Algèbre générale et algèbre linéaire

Georges Skandalis

Université Paris Diderot (Paris 7) - IREM

Préparation à l'Agrégation Interne
Année 2013 – 2014

Table des matières

Première partie

Algèbre générale

1 Arithmétique dans $\mathbb{Z}$

1.1 Division dans $\mathbb{Z}$

1.1 Définition. Soient $a, b \in \mathbb{Z}$. On dit que a divise b et on écrit $a|b$ s'il existe $c \in \mathbb{Z}$ tel que $b = ac$.

On dit aussi que b est un multiple de a, que b est divisible par a, que a est un diviseur de b...

1.2 Propriétés élémentaires. a) Pour tout $a \in \mathbb{Z}$, on a : $1|a$, $a|a$ et $a|0$.

b) Pour tout $a, b \in \mathbb{Z}$, on a : $(a|b$ et $b|a) \iff |a| = |b|$.

c) Pour tout $a, b, c \in \mathbb{Z}$, on a : $(a|b$ et $b|c) \Rightarrow a|c$.

d) Pour tout $a, b, c \in \mathbb{Z}$, on a : $(a|b$ et $a|c) \Rightarrow a|b + c$.

1.3 Exercice. a) Soient $a, b, c, d \in \mathbb{Z}$. Démontrer que si $a|b$ et $c|d$ alors $ac|bd$.

b) Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}$. Démontrer que si $a|b$, alors $a^n|b^n$.

1.4 Théorème : Division euclidienne. *Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}$ non nul. Alors il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tels que $a = bq + r$ et $0 \leqslant r < b$.*

1.5 Définition. Un nombre $p \in \mathbb{Z}$ est dit *premier* s'il a exactement 4 diviseurs : $1, p, -1$ et $-p$.

En particulier, 1 (et -1) n'est pas (ne sont) pas premier(s).

1.6 Proposition. *Soit $n \in \mathbb{Z}$ un nombre distinct de 1 et de -1. Alors n admet un diviseur premier.*

Le plus petit diviseur strictement supérieur à 1 de n est un nombre premier.

1.7 Théorème. *Il y a une infinité de nombres premiers.*

Il suffit en effet de remarquer que tout diviseur premier de $n! + 1$ est $\geqslant n + 1$.

1.2 Sous-groupes additifs de $\mathbb{Z}$

1.8 Notation. Soit $a \in \mathbb{Z}$. L'ensemble des multiples de a, c'est à dire l'ensemble $\{ab;\ b \in \mathbb{Z}\}$ est noté $a\mathbb{Z}$.

1.9 Remarque. Pour $a, b \in \mathbb{Z}$ on a l'équivalence entre :

$$\text{(i) } a|b; \qquad \text{(ii) } b \in a\mathbb{Z} \qquad \text{et} \quad \text{(iii) } b\mathbb{Z} \subset a\mathbb{Z}.$$

D'après 1.2.a), on a $a\mathbb{Z} = b\mathbb{Z}$ si et seulement si $|a| = |b|$ (*i.e.* $b = \pm a$).

1.10 Proposition. *Pour tout $a \in \mathbb{Z}$, l'ensemble $a\mathbb{Z}$ est un sous-groupe additif de $\mathbb{Z}$. C'est le plus petit sous-groupe de $\mathbb{Z}$ contenant a.*

1.11 Théorème. *Tout sous-groupe de $\mathbb{Z}$ est de cette forme : si $G \subset \mathbb{Z}$ est un sous-groupe additif, il existe (un unique) $a \in \mathbb{N}$ tel que $G = a\mathbb{Z}$.*

1.3 PGCD, PPCM algorithme d'Euclide

1.12 Corollaire. *Soient $a, b \in \mathbb{Z}$.*

a) *Il existe un unique $m \in \mathbb{N}$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$. Le nombre m est un multiple commun de a et de b. Les multiples communs de a et b sont les multiples de m.*

b) *Il existe un unique $d \in \mathbb{N}$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Le nombre d est un diviseur commun de a et de b. Les diviseurs communs de a et b sont les diviseurs de d.*

1.13 Définition. Le nombre d de ce corollaire s'appelle le plus grand commun diviseur (PGCD) de a et b ; on le note $pgcd(a, b)$. Le nombre m de ce corollaire s'appelle le plus petit commun multiple (PPCM) de a et b ; on le note $ppcm(a, b)$.

1.14 Remarque. Soient $n \in \mathbb{N}^*$ et $x_1, \ldots, x_n \in \mathbb{Z}$. On définit de même le plus grand commun diviseur d et le plus petit commun multiple m de $x_1, \ldots, x_n$:

- Le nombre $m \in \mathbb{N}$ est un multiple commun des x_i ; les multiples communs des x_i sont les multiples de m. Autrement dit
$$m\mathbb{Z} = x_1\mathbb{Z} \cap x_2\mathbb{Z} \cap \ldots \cap x_n\mathbb{Z} = \bigcap_{i=1}^{n} x_i\mathbb{Z}.$$
- Le nombre $d \in \mathbb{N}$ est un diviseur commun des x_i ; les diviseurs communs des x_i sont les diviseurs de d. On a
$$d\mathbb{Z} = x_1\mathbb{Z} + x_2\mathbb{Z} + \ldots + x_n\mathbb{Z} = \sum_{i=1}^{n} x_i\mathbb{Z}.$$

1.15 Lemme. *Soient $a, b \in \mathbb{Z}$. On suppose que $b \neq 0$. On note r le reste de la division euclidienne de a par $|b|$. On a $pgcd(a, b) = pgcd(b, r)$.*

1.16 Algorithme d'Euclide. Soient $a, b \in \mathbb{N}$. On suppose que $b \neq 0$.

- On pose $r_0 = a$, $r_1 = b$ et on note r_2 le reste de la division euclidienne de a par b.
- Soit $n \in \mathbb{N}$ non nul et supposons r_j construits pour $1 \leqslant j \leqslant n$. Si r_n n'est pas nul, alors on définit r_{n+1} comme le reste de la division euclidienne de r_{n-1} par r_n : $r_{n-1} = q_n r_n + r_{n+1}$. Si r_n est nul, on arrête la construction.

a) La construction s'arrête en un nombre fini d'étapes.

b) Le PGCD de a et b est le dernier reste non nul.

1.17 Remarques. a) On peut majorer le nombre N d'étapes qu'il faut pour trouver le PGCD. Sachant que la suite r_k est strictement décroissante, on trouve évidemment $N \leqslant b$. Mais on peut faire bien mieux !

Remarquons que $r_{N-1} = q_N r_N \geqslant 2r_N$ (puisque et $0 \leqslant r_N < r_{N-1}$), et pour $1 \leqslant k \leqslant N-1$, on a $r_{k-1} = q_k r_k + r_{k+1} \geqslant r_k + r_{k+1}$, de sorte que, par récurrence, $r_{N-k} \geqslant r_N F_{k+2}$, où F_k est le k-ième nombre de Fibonacci (donné par récurrence par les formules $F_0 = 0$, $F_1 = 1$ et $F_{k+1} = F_k + F_{k-1}$ pour $k \geqslant 1$ - on initialise la récurrence avec $k = 0$ et 1 sachant que $F_2 = 1$ et $F_3 = 2$). Rappelons que F_k croît géométriquement : $F_k = \dfrac{\phi^k - (-1)^k \phi^{-k}}{\sqrt{5}}$ où $\phi = \dfrac{1+\sqrt{5}}{2}$ est le nombre d'or. On a donc $b = r_1 \geqslant F_{N+1} > \dfrac{\phi^{N+1} - 1}{\sqrt{5}}$ une estimation pour N logarithmique en b : $N < \dfrac{\ln(1 + b\sqrt{5})}{\ln \phi} - 1$.

On en déduit que le nombre de nombre N d'étapes nécessaires pour trouver le PGCD est inférieur ou égal à 5 fois le nombre de décimales de b (théorème de Lamé - *cf.* exerc. 1.8).

b) Pour écrire une relation de Bézout $d = r_N = au + bv$, on peut remonter les opérations : $r_N = r_{N-2} - r_{N-1}q_{N-1} = r_{N-2} - q_{N-1}(r_{N-3} - r_{N-2}q_{N-2}) = (1 + q_{N-1}q_{N-2})r_{N-2} - q_{N-1}r_{N-3}$, puis en écrivant $r_{N-2} = r_{N-4} - r_{N-3}q_{N-3}$ on exprime r_N en fonction de r_{N-3} et r_{N-4}, et on continue...

Cela demande de garder en mémoire la suite des quotients q_k.

On peut faire un peu mieux, en écrivant à chaque étape de l'algorithme $r_k = u_k a + v_k b$. On aura $r_{k+1} = r_{k-1} - q_k r_k = (u_{k-1} - q_k u_k)a + (v_{k-1} - q_k v_k)b$. En même temps qu'on trouvera le PGCD, on aura une relation de Bézout !

