-1} & b_2 & a_{2,j+1} & \ldots & a_{2,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & \ldots & a_{n,j-1} & b_n & a_{n,j+1} & \ldots & a_{n,n} \end{vmatrix}}{\begin{vmatrix} a_{1,1} & \ldots & a_{1,j-1} & a_{1,j} & a_{1,j+1} & \ldots & a_{1,n} \\ a_{2,1} & \ldots & a_{2,j-1} & a_{2,j} & a_{2,j+1} & \ldots & a_{2,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & \ldots & a_{n,j-1} & a_{n,j} & a_{n,j+1} & \ldots & a_{n,n} \end{vmatrix}}.$$

Preuve : Soit $x = (x_1, \ldots, x_n)$ le vecteur donné par la formule ci-dessus Nous avons pour tout j

$$\begin{vmatrix} a_{1,1} & \ldots & a_{1,j-1} & b_1 & a_{1,j+1} & \ldots & a_{1,n} \\ a_{2,1} & \ldots & a_{2,j-1} & b_2 & a_{2,j+1} & \ldots & a_{2,n} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{n,1} & \ldots & a_{n,j-1} & b_n & a_{n,j+1} & \ldots & a_{n,n} \end{vmatrix} = b_1 A_{1,j} + b_2 A_{2,j} + \ldots + b_n A_{n,j},$$

d'où

$$\begin{aligned} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} &= \frac{1}{\det A} \begin{pmatrix} b_1 A_{1,1} + b_2 A_{2,1} + \ldots + b_n A_{n,1} \\ \vdots \\ b_1 A_{1,n} + b_2 A_{2,n} + \ldots + b_n A_{n,n} \end{pmatrix} \\ &= \frac{1}{\det A} \mathrm{com}(A)^t \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \\ &= A^{-1} b. \end{aligned}$$

Ainsi x vérifie bien $Ax = b$. Comme A est inversible, c'est l'unique solution. □
D'un point de vue numérique, le temps de calcul d'un déterminant est très important en comparaison de la résolution directe d'un système d'équations linéaires. Les formules de Cramer ne sont pas exploitables dans la pratique.

5.2 Chiffrement de Hill

Il s'agit d'une généralisation du chiffrement affine vu dans le cours "Mathématiques, Informatique : Arithmétique et Cryptographie". On travaille avec l'alphabet à 26 lettres "ABCDEFGHIJKLMNOPQRSTUVWXYZ", A étant identifié au nombre 0, B à 1, C à 2...

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

Soit $A \in \mathcal{M}_2(\mathbb{Z}/26\mathbb{Z})$ et $b \in \mathcal{M}_{2\times 1}(\mathbb{Z}/26\mathbb{Z})$. On considère l'application de chiffrement

$$\phi : \begin{cases} \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} & \longrightarrow & \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z} \\ \begin{pmatrix} x \\ y \end{pmatrix} & \longmapsto & A\begin{pmatrix} x \\ y \end{pmatrix} + b \end{cases} .$$

On chiffre donc des digrammes. Par exemple, si $A = \begin{pmatrix} 1 & 2 \\ 5 & 3 \end{pmatrix}$ et $b = \begin{pmatrix} 1 \\ 2 \end{pmatrix}$, le mot "COUCOU" sera chiffré comme suit :

$$\begin{aligned} \text{"COUCOU"} &\to \begin{pmatrix} 2 \\ 14 \end{pmatrix}, \begin{pmatrix} 20 \\ 2 \end{pmatrix} \begin{pmatrix} 14 \\ 20 \end{pmatrix}, \\ &\xrightarrow{\phi} \begin{pmatrix} 5 \\ 2 \end{pmatrix}, \begin{pmatrix} 25 \\ 4 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \\ &\to \text{"FCZEDC"} \end{aligned}$$

Remarque 5.2.1
1. Deux lettres ne sont pas codées de la même façon et deux lettres différentes peuvent être codées par la même lettre. Il s'agit d'un chiffre poly-alphabétique.
2. Si A est la matrice identité, on retrouve un chiffre de Vigenère.
3. On peut généraliser à des matrices de tailles plus grandes ou plus petite : Si A est une matrice carrée de taille 1, on retrouve le chiffre affine.

Qu'en est-il de la fonction de déchiffrement ?

Rappelez-vous que le chiffrement affine $x \mapsto ax + b \mod 26$, $(a, b) \in \mathbb{Z}/26\mathbb{Z} \times \mathbb{Z}/26\mathbb{Z}$ est inversible si et seulement a est premier avec 26. Tous les a ne conviennent donc pas.