1.18 Quelques explications sur la suite de Fibonacci. Soient $a, b \in \mathbb{C}$. On considère les suites u_n qui satisfont une propriété de récurrence $u_{n+2} = au_{n+1} + bu_n$. Elles forment un sous-espace vectoriel E de l'espace $\mathbb{C}^{\mathbb{N}}$ des suites complexes. Comme une telle suite est entièrement déterminée par u_0 et u_1, cet espace vectoriel est de dimension 2 (l'application linéaire $(u) \mapsto (u_0, u_1)$ est un isomorphisme de E sur $\mathbb{C}^2$). On cherche une base de E de la forme $u_n = x^n$ (avec $x \in \mathbb{C}$). La suite (x^n) est dans E si et seulement si $x^2 = ax + b$. Si les racines r_1 et r_2 du polynôme $X^2 - aX - b$ sont distinctes, on obtient deux suites indépendantes r_1^n et r_2^n, donc toutes les solutions s'écrivent $u_n = \alpha r_1^n + \beta r_2^n$ (avec $\alpha, \beta \in \mathbb{C}$). Si $r_1 = r_2 = r$, on vérifie que $u_n = nr^n$ est aussi solution ; les solutions s'écrivent donc (si $r \neq 0$) $u_n = (\alpha + n\beta)r^n$ (avec $\alpha, \beta \in \mathbb{C}$).

Dans le cas de la suite de Fibonacci, $a = b = 1$ et les racines du polynôme $X^2 - X - 1$ sont ϕ et $-\phi^{-1}$ où ϕ est le nombre d'or. Donc $F_k = \alpha\phi^k + \beta(-1)^k\phi^{-k}$. On détermine α et β à l'aide des premiers termes.

1.4 Nombres premiers entre eux

1.19 Définition. On dit que a et b sont premiers entre eux si leur plus grand commun diviseur est 1.

Si $a, b \in \mathbb{Z}$, on peut écrire $a = a'd$ et $b = b'd$ où a' et b' sont premiers entre eux et d est le plus grand commun diviseur de a et b.

Soient $n \in \mathbb{N}^*$ et $x_1, \ldots, x_n$ des nombres entiers. On dit que les x_i sont *premiers entre eux dans leur ensemble* si le plus grand commun diviseur de $x_1, \ldots, x_n$ est 1 ; on dit que les x_i sont *premiers entre eux deux à deux*, si pour tout couple d'entiers i, j avec $1 \leqslant i < j \leqslant n$, les nombres x_i et x_j sont premiers entre eux.

1.20 Théorème de Bézout. *Soient $a, b \in \mathbb{Z}$. Alors a et b sont premiers entre eux si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que $au + bv = 1$.*

1.21 Théorème de Gauss. *Soient $a, b, c \in \mathbb{Z}$. Si a divise bc et est premier à b, alors a divise c.*

1.22 Corollaire. *Soient $a, b \in \mathbb{Z}$ et p un nombre premier. Si p divise ab alors p divise a ou b.*

1.23 Lemme. *Soient $p_1, \ldots, p_k \in \mathbb{N}$ des nombres premiers distincts deux à deux et $\beta_1, \ldots \beta_k \in \mathbb{N}^*$. Posons $n = \prod_{j=1}^{k} p_j^{\beta_j}$. L'ensemble des diviseurs premiers de n est $\{p_1, \ldots, p_k\}$ et pour tout j, $p_j^{\beta_j}$ divise n et $p_j^{\beta_j+1}$ ne divise pas n.*

1.24 Théorème. *Tout nombre entier admet une décomposition en produit de nombres premiers unique à permutation des termes près.*

On démontre l'existence à l'aide d'une « récurrence forte » sur n. L'unicité résulte du lemme.

1.5 Congruences, l'anneau $\mathbb{Z}/n\mathbb{Z}$

1.25 Définition. Soient $a, b, n \in \mathbb{Z}$. On dit que a est congru à b modulo n et on écrit $a \equiv b\ [n]$ si n divise $b - a$.

1.26 Proposition. *Soit $n \in \mathbb{Z}$. La relation de congruence modulo n est une relation d'équivalence.*

1.27 Lemme. *Soit p un nombre premier. Pour tout entier k tel que $1 \leqslant k \leqslant p - 1$ le coefficient binomial $\binom{p}{k}$ est divisible par p.*

On a $(p-k)\binom{p}{k} = p\binom{p-1}{k}$.

1.28 Petit théorème de Fermat. *Soit p un nombre premier. Pour tout entier k on a $k^p \equiv k\ [p]$. Si k n'est pas divisible par p, alors $k^{p-1} \equiv 1\ [p]$.*

1.29 Théorème de Wilson. *Pour tout nombre premier p, on a $(p-1)! \equiv -1\ [p]$.*

1.30 Définition. Soit $n \in \mathbb{Z}$. On note $\mathbb{Z}/n\mathbb{Z}$ le *quotient d'équivalence* pour la relation de congruence modulo n.

Pour $n \in \mathbb{N}^*$, on a $a \equiv b\ [n]$ si et seulement si a et b ont même reste dans la division euclidienne par n ; on en déduit que $\mathbb{Z}/n\mathbb{Z}$ a n éléments (autant que des restes possibles).

1.31 Proposition. *Soit $n \in \mathbb{Z}$. L'addition et la multiplication de $\mathbb{Z}$ passent au quotient et définissent une structure d'anneau sur $\mathbb{Z}/n\mathbb{Z}$.*

En d'autres termes, si $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$, alors $a + a' \equiv b + b'\ [n]$ et $aa' \equiv bb'\ [n]$.

1.32 Proposition. *Soit $n \in \mathbb{N}^*$. Les propriétés suivantes sont équivalentes.*

(i) *L'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps.*

(ii) *Le nombre n est premier.*

1.33 Proposition. *Soient $n \in \mathbb{Z}$. La classe d'un élément $a \in \mathbb{Z}$ est un élément inversible de l'anneau $\mathbb{Z}/n\mathbb{Z}$ si et seulement si a et n sont premiers entre eux.*

Pour $n \in \mathbb{N}^*$, le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est donc égal au nombre d'entiers $a \in [0, n-1]$ premiers à n. Ce nombre se note $\varphi(n)$. L'application φ ainsi construite s'appelle *l'indicatrice d'Euler.*

Soit p un nombre premier. Tout nombre non divisible par p est premier à p ; on a donc $\varphi(p) = p - 1$. Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$; alors a est premier avec p^n si et seulement si a est premier avec p, *i.e.* s'il n'est pas divisible par p. Les nombres $a \in [0, p^n - 1]$ divisibles par p sont les kp avec $0 \leqslant k < p^{n-1}$. Ils sont au nombre de p^{n-1}. Donc $\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}$.

1.34 Remarque. Soient $m, n \in \mathbb{Z}$ deux nombres entiers. On suppose que $m|n$. Pour $a, b \in \mathbb{Z}$, si $a \equiv b\ [n]$, alors *a fortiori* $a \equiv b\ [m]$. On définit une application naturelle $\pi_{m,n} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ qui à la classe de a modulo n associe sa classe modulo m. C'est clairement un homomorphisme d'anneaux.

1.35 Théorème « Chinois ». *Soient m, n deux nombres premiers entre eux. L'application*

$$\begin{array}{rcl} \mathbb{Z}/mn\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ a & \mapsto & (\pi_{m,mn}(a), \pi_{n,mn}(a)) \end{array}$$

est bijective ; c'est un isomorphisme d'anneaux.

En particulier, si m, n sont premiers entre eux on a $\varphi(mn) = \varphi(m)\varphi(n)$.

1.36 Proposition. *Soit $n \in \mathbb{N}$, $n \geqslant 2$. Notons $p_1, \ldots, p_k$ les nombres premiers (positifs et) distincts qui divisent n. On a $\varphi(n) = n \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right)$.*

1.37 Résolution générale de deux équations type. On va donner une méthode générale pour deux équations : un système de congruences et une équation diophantienne. Chacune de ces équations demande d'abord un calcul de plus grand commun diviseur et une « relation de Bézout ».

a) Résoudre l'équation de congruences : $x \equiv a\ [m]$ et $x \equiv b\ [n]$.

- **On suppose que m et n sont premiers entre eux.** Écrivons une relation de Bézout $mu + nv = 1$. Posons $x_0 = mub + nva$. Alors $x_0 - a = mub + (nv - 1)a = mub - mua$ est un multiple de m et $x_0 - b = (mu - 1)b + nva = nv(a - b)$ est un multiple de n. Notre équation devient
$$x \equiv x_0 \ [m] \ \text{ et } \ x \equiv x_0 \ [n],$$
qui est équivalente à $x \equiv x_0 \ [mn]$. L'ensemble de ses solutions est $\{x_0 + mnk;\ k \in \mathbb{Z}\}$.
- **Cas général.** Notons d le plus grand commun diviseur de m et n. Si x est solution de notre équation, comme d divise $x - a$ et $x - b$, alors $d|b - a$. Si a n'est pas congru à b modulo d, alors notre équation n'a pas de solution. Sinon, écrivons $b - a = \ell d$ et écrivons une relation de Bézout $mu + nv = d$. Posons $x_0 = a + \ell mu = a + \ell(d - nv) = b - n\ell v$. C'est une solution de notre équation. Notre équation devient
$$x \equiv x_0 \ [m] \ \text{ et } \ x \equiv x_0 \ [n],$$
qui est équivalente à $x \equiv x_0 \ [M]$ où $M = \dfrac{|mn|}{d}$ est le plus petit commun multiple de m et n. L'ensemble de ses solutions est $\{x_0 + Mk;\ k \in \mathbb{Z}\}$.

b) Résoudre l'équation diophantienne : $ax + by = c$.
On va supposer que a n'est pas nul. Notons d le plus grand commun diviseur de a et b. Écrivons $a = da'$ et $b = db'$ où a' et b' sont deux nombres premiers entre eux, et donnons une relation de Bézout $a'u + b'v = 1$. L'équation devient $d(a'x + b'y) = c$. Si c n'est pas multiple de d, il n'y a pas de solution. Sinon, écrivons $c = dc'$. L'équation devient $a'x + b'y = c' = c'(a'u + b'v)$, soit $a'(x - c'u) = b'(c'v - y)$. Si (x, y) est solution, alors a' divise $b'(c'v - y)$ et est premier avec b', donc il divise $c'v - y$. Écrivons $c'v - y = ka'$. On doit alors avoir : $a'(x - c'u) = a'b'k$, donc $x - c'u = b'k$. L'ensemble des solutions est contenu dans $\{(c'u + b'k, c'v - ka');\ k \in \mathbb{Z}\}$. On vérifie immédiatement que, inversement, pour tout $k \in \mathbb{Z}$, on a $a(c'u + b'k) + b(c'v - ka') = c$.

Remarquons que dans ces deux équations on a trouvé une *solution particulière* et résolu l'*équation homogène associée.* ***Pourquoi ?***

1.6 Exercices

1.6.1 Divisibilité et congruences

1.1 Exercice. 1. Soient $a, b, \delta \in \mathbb{Z}$. On suppose que δ est un diviseur commun de a et b et qu'il existe $u, v \in \mathbb{Z}$ tels que $\delta = au + bv$. Démontrer que le plus grand commun diviseur de a et b est $|\delta|$.

2. Soient $a, b, c \in \mathbb{N}$. Notons d et m le plus grand commun diviseur et le plus petit commun multiple de a et b. Démontrer que le plus grand commun diviseur de ac et bc est dc et que le plus petit commun multiple de ac et bc est mc.

3. Soient $a, b \in \mathbb{N}$. Démontrer que $dm = ab$ où l'on a noté d et m le plus grand commun diviseur et le plus petit commun multiple de a et b respectivement.

1.2 Exercice. 1. Soient $a, b, c \in \mathbb{Z}$. On suppose que a et b sont premiers entre eux, que $a|c$ et $b|c$. Démontrer que $ab|c$.

2. Soient $a, b, c \in \mathbb{Z}$. On suppose que a est premier à b et à c. Démontrer que a est premier à bc.

3. Soient $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$.

a) On suppose que a et b sont premiers entre eux. Démontrer que a et b^n sont premiers entre eux. En déduire que a^n et b^n sont premiers entre eux.

b) Démontrer que le plus grand commun diviseur de a^n et b^n est d^n où d est le plus grand commun diviseur de a et b.

4. Soient $a, b, c \in \mathbb{Z}$ tels que $a|bc$. Démontrer qu'il existe $d, e \in \mathbb{Z}$ tels que $a = de$ et $d|b$ et $e|c$.

1.3 Exercice. Quel est le reste de la division de $(n-1)!$ par n pour $n \geqslant 2$?

1.4 Exercice. (*Suggéré par Gentiana Danila*). Cent condamnés sont alignés en file indienne dans la cour de la prison. On leur met des chapeaux blancs ou noirs, mais aucun prisonnier ne connaît la couleur de son propre chapeau, ne voyant que la couleur de ceux qui sont devant lui dans la file. Il peut y avoir un nombre arbitraire de chapeaux blancs et noirs.

On s'apprête à exécuter les prisonniers, en leur laissant une chance d'être sauvés de la façon suivante. L'un après l'autre, chaque prisonnier doit annoncer sa couleur à voix haute (en commençant par celui qui voit tous les autres), et il n'est sauvé que s'il trouve juste.

Avant d'entrer dans la cour de la prison les prisonniers ont eu la possibilité de convenir d'une tactique pour annoncer les couleurs. Quel nombre maximal de prisonniers peuvent être sauvés de manière certaine, et par quelle stratégie ?

Commentaire. Les nombres p de prisoniers et le nombre d de couleurs est arbitraire ; dans l'énoncé c'est 2 mais après, par exemple pour une mise en pratique, on peut prendre 3 couleurs...

1.5 Exercice. *Propriétés arithmétiques à la base de RSA.*
Soient p, q deux nombres premiers distincts, on note N un multiple commun de $p-1$ et $q-1$. Soit $e \in \{1, \ldots, N\}$ un entier premier avec N.

1. Démontrer qu'il existe un entier $d \in \{1, \ldots, N\}$ tel que $ed \equiv 1[N]$.
2. En utilisant le théorème de Fermat, démontrer que pour tout entier n, $n^{ed} \equiv n[p]$ et $n^{ed} \equiv n[q]$.
3. En déduire que l'application $C : \{0, \ldots, pq-1\} \to \{0, \ldots, pq-1\}$ qui à a associe le reste dans la division de a^e par pq est une bijection de $\{0, \ldots, pq-1\}$ sur lui-même.

Sur le système de cryptage à clé appelé RSA (Ron Rivest, Adi Shamir, and Leonard Adleman, 1977) :
Je veux pouvoir recevoir des messages chiffrés de telle sorte que je serai seul à pouvoir les déchiffrer. Pour cela

- Je choisis deux nombres premiers p et q grands (environ 100 chiffres chacun), je calcule leur produit n que je rends public, ainsi que la clé de chiffrement e - un nombre premier à $(p-1)(q-1)$.
- Je calcule aussi un nombre d qui est inverse de e modulo $p-1$ et modulo $q-1$; ce nombre je suis le seul à le connaître, ainsi que les nombres p et q qui m'ont permis de le trouver.

Supposons maintenant que vous vouliez m'envoyer de façon secrète un message qui est un nombre a ayant à peu près 200 chiffres, c'est à dire grand mais inférieur à $n = pq$ (ou une suite a_i de tels nombres si votre message est long). Vous m'envoyez juste le nombre b qui est le reste de a^e dans la division par n (ou la suite des $b_i \equiv a_i^e$ modulo n). Pour retrouver le message d'origine, je n'aurai qu'à calculer le reste de b^d (ou b_i^d) modulo n. Ce système repose sur les faits suivants :

1. Il est « relativement rapide » de vérifier qu'un nombre est premier, et il y a beaucoup de nombres premiers : si je donne un nombre m de 100 chiffres au hasard, d'après le théorème des nombres premiers, le plus petit nombre premier $p > m$ a beaucoup de chances d'être tel que $p - m$ soit du même ordre que $\ln m \sim 100 \ln 10$. Donc je peux trouver des nombres premiers p et q « rapidement ».
2. Le nombre e est en général choisi petit ($e = 3, 5$ ou 7 sont des choix courants). Le nombre d est par contre grand (200 chiffres...). Élever à la puissance d modulo n un nombre x est cependant une opération « rapide » : cela implique d'élever des éléments de $\mathbb{Z}/n\mathbb{Z}$ au carré $\log_2 d$ ($\simeq 700$) fois et de multiplier des nombres par x au plus $\log_2 d$ fois.
3. Par contre, on ne sait pas trouver le nombre d connaissant n et e sans trouver p et q, et on ne sait pas trouver la décomposition $n = pq$ rapidement.

1.6 Exercice. *Équations Diophantiennes*
Soient $a, b \in \mathbb{N}^*$ des nombres entiers.

1. Soit $c \in \mathbb{Z}$. Quelles sont toutes les solutions de l'équation $ax + by = c$ avec $(x, y) \in \mathbb{Z}$?
   On suppose dorénavant que a et b sont premiers entre eux.
2. Quel est le plus petit entier qui s'écrit de deux façons sous la forme $ax + by$ avec $x, y \in \mathbb{N}$?
3. On suppose que a et b sont tous deux distincts de 1. Notons A l'ensemble des entiers naturels qui ne peuvent s'écrire sous la forme $ax + by$ avec $x, y \in \mathbb{N}$.
   a) Quel est le plus grand élément de A ?
   b) Démontrer que $A = \{|ua - vb|; (u, v) \in \mathbb{N}^2;\ 1 \leqslant u \leqslant b - 1;\ 1 \leqslant v \leqslant a - 1\}$.
   c) Combien d'éléments a A ?
4. Rappelons qu'au rugby un essai transformé vaut 7 points, un essai non transformé en vaut 5, un drop ou une pénalité 3.
   a) Quel est le plus grand score pour lequel on est sûr qu'il n'a pas été obtenu que par des essais - transformés ou non ?
   b) Quels sont les scores impossibles ?

1.7 Exercice. *Théorème Chinois.* Soient $a, b \in \mathbb{N}^*$. Posons $d = \text{pgcd}(a, b)$ et $m = \text{ppcm}(a, b)$.

1. Ecrire la décomposition de d et m en facteurs premiers en fonction de celle de a et de b. Comparer cette méthode de calcul de pgcd avec l'algorithme d'Euclide.
2. Démontrer qu'il existe a_1, a_2, b_1, b_2 tels que
   - $a = a_1a_2$, $b = b_1b_2$;
   - $a_1|b_1$, $b_2|a_2$;
   - a_2 et b_1 sont premiers entre eux.
3. Démontrer que $a_1b_2 = d$ et $a_2b_1 = m$.
4. En déduire que $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est isomorphe à $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

1.8 Exercice. Soient a, b des nombres entiers tels que $a > b > 0$. On suppose que l'algorithme d'Euclide (tel que décrit p. 2) comporte n étapes avec $n \geqslant 2$, c'est à dire $r_n > 0$ et $r_{n+1} = 0$.

Notons $F_k = \dfrac{\phi^k - (-1)^k\phi^{-k}}{\sqrt{5}}$ le k-ième nombre de Fibonacci, où $\phi = \dfrac{1 + \sqrt{5}}{2}$ est le nombre d'or.

1. Justifier que $r_n \geqslant 1 = F_2$ et $r_{n-1} \geqslant 2 = F_3$. Démontrer que pour tout entier k tel que $0 \leqslant i \leqslant n$, on a $r_{n-k} \geqslant F_{k+2}$.
2. Démontrer que $F_{k+1} \geqslant \phi^{k-1}$ pour tout $k \geqslant 0$.
3. Sachant que $\dfrac{\ln 10}{\ln \phi} < 5$ (on a $\dfrac{\ln 10}{\ln \phi} \simeq 4,78497$) en déduire que b a au moins $n/5$ chiffres (dans l'écriture en base 10).

1.9 Exercice. *Jouons avec la suite de Fibonacci.*

1. Écrire les premiers nombres de Fibonacci. Lesquels sont pairs ? multiples de 3 ? multiples de 5 ?
2. a) Démontrer que, si m divise n alors F_m divise F_n.
   b) Démontrer que pour tout n, l'ensemble des $k \in \mathbb{N}$ tel que n divise F_k est de la forme $a\mathbb{N}$ où $a \in \mathbb{N}^*$. *(Utiliser l'exercice 1.10.3).*
3. Soit $p \geqslant 7$ un nombre premier. Notons J la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ à coefficients dans $\mathbb{F}_p$.
   a) On suppose que 5 est un carré modulo p. Démontrer que la matrice J est diagonalisable (dans $\mathbb{F}_p$). En déduire que F_{p-1} est multiple de p.

b) (**) On suppose que 5 n'est pas un carré modulo p. Notons $K = \{aI_2 + bJ;\ a, b \in \mathbb{F}_p\}$. Démontrer que

(i) K est un sous-anneau commutatif de $M_2(\mathbb{F}_p)$;

(ii) l'anneau K est un corps ;

(iii) l'application $x \mapsto x^p$ est un automorphisme de K ;

(iv) pour $x \in K$ on a $x^p = x \iff x \in \{aI_2;\ a \in \mathbb{F}_p\}$;

(v) posant $J' = J^p$, on a $J' \neq J$ et $J'^2 = J' + 1$;

(vi) on a $J^p = -J^{-1}$;

(vii) p divise F_{p+1} ; de plus $F_p \equiv F_{p+2} \equiv -1 \ \ [p]$.

1.10 Exercice. *Algorithme d'Euclide et matrices* 2×2.
Soient $a, b \in \mathbb{N}$, avec $0 < a < b$. On effectue l'algorithme d'Euclide : on pose $r_0 = b,\ r_1 = a$, et, supposant r_{j-1} et r_j construits, si $r_j \neq 0$ on note $r_{j-1} = r_j q_j + r_{j+1}$ la division euclidienne de r_{j-1} par r_j. On note n l'entier pour lequel l'algorithme s'arrête de sorte que $r_{n+1} = 0$ et r_n est le $PGCD$ de a, b.

1. Démontrer que $q_n \geqslant 2$.
2. a) Démontrer que, pour tout $k \in \{1, \dots, n\}$, on a
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} \begin{pmatrix} r_{k+1} \\ r_k \end{pmatrix} = \begin{pmatrix} r_1 \\ r_0 \end{pmatrix}.$$
b) Démontrer qu'il existe des suites $(a_k)_{1 \leqslant k \leqslant n+1}$ et $(b_k)_{1 \leqslant k \leqslant n+1}$ de nombres entiers telles que pour $k \in \{1, \dots, n\}$ on ait
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} = \begin{pmatrix} a_k & a_{k+1} \\ b_k & b_{k+1} \end{pmatrix}.$$
c) Démontrer que $a_1 = 0,\ a_2 = 1,\ b_1 = 1,\ b_2 = q_1$ et, pour $2 \leqslant j \leqslant n$, on a $a_{j+1} = a_j q_j + a_{j-1}$ et $b_{j+1} = b_j q_j + b_{j-1}$. En déduire que les suites a_k et b_k sont croissantes et que l'on a $a_{n+1} \geqslant 2a_n$ et $b_{n+1} \geqslant 2b_n$. Dans quel cas a-t-on égalité dans l'une de ces inégalités ?
d) Démontrer que l'on a $a_k b_{k+1} - a_{k+1} b_k = (-1)^k$ pour $1 \leqslant k \leqslant n$.
e) Démontrer que l'on a une relation de Bézout $r_n = (-1)^n a_n b + (-1)^{n+1} b_n a$.
3. a) Démontrer que $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^k = \begin{pmatrix} F_{k-1} & F_k \\ F_k & F_{k+1} \end{pmatrix}$ où F_k est le k-ème nombre de Fibonacci.
b) Démontrer que $b_k \geqslant F_k$ et $a_k \geqslant F_{k-1}$.
4. Expliquer en quoi cette méthode permet de trouver « rapidement » le $PGCD$ de a et b et une identité de Bézout $d = au + bv$.
5. On suppose que a et b sont premiers entre eux. Démontrer qu'il existe $n \in \mathbb{N}^*$ une suite $q_1, \dots, q_n$ de nombres entiers strictement positifs et $u, v \in \mathbb{N}$ tels que $q_n \geqslant 2$ et
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} u & a \\ v & b \end{pmatrix}.$$
6. On suppose qu'il existe une suite $q_1, \dots, q_n$ de nombres entiers strictement positifs et $u, v \in \mathbb{N}$ tels que $q_n \geqslant 2$ et
$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} u & a \\ v & b \end{pmatrix}.$$
Démontrer que a et b sont premiers entre eux et que la suite des quotients successifs de la division euclidienne de b par a est $q_1, q_2, \dots, q_n$.

1.11 Exercice. *Algorithme de Cornacchia* (**)

1. Soient $a, b \in \mathbb{N}$ tels que $a < b$ et $a^2 + b^2$ soit un nombre premier p.
   a) Démontrer que a et b sont premiers entre eux.
   b) Démontrer qu'il existe $n \in \mathbb{N}^*$, des nombres entiers strictement positifs $q_1, \ldots, q_n$ avec $q_n \geqslant 2$ et des nombres $u, v \in \mathbb{N}$ tels que
   $$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} u & a \\ v & b \end{pmatrix}.$$
   c) Démontrer que $2u \leqslant a$ et $2v \leqslant b$.
   d) Démontrer que $\begin{pmatrix} u & v \\ a & b \end{pmatrix} \begin{pmatrix} u & a \\ v & b \end{pmatrix}$ s'écrit $\begin{pmatrix} x & \ell \\ \ell & p \end{pmatrix}$ où ℓ est l'unique entier tel que $\ell^2 \equiv -1\ [p]$ et $0 \leqslant \ell < p/2$.
2. Soit $p > 2$ un nombre premier tel que -1 est un carré modulo p (*i.e.* congru à 1 modulo 4 - voir exercice 1.14). Supposons qu'on ait trouvé ℓ tel que $0 \leqslant \ell < p/2$ et $\ell^2 = xp - 1$ avec $x \in \mathbb{N}$. Expliquer comment, grâce à l'algorithme d'Euclide, on trouve alors a et b tels que $a^2 + b^2 = p$.

1.6.2 Nombres premiers

1.12 Exercice. *Nombres de Fermat, nombres de Mersenne.*
Pour tout entier $n \geqslant 1$, on note $f_n = 2^n + 1$ et $M_n = 2^n - 1$.

1. Soit $n \geqslant 1$ un entier.
   Démontrer que si M_n est premier, alors n aussi, et que si f_n est premier alors n est une puissance de 2.

   Indication : Remarquer que, pour $a \in \mathbb{Z}$ et $k, m \in \mathbb{N}$, $a^k - 1$ divise $a^{km} - 1$ et, si m est impair $a^k + 1$ divise $a^{mk} + 1$.

   On pose $F_k = f_{2^k}$.
2. Soient k, ℓ deux nombres entiers avec $k < \ell$. Démontrer que $2^{2^\ell} \equiv 1[F_k]$. En déduire que F_k et F_ℓ sont premiers entre eux.
3. Soit $p > 2$ un nombre premier et soit q un diviseur premier de M_p. Quel est l'ordre de 2 dans le groupe $(\mathbb{F}_q^*, \cdot)$? En déduire que q est de la forme $2kp + 1$.
4. Démontrer que M_{13} est premier.
5. De même soit $\ell \in \mathbb{N}$ et q un diviseur premier de F_ℓ.
   a) Quel est l'ordre de 2 dans le groupe $(\mathbb{F}_q^*, \cdot)$?
   b) En déduire que q est de la forme $2^{\ell+1}k + 1$.
   c) On suppose que $\ell \geqslant 2$. Notons ω le classe de $2^{2^{\ell-2}}$ dans $\mathbb{F}_q$. Remarquant que $\omega^4 = -1$, démontrer que $2 = (\omega + \omega^{-1})^2$ est un carré modulo q. En déduire que $2^{\ell+2}$ divise $q - 1$.
   d) Démontrer que le plus petit diviseur de F_5 distinct de 1 est $\geqslant 641$.
   e) En remarquant que $641 = 5^4 + 2^4$, démontrer que $F_5 \equiv 1 - 5^4 2^{28}\ \ [641]$.
   f) Démontrer que $641 | F_5$.

1.13 Exercice. *Cas du théorème de Dirichlet.* (*cf.* Combes. *Algèbre et géométrie* 12.6).

Théorème de Dirichlet. *Soient $a, b \in \mathbb{N}^*$ premiers entre eux. Il y a une infinité de nombres premiers congrus à a modulo b.*

Nous étudions ici le cas où $a = 1$.

Le cas $b = 4$ **:** Soit $a \in \mathbb{N}$ et p un diviseur premier de $a^2 + 1$ distinct de 2.

1. Démontrer que a et p sont premiers entre eux.
2. On note x la classe de a dans $\mathbb{F}_p$. Démontrer que $x^4 = 1$.
3. Démontrer que $x^2 \neq 1$.
4. En déduire que p est congru à 1 modulo 4.
5. En prenant a sous-la forme $n!$, démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.
6. Démontrer que, pour $n \geqslant 4$, $n! - 1$ a au moins un diviseur premier congru à 3 modulo 4. En déduire qu'il existe une infinité de nombres premiers congrus à 3 modulo 4.

Le cas $b = 6$ Soit $a \in \mathbb{N}$ et p un diviseur premier de $a^2 + a + 1$ distinct de 3.

1. Démontrer que a et p sont premiers entre eux.
2. On note x la classe de a dans $\mathbb{F}_p$. Démontrer que $x^3 = 1$.
3. Démontrer que $x \neq 1$.
4. En déduire que p est congru à 1 modulo 3.
5. En prenant a sous-la forme $n!$, démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 6.
6. Démontrer que, pour $n \geqslant 3$, $n! - 1$ a au moins un diviseur premier congru à 5 modulo 6. En déduire qu'il existe une infinité de nombres premiers congrus à 5 modulo 6.

Le cas $b = 12$ **:** Soit $a \in \mathbb{N}$ et p un diviseur premier de $a^4 - a^2 + 1$.

1. Démontrer que $p \neq 2$ et $p \neq 3$. Démontrer que a et p sont premiers entre eux.
2. On note x la classe de a dans $\mathbb{F}_p$. Démontrer que $x^{12} = 1$.
3. Démontrer que $x^4 \neq 1$ et $x^6 \neq 1$.
4. En déduire que p est congru à 1 modulo 12.
5. En prenant a sous-la forme $n!$, démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo 12.

Le cas général [**] Pour $n \in \mathbb{N}^*$, on note Φ_n le n-ième polynôme cyclotomique : $\Phi_n = \prod_{0 \leqslant k < n;\ k \wedge n = 1} X - e^{\frac{2ik\pi}{n}}$. Rappelons que $\Phi_n \in \mathbb{Z}[X]$ et que l'on a l'égalité $X^n - 1 = \prod_{d|n} \Phi_d$.
Soient $n \in \mathbb{N}$, $n \geqslant 2$, $a \in \mathbb{N}$ un multiple de n et p un diviseur premier de $\Phi_n(a)$.

1. Démontrer que $\Phi_n(0) = 1$. En déduire que a et p sont premiers entre eux.
2. On note x la classe de a dans $\mathbb{F}_p$. Démontrer que $x^n = 1$.
3. Démontrer que le polynôme $X^n - 1$ n'a pas de facteur carré dans $\mathbb{F}_p[X]$.

   Indication : Utiliser la dérivée
4. Soit $d \in \mathbb{N}$ un diviseur de n distinct de n. Démontrer que les polynômes $X^d - 1$ et Φ_n sont premiers entre eux dans $\mathbb{F}_p[X]$. En déduire que $x^d \neq 1$.
5. En déduire que p est congru à 1 modulo n.
6. En prenant a sous-la forme $N!$, démontrer qu'il existe une infinité de nombres premiers congrus à 1 modulo n.

1.14 Exercice. *Carrés dans* $\mathbb{F}_p$. (*cf.* Combes p. 267)
Soit p un nombre premier distinct de 2. Notons $C \subset \mathbb{F}_p^*$ l'ensemble des carrés, *i.e.* l'ensemble des $x \in \mathbb{F}_p^*$ tels qu'il existe $y \in \mathbb{F}_p^*$ avec $x = y^2$.

1. Le cas de -1.

a) Démontrer que pour tout $x \in C$ il existe un et un seul $c \in \left\{1, \ldots, \frac{p-1}{2}\right\}$ tel que x soit la classe de c^2. Combien y a-t-il de carrés dans F_p^* ?

b) Démontrer que tout $x \in C$, on a $x^{\frac{p-1}{2}} = 1$.

c) En déduire que, pour $x \in \mathbb{F}_p^*$, on a $x \in C \iff x^{\frac{p-1}{2}} = 1$.

d) Démontrer que -1 est un carré modulo p si et seulement si p est congru à 1 modulo 4.

2. Le cas de 3.

a) Soit $P = X^2 + aX + b$ un polynôme à coefficients dans $\mathbb{F}_p$. Démontrer que P a une racine dans $\mathbb{F}_p$ si et seulement si $a^2 - 4b$ est un carré (*i.e.* $a^2 - 4b \in \{0\} \cup C$).

b) On suppose que $p \notin \{2, 3\}$. Démontrer l'équivalence entre

(i) $-3 \in C$.

(ii) Il existe $x \in \mathbb{F}_p^*$, $x^2 + x + 1 = 0$.

(iii) Il existe x d'ordre 3 dans le groupe $\mathbb{F}_p^*$.

(iv) $p \equiv 1$ [3] (ce qui signifie encore $p \equiv 1$ [6]).

3. Le polynôme $X^4 + 1$.

a) Démontrer que si $a, b \in \mathbb{F}_p^* \setminus C$, alors $ab \in C$.

b) En déduire qu'un au moins des éléments $-1, 2, -2$ est un carré dans $\mathbb{F}_p$.

c) En écrivant $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - 1)^2 + 2X^2$ en déduire que pour tout p le polynôme $X^4 + 1$ n'est pas irréductible dans $\mathbb{F}_p[X]$.

d) Quelle est la décomposition dans $\mathbb{R}[X]$ du polynôme $X^4 + 1$ en polynômes irréductibles ?

e) En déduire que $X^4 + 1$ est irréductible sur $\mathbb{Q}$ (et sur $\mathbb{Z}$).

1.15 Exercice. *Réciprocité quadratique pour* 2*, pour* 5.
Soit p un nombre premier.

1. Soit L un corps commutatif de caractéristique p, autrement dit une extension de $\mathbb{F}_p$.

a) Démontrer que $x \mapsto x^p$ est un endomorphisme de corps de L.

b) Quelles sont les racines du polynôme $X^p - X$ dans L ?

2. On suppose que p est distinct de 2. Soit L une extension de $\mathbb{F}_p$ et $\omega \in L$ tel que $\omega^4 = -1$. Une telle extension existe d'après le corollaire 3.18. Posons $x = \omega + \omega^{-1}$.

a) Démontrer que $\omega^2 + \omega^{-2} = 0$ et $x^2 = 2$.

b) Démontrer que les assertions suivantes sont équivalentes :

(i) Il existe $y \in \mathbb{F}_p$ tel que $y^2 = 2$.

(ii) $x \in \mathbb{F}_p$;

(iii) $x^p = x$;

(iv) $\omega^p = \omega$ ou $\omega^p = \omega^{-1}$;

(v) $p \equiv \pm 1$ [8] ;

3. On suppose que p est distinct de 2 et de 5. Soit L une extension de $\mathbb{F}_p$ et $\omega \in L$ tel que $\omega^5 = 1$ et $\omega \neq 1$ (*i.e.* une racine du polynôme $1 + X + X^2 + X^3 + X^4$ - une telle extension L existe d'après le corollaire 3.18). Posons $x = \omega + \omega^{-1}$.

a) Démontrer que $\omega^2 + \omega^{-2} = -1 - x$ et $x^2 + x - 1 = 0$.

b) Démontrer que les assertions suivantes sont équivalentes :

(i) Il existe $y \in \mathbb{F}_p$ tel que $y^2 = 5$.

(ii) $x \in \mathbb{F}_p$;

(iii) $x^p = x$;

(iv) $\omega^p = \omega$ ou $\omega^p = \omega^{-1}$;

(v) $p \equiv \pm 1$ [5] ;

(vi) La classe de p est un carré modulo 5.

1.16 Exercice. *Racine carrée de -1 dans $\mathbb{F}_p$.*

Soit p un (grand !) nombre premier. Soit $x \in \mathbb{F}_p^*$.

1. Démontrer que x est un carré dans $\mathbb{F}_p$ si et seulement si $x^{(p-1)/2} = 1$. *(Voir exercice 1.14).*
   On suppose que x est un carré et on veut trouver une racine carrée de x.
2. On suppose que $p \equiv 3$ [4]. Démontrer que, si x est un carré, alors $x^{\frac{p+1}{4}}$ est une racine carrée de x.
3. On suppose que $p \equiv 1$ [4] et on cherche une racine carrée de -1. On écrit $p - 1 = 2^\ell u$ avec u entier impair.
   a) Soit $a \in \mathbb{F}_p^*$; posons $b = a^u$. Démontrer que b est d'ordre 2^k avec $0 \leqslant k \leqslant \ell$.
   b) En choisissant a au hasard, quelle est la probabilité que $b = \pm 1$?
   c) Expliquer comment trouver une racine carrée de -1 si $b \neq \pm 1$.

1.17 Exercice. 1. *Les nombres premiers sont espacés.* Démontrer que pour tout $n \in \mathbb{N}$, il existe une suite de n nombres consécutifs non premiers (*i.e.* il existe $a \in \mathbb{N}$ tel que les nombres entiers k avec $a \leqslant k \leqslant a + n - 1$ ne soient pas premiers).

2. *Il y a beaucoup de nombres premiers.* On désigne par $(p_n)_{n \geqslant 1}$ la suite ordonnée des nombres premiers. On veut démontrer que la série $\displaystyle\sum_{n=1}^{+\infty} 1/p_n$ diverge.

   On suit Combes (p. 269).
   Soit $k \in \mathbb{N}$. Notons $A_k \subset \mathbb{N}^*$ l'ensemble des nombres entiers dont tous les diviseurs premiers sont $\leqslant p_k$.

   a) Démontrer que tout $a \in A_k$ s'écrit sous la forme $a = b^2 p_1^{\varepsilon_1} \dots p_k^{\varepsilon_k}$ avec $b \in \mathbb{N}$ et $\varepsilon_j \in \{0, 1\}$. En déduire que, pour tout $x \in \mathbb{N}^*$, le nombre d'éléments de A_k inférieurs à x est $\leqslant \sqrt{x} 2^k$.

   b) Démontrer que, pour $x \in \mathbb{N}^*$, la proportion d'éléments $\mathbb{N} \setminus A_k$ dans $[1, x]$ est plus petite que $\displaystyle\sum_{p \in \mathcal{P},\ p_k < p \leqslant x} 1/p$.

   c) Démontrer que pour $x = 4^{k+1}$ on a $\displaystyle\sum_{p \in \mathcal{P},\ p_k < p \leqslant x} 1/p \geqslant 1/2$. En déduire que la série $\displaystyle\sum_{n=1}^{+\infty} 1/p_n$ diverge.

3. a) Démontrer que pour tout entier $k \geqslant 1$, $\displaystyle\prod_{i=1}^{k} \frac{p_i}{p_i - 1} \geqslant \sum_{i=1}^{k} \frac{1}{i}$.

   b) En déduire que $\displaystyle\sum_{k=1}^{+\infty} \frac{1}{p_k}$ diverge.

4. Démontrer qu'il existe une infinité de nombres premiers comportant au moins un 9 dans leur développement décimal.

D'après le théorème des nombres premiers, $\pi(x)$ est équivalent à $\dfrac{x}{\ln x}$. Les inégalités de Tchebychef, ci-dessous s'approchent de cet équivalent.

1.18 Exercice. *Inégalités de Tchebychef*

1. Pour $N \in \mathbb{Z}^*$ et un nombre premier p, on appelle *valuation* p-adique de N et on note $v_p(N)$ le plus grand entier k tel que $p^k | N$ - de sorte que l'on a $|N| = \prod_p p^{v_p(N)}$.

   Soient $n \in \mathbb{N}$, $n \geqslant 3$ et p un nombre premier.

   a) Démontrer que l'on a $v_p(n!) = \sum_{k=1}^{+\infty} E\big(np^{-k}\big)$ (où E désigne la partie entière).

   b) En déduire que $v_p\binom{2n}{n}$ est le nombre de $k \in \mathbb{N}$ tel que $E\big(2np^{-k}\big)$ soit impair.

   c) Démontrer que
   - $v_p\binom{2n}{n} \leqslant \dfrac{\ln 2n}{\ln p}$.
   - Si $n < p \leqslant 2n$ alors $v_p\binom{2n}{n} = 1$.
   - Si $p \leqslant n < \dfrac{3p}{2}$ alors $v_p\binom{2n}{n} = 0$.

   d) Démontrer que l'on a :

   (i) $\ln\binom{2n}{n} \geqslant \sum_{n \leqslant p \leqslant 2n;\ p \text{ premier}} \ln p$.

   (ii) $\ln\binom{2n}{n} \leqslant (\ln 2n)\Big(\pi(2n/3) + \pi(2n) - \pi(n)\Big) \leqslant (\ln 2n)\pi(2n)$.

2. Soit $n \in \mathbb{N}^*$. Démontrer que $\sum_{k=0}^{n-1}\binom{2n-1}{k} = 2^{2n-2}$. En déduire que $\dfrac{2^{2n-2}}{n} \leqslant \binom{2n-1}{n-1} \leqslant 2^{2n-2}$, puis que $\dfrac{2^{2n-1}}{n} \leqslant \binom{2n}{n} \leqslant 2^{2n-1}$.

3. Démontrer que, pour tout $n \in \mathbb{N}$, $n > 2$, on a

   a) $\sum_{n < p \leqslant 2n;\ p \text{ premier}} \ln p \leqslant (n-1)\ln 4$ et en déduire que $\sum_{p \leqslant n;\ p \text{ premier}} \ln p \leqslant (n-1)\ln 4$.

   b) $\pi(n) \geqslant \dfrac{n(\ln 2)}{\ln n} - 1$.

2 Anneaux

2.1 Généralités

2.1 Définition. Un anneau est un ensemble A muni de deux lois : la première s'appelle en général l'addition et est notée $+$; la deuxième s'appelle en général la multiplication et est notée $(x, y) \mapsto xy$. On suppose que :

- Muni de l'addition A est un groupe abélien ; son élément neutre est noté en général 0 ou 0_A en cas d'ambiguïté ; le symétrique d'un élément $x \in A$ pour $+$ s'appelle l'opposé de x et se note $-x$.
- La multiplication est associative et possède un élément neutre, en général noté 1 ou 1_A en cas d'ambiguïté.
- La multiplication est distributive par rapport à l'addition : pour tout $a, b, c \in A$, on a $a(b+c) = ab+ac$ et $(a + b)c = ac + bc$.
  Lorsque la multiplication est aussi commutative, on dit que l'anneau A est abélien ou commutatif.

2.2 Exemples. a) Munis des opérations (addition et multiplication) usuelles, les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sont des anneaux commutatifs, ainsi que l'anneau $K[X]$ des polynômes sur un corps (ou un anneau) commutatif K.

b) L'ensemble des matrices carrées de taille n à coefficients dans $\mathbb{R}$, muni de l'addition et de la multiplication des matrices est un anneau non commutatif pour $n \geqslant 2$.

Si A et B sont deux anneaux, une application $f : A \to B$ est appelée un *homomorphisme (ou morphisme) d'anneaux* si pour tout $x, y \in A$ on a $f(x + y) = f(x) + f(y)$ et $f(xy) = f(x)f(y)$ et si $f(1_A) = 1_B$. (Remarquons qu'on a automatiquement $f(0_A) = 0_B$).

Soient A un anneau et $x \in A$. On définit nx pour $n \in \mathbb{Z}$ en posant $0x = 0$, $1x = x$, puis, pour tout $n \in \mathbb{N}$, $(n + 1)x = (nx) + x$; enfin pour n négatif $nx = -\big((-n)x\big)$. L'application $n \mapsto nx$ est un homomorphisme d'anneaux de $\mathbb{Z}$ dans A.

L'élément $n1_A$ se note parfois n même lorsque cet homomorphisme n'est pas injectif.

On définit de même x^n pour $x \in A$ et $n \in \mathbb{N}$: on pose $x^0 = 1_A$, $x^1 = x$ puis $x^{n+1} = x^n x (= xx^n)$.

2.3 Formule du binôme. Soient A un anneau et $a, b \in A$ deux éléments *permutables* - *i.e.* tels que $ab = ba$. Alors, pour tout $n \in \mathbb{N}$, on a

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

C'est faux si $ab \neq ba$. Par exemple $(a + b)^2 = a^2 + ab + ba + b^2 \neq a^2 + 2ab + b^2$.

2.4 Définition. Soit A un anneau. Un élément $a \in A$ est dit *inversible* (on dit parfois une unité de A) s'il existe a' dans A (nécessairement unique) tel que $a'a = aa' = 1_A$. Si a est inversible, l'élément a' tel que $a'a = aa' = 1_A$ s'appelle l'inverse de a et se note a^{-1}.

2.5 Proposition. *L'ensemble (noté parfois A^{-1}) des éléments inversibles de A est un groupe pour la multiplication.*

2.6 Définition. Un corps est un anneau K tel que $K^{-1} = K - \{0_K\}$.

2.7 Exercice. Soient A un anneau et $a \in A$. Démontrer que a est inversible si et seulement si l'application $b \mapsto ab$ est bijective de A dans A.

2.2 Anneaux intègres ; anneaux principaux

Dans la suite, tous les anneaux seront supposés commutatifs.

2.8 Définition. On dit qu'un anneau commutatif A est *intègre* si le produit de deux éléments non nuls de A est non nul.

2.9 Division ; éléments associés. Dans un anneau commutatif intègre, on peut définir la divisibilité comme dans $\mathbb{Z}$. On dit que a divise b et on écrit $a|b$ s'il existe c (*nécessairement unique* si a n'est pas nul) tel que $b = ac$. Autrement dit $a|b$ si $b \in aA$.

On dira que deux éléments a et b de A sont *associés* si $a|b$ et $b|a$, c'est à dire s'il existe $u \in A$ inversible tel que $a = ub$.

Le sous-ensemble aA de A est un sous-groupe de A. Mais contrairement au cas de $\mathbb{Z}$, les sous-groupes de A sont loin d'être en général tous de cette forme.

2.10 Définition. Soit A un anneau commutatif. On appelle *idéal* de A une partie I de A qui est un sous-groupe de $(A, +)$ et telle que, pour tout $a \in A$ et tout $x \in I$ on ait $ax \in I$.

A un idéal on peut encore associer une relation d'équivalence et définir un anneau quotient :

2.11 Proposition. *Soient A un anneau commutatif et I un idéal dans A. La relation R définie sur A par $a\,R\,b$ si $b - a \in I$ est une relation d'équivalence.*

2.12 Définition. Soient A un anneau commutatif et I un idéal dans A. On note A/I le *quotient d'équivalence* pour la relation R.

2.13 Proposition. *Soient A un anneau commutatif et I un idéal dans A. L'addition et la multiplication de A passent au quotient et définissent une structure d'anneau sur A/I.*

En effet, si $a, b \in A$ et $x, y \in I$, alors $(a+x)+(b+y)\,R\,a+b$ et $(a+x)(b+y) = ab+(ay+x(b+y))\,R\,ab$.

2.14 A retenir. a) Si I est un idéal d'un anneau (commutatif) A, on peut construire un anneau A/I et un homomorphisme surjectif d'anneaux $\pi : A \to A/I$ de noyau I.

b) Inversement, le noyau d'un homomorphisme d'anneaux $\pi : A \to B$ est un idéal.

Pour $a \in A$, l'ensemble aA est un idéal de A. On l'appelle l'idéal principal associé à a.

2.15 Définition. On dit qu'un anneau commutatif est *principal* s'il est intègre et tous ses idéaux sont principaux.

Un idéal étant en particulier un sous-groupe, l'anneau $\mathbb{Z}$ est principal. Nous verrons que si K est un corps commutatif, l'anneau $K[X]$ des polynômes à coefficients dans K est aussi un anneau principal. D'autres exemples d'anneaux principaux et d'anneaux intègres non principaux seront donnés dans les exercices 2.5, 2.7, 2.8.

Dans un anneau principal, la division se comporte essentiellement comme dans $\mathbb{Z}$.

2.16 Théorème. *Soient A un anneau principal et $a, b \in A$.*

a) *Il existe un élément $m \in A$ tel que $aA \cap bA = mA$. L'élément m est un multiple commun de a et de b. Les multiples communs de a et b sont les multiples de m.*

b) *Il existe un élément $d \in A$ tel que $aA + bA = dA$. L'élément d est un diviseur commun de a et de b. Les diviseurs communs de a et b sont les diviseurs de d.*

2.17 Définition. L'élément d de ce théorème s'appelle un plus grand commun diviseur (PGCD) de a et b. L'élément m s'appelle un plus petit commun multiple (PPCM) de a et b.

Un *PGCD* de a et de b n'est en général pas unique : il est unique à multiplication par un élément inversible de A près. On a fait un choix dans $\mathbb{Z}$ en les prenant dans $\mathbb{N}$ ce qui les a rendus uniques. On fait un tel choix aussi dans $K[X]$, mais il n'y a pas en général un choix « meilleur que les autres ».

Comme dans le cas de $\mathbb{Z}$, on peut définir la notion d'éléments premiers entre eux : leurs seuls diviseurs communs sont les éléments inversibles. Alors 1_A est un PGCD, *i.e.* $aA+bA = A$. On a donc le théorème de Bézout dans ce cadre, dont découle le théorème de Gauss :

2.18 Théorème de Bézout. *Soit A un anneau principal. Soient $a, b \in A$. Alors a et b sont premiers entre eux si et seulement s'il existe $u, v \in A$ tels que $au + bv = 1$.*

2.19 Théorème de Gauss. *Soit A un anneau principal. Soient $a, b, c \in A$. Si a divise bc et est premier à b, alors a divise c.*

Le rôle des nombres premiers est ici joué par les éléments irréductibles.

2.20 Définition. Soit A un anneau intègre. Un élément $a \in A$ est dit *irréductible* s'il n'est pas inversible et dans toute décomposition $a = bc$ un des deux facteurs b ou c est inversible.

2.21 Proposition. *Soient A un anneau principal et $a \in A$ non nul. Alors a est irréductible si et seulement si l'anneau quotient A/aA est un corps.*

Pour établir la décomposition en produit d'éléments irréductibles 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. Nous esquissons une preuve ci-dessous :

2.22 Lemme. a) *Soit A un anneau principal. Toute suite croissante d'idéaux de A stationne.*

b) *Toute suite décroissante d'idéaux d'intersection non nulle stationne.*

Démonstration. Soit I_n une suite d'idéaux de A.

a) On suppose que la suite I_n est croissante, c'est à dire que, pour $k, \ell \in \mathbb{N}$ avec $k \leqslant \ell$, on a $I_k \subset I_\ell$. On veut démontrer qu'il existe n tel que, pour $k \geqslant n$ on a $I_k = I_n$.
Comme la suite (I_n) est croissante, on vérifie que la réunion des I_n est un idéal J de A.
Puisque A est principal, il existe $a \in A$ tel que $J = aA$. Alors $a \in J$ et il existe $n \in \mathbb{N}$ tel que $a \in I_n$ (par définition d'une réunion). On a alors $J = aA \subset I_n$ donc $J = I_n$ (puisque J est la réunion de I_k). Pour $k \geqslant n$, on a $I_n \subset I_k \subset J = I_n$.

b) On suppose que la suite I_n est décroissante, c'est à dire que, pour $k, \ell \in \mathbb{N}$ avec $k \leqslant \ell$, on a $I_k \supset I_\ell$. Soit a un élément non nul de l'intersection $\bigcap_{k\in\mathbb{N}} I_k$. Pour $k \in \mathbb{N}$, il existe b_k tel que $I_k = b_k A$ (A étant principal). Comme $a \in I_k$, il existe $c_k \in A$ tel que $b_k c_k = a$. Posons $J_k = c_k A$. Pour $k \leqslant \ell$, on a $I_k \supset I_\ell$, de sorte que $b_\ell \in I_k$: il existe $x \in A$ tel que $b_\ell = x b_k$. Comme $b_k c_k = a = b_\ell c_\ell$, il vient $c_k = x c_\ell$, soit $c_k \in J_\ell$. La suite J_k est croissante, donc stationne d'après a). Il existe donc n tel que, pour $k \geqslant n$ on ait $J_k = J_n$. Pour $k \geqslant n$, on a $c_k \in J_n$, donc il existe $y \in A$ tel que $c_k = y c_n$; comme $b_k c_k = a = b_n c_n$ il vient $b_n = y b_k$, donc $I_n \subset I_k$, et l'on a l'égalité.

□

2.23 Théorème. *Soient A un anneau principal et $a \in A$ un élément non nul et non inversible.*

a) *Il existe un élément irréductible $p \in A$ tel que $p|a$.*

b) *Il existe un ensemble fini F d'éléments irréductibles de A tels que tout élément irréductible de A qui divise a est associé à un élément de F ; pour tout irréductible p, il existe $n \in \mathbb{N}$ tel que $p^n \not| a$.*

Une fois ce théorème établi, on en déduit immédiatement l'existence de la décomposition en facteurs irréductibles. L'unicité est plus difficile à énoncer mais se démontre comme dans le cas de $\mathbb{Z}$:

2.24 Théorème. *Soient A un anneau principal et $a \in A$ un élément non nul et non inversible. Il existe un entier $n \geqslant 1$ et des éléments irréductibles $p_1, \ldots, p_n \in A$ tels que $a = \prod_{j=1}^{n} p_j$. Cette décomposition est unique à l'ordre des facteurs près : si $a = \prod_{j=1}^{n} p_j = \prod_{j=1}^{m} q_j$, alors $n = m$ et il existe $\sigma \in \mathfrak{S}_n$, i.e. une bijection $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ telle que p_j soit associé à $q_{\sigma(j)}$ (pour tout j).*

2.3 Anneaux euclidiens

Les anneaux euclidiens sont ceux pour lesquels on dispose d'une division euclidienne. La même preuve que pour $\mathbb{Z}$ démontre qu'ils sont principaux. De plus, dans un anneau euclidien, comme dans $\mathbb{Z}$, on peut calculer le PGCD, écrire une relation de Bézout, résoudre des équations diophantiennes ou de congruence, *etc.* de façon algorithmique.

2.25 Définition. Soit A un anneau commutatif et intègre. On dit que A est *euclidien* s'il existe une application $v : A - \{0\} \to \mathbb{N}$, - appelée *stathme euclidien* telle que pour tous $a, b \in A - \{0\}$ il existe $q, r \in A$ tels que $a = bq + r$ et $r = 0$ ou $v(r) < v(b)$.

2.26 Remarque. En général, on demande de plus que, pour tous $a, b \in A - \{0\}$ tels que $a|b$ on ait $v(a) \leqslant v(b)$. Cette condition est en pratique toujours vérifiée, mais n'est pas utile dans ce qui suit. On peut démontrer que si A possède un stathme qui ne vérifie pas cette propriété, il en possède un qui la vérifie.

L'anneau $\mathbb{Z}$ est euclidien de stathme $a \mapsto |a|$. Nous verrons plus bas que l'anneau $K[X]$ est aussi euclidien : l'application qui à un polynôme associe son degré est un stathme euclidien sur $K[X]$.

2.27 Théorème. *Tout anneau euclidien est principal.*

Démonstration. Soit A un anneau euclidien ; notons v son stathme. Soit I un idéal non nul de A et $a \in I - \{0\}$ tel que $v(a) = \inf\{v(x);\ x \in I - \{0\}\}$. Puisque $a \in I$, on a $aA \subset I$. Soit x un élément de I ; écrivons $x = aq + r$, avec $q, r \in A$ et $r = 0$ ou $r \neq 0$ et $v(r) < v(a)$. Or $r = x - aq \in I$, et on ne peut avoir $r \neq 0$ et $v(r) < v(a)$ par définition de a. Il vient $r = 0$, donc $x \in aA$. Cela prouve que $I = aA$. □

2.28 Remarque. Dans un anneau euclidien, comme pour le cas de $\mathbb{Z}$, on dispose de l'*algorithme d'Euclide* qui permet de calculer en pratique le plus grand commun diviseur de deux éléments.

2.4 Un exemple

Nous allons développer ici assez en détail une famille d'anneaux.

Soit $\tau \in \mathbb{C} - \mathbb{R}$ un entier quadratique, *i.e.* tel qu'il existe $a, b \in \mathbb{Z}$ avec $\tau^2 + a\tau + b = 0$. Il est alors immédiat que l'ensemble $\mathbb{Z} + \tau\mathbb{Z} = \{m + n\tau;\ (m, n) \in \mathbb{Z}^2\}$ est un sous-anneau - noté $\mathbb{Z}[\tau]$ de $\mathbb{C}$. Inversement, si $\mathbb{Z} + \tau\mathbb{Z}$ est un anneau, alors $\tau^2 \in \mathbb{Z} + \tau\mathbb{Z}$, donc τ est racine d'un polynôme $X^2 + aX + b$ avec $a, b \in \mathbb{Z}$.

Les racines du polynôme $X^2 + aX + b$ sont τ et $\overline{\tau}$, de sorte que $\tau + \overline{\tau} = -a$ et $\tau\overline{\tau} = b$. En particulier $\overline{\tau} = -a - \tau \in \mathbb{Z}[\tau]$.

Pour $x \in \mathbb{Z}[\tau]$, on a $\overline{x} \in \mathbb{Z}[\tau]$, donc $|x|^2 = \overline{x}x \in \mathbb{Z}[\tau] \cap \mathbb{R}_+ = \mathbb{N}$ (et, de même, $\overline{x} + x \in \mathbb{Z}[\tau] \cap \mathbb{R} = \mathbb{Z}$). Posons $v(x) = |x|^2$. Nous allons voir que *pour des valeurs très particulières* de τ, l'anneau $\mathbb{Z}[\tau]$ est euclidien de stathme v, et que dans d'autres cas, il n'est pas principal.

Inversibles. *Un élément x de $\mathbb{Z}[\tau]$ est inversible si et seulement si $v(x) = 1$.*

Démonstration. Si $xy = 1$, on a $v(x)v(y) = |x|^2|y|^2 = 1$ donc $v(x)$ est inversible dans $\mathbb{N}$: $v(x) = 1$. Si $v(x) = 1$ alors $x\overline{x} = 1$, donc x est inversible dans $\mathbb{Z}[\tau]$. □

Lemme. *On suppose que $|\mathrm{Im}(\tau)| < \sqrt{3}$. Alors pour tout $z \in \mathbb{C}$, il existe $q \in \mathbb{Z}[\tau]$ tel que $|z - q| < 1$.*

Démonstration. Soit $n \in \mathbb{Z}$ l'entier le plus proche de $\dfrac{\mathrm{Im}(z)}{\mathrm{Im}(\tau)}$, de sorte que $|\mathrm{Im}(z - n\tau)| \leqslant \dfrac{|\mathrm{Im}(\tau)|}{2}$. Soit aussi m le nombre entier le plus proche de la partie réelle de $z - n\tau$, de sorte que $|\mathrm{Re}(z - n\tau - m)| \leqslant \dfrac{1}{2}$. Posons $q = m + n\tau$. On a $|\mathrm{Re}(z - q)| \leqslant \dfrac{1}{2}$ et $|\mathrm{Im}(z - q)| \leqslant \dfrac{|\mathrm{Im}(\tau)|}{2}$, donc $|z - q|^2 \leqslant \dfrac{1 + \mathrm{Im}(\tau)^2}{4} < 1$. □

Anneau Euclidien. *Si $|\mathrm{Im}(\tau)| < \sqrt{3}$, l'anneau $\mathbb{Z}[\tau]$ est euclidien de stathme $v : x \mapsto |x|^2$.*

Démonstration. Soient $a, b \in \mathbb{Z}[\tau] - \{0\}$; posons $z = \dfrac{a}{b}$ et soit $q \in \mathbb{Z}[\tau]$ tel que $|z - q| < 1$. Posons $r = a - bq$. On a $a = bq + r$ et $|r| = |b||z - q| < |b|$ donc $v(r) < v(b)$. □

Sans changer l'anneau $\mathbb{Z