Ici, on a envie de dire que $\phi^{-1}\begin{pmatrix} x' \\ y' \end{pmatrix} = A^{-1}\begin{pmatrix} x' \\ y' \end{pmatrix} - b$. A quelle condition A^{-1} existe ?
Le calcul de l'inverse utilisant la commatrice (Proposition 5.1.2) est toujours valable dans un anneau :

$$A \cdot \mathrm{com}(A)^t = (\det A) I_n.$$

Cela signifie que si $\det A$ est inversible modulo 26, on a

$$(\det A)^{-1}\mathrm{com}(A)^t \cdot A = I_n$$

où $(\det A)^{-1}$ est l'inverse de $\det A$ modulo 26. Autrement dit, si $\det A$ est premier avec 26, A est inversible modulo 26 et son inverse est

$$A^{-1} = (\det A)^{-1}\mathrm{com}(A)^t.$$

Dans note exemple, $\det A = 3 - 10 = -7 = 19 \mod 26$ est inversible modulo 26 et son inverse est 11. Ainsi, dans $\mathbb{Z}/26\mathbb{Z}$:

$$\begin{aligned} A^{-1} &= 11 \cdot \begin{pmatrix} 3 & -5 \\ -2 & 1 \end{pmatrix}^t \\ &= 11 \begin{pmatrix} 3 & -2 \\ -5 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 7 & 4 \\ 23 & 11 \end{pmatrix} \mod 26, \end{aligned}$$

ce que l'on peut vérifier :

$$\begin{aligned} A \cdot A^{-1} &= \begin{pmatrix} 1 & 2 \\ 5 & 3 \end{pmatrix} \cdot \begin{pmatrix} 7 & 4 \\ 23 & 11 \end{pmatrix} \\ &= \begin{pmatrix} 53 & 26 \\ 104 & 53 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod 26. \end{aligned}$$

5.3 Déterminant et rang

Définition 5.3.1 Soit $A = (a_{i,j})_{\substack{1 \le i \le p \\ 1 \le j \le q}}$. Soit $I \subset \{1, \dots, p\}$ et $J \subset \{1, \dots, q\}$.
La matrice $B = (a_{i,j})_{\substack{i \in I \\ j \in J}}$ est appelée matrice extraite de A. On appelle déterminant extrait de A le déterminant d'une matrice carrée extraite de A.

Théorème 5.3.2 Soit $A = (a_{i,j})_{\substack{1 \le i \le p \\ 1 \le j \le q}}$ et r un entier, $1 \le r \le \min(p, q)$.
Alors rg $(A) \ge r$ si et seulement si il existe une matrice $B \in \mathcal{M}_r(\mathbb{K})$ extraite de A telle que $\det B \neq 0$.

Preuve : Si $B \in \mathcal{M}_r(\mathbb{K})$ est une matrice extraite de A telle que $\det B \neq 0$ alors les r colonnes de A extraites pour former B sont linéairement indépendantes et donc rg $(A) \ge r$.
Supposons que rg $(A) \ge r$. Alors on peut trouver r colonnes de A linéairement indépendantes, par exemple les r première $c_1, \dots, c_r$. On complète cette famille libre en une base $c_1, \dots, c_r, e'_{r+1}, \dots e'_n$ de $\mathbb{K}^n$ en choisissant les e'_i parmi les vecteurs de la base canonique. Alors en développant successivement $\det(c_1, \dots, c_r, e'_{r+1}, \dots, e'_n)$ par rapport à aux $n - r$ dernières colonnes, on extrait r lignes parmi des ligne de la matrice $(c_1, \dots, c_r)$ dont le déterminant est non nul. □

5.4 Orientation de l'espace

Dans cette partie, E est un $\mathbb{R}$ espace vectoriel. De plus, lorsque nous parlerons d'une base de E, l'ordre des vecteurs sera important : une base sera la donnée d'un n-uplet de vecteurs de E.
Si $(e_1, \dots, e_n)$ et $(e'_1, \dots, e'_n)$ sont deux base de E, alors $\det_{(e_j)}(e'_1, \dots, e'_n)$ est non nul, donc puisque c'est un réel, ce nombre est strictement positif ou strictement négatif.
On définit la relation suivante entre deux bases $(e_1, \dots, e_n)$ et $(e'_1, \dots, e'_n)$ de E : On dit que $(e_1, \dots, e_n)$ est équivalente à $(e'_1, \dots, e'_n)$ si

$$\det{}_{(e_j)}(e'_1, \dots, e'_n) > 0.$$

Cette relation est

- réflexive car $\det{}_{(e_j)}(e_1, \dots, e_n) = 1 > 0$.
- symétrique : Supposons que $\det{}_{(e_j)}(e'_1, \dots, e'_n) > 0$. Soit P la matrice de passage de $(e_1, \dots, e_n)$ à $(e'_1, \dots, e'_n)$. Alors

  $$\det P = \det{}_{(e_j)}(e'_1, \dots, e'_n) > 0,$$

  et

  $$\det P^{-1} = \det{}_{(e'_j)}(e_1, \dots, e_n) = \frac{1}{\det P} > 0.$$

— transitive : supposons que $\det_{(e_j)}(e'_1, \ldots, e'_n) > 0$ et $\det_{(e'_j)}(e''_1, \ldots, e''_n) > 0$. Soit P la matrice de passage de $(e_1, \ldots, e_n)$ à $(e'_1, \ldots, e'_n)$ et Q celle de $(e'_1, \ldots, e'_n)$ à $(e''_1, \ldots, e''_n)$. Alors PQ est la matrice de passage de $(e_1, \ldots, e_n)$ à $(e''_1, \ldots, e''_n)$ et $\det(PQ) = \det Q \det P > 0$.

Définition 5.4.1 Deux bases $(e_1, \ldots, e_n)$ et $(e'_1, \ldots, e'_n)$ ont même orientation si $\det_{(e_j)}(e'_1, \ldots, e'_n) > 0$. Avoir la même orientation est une relation d'équivalence sur les bases de E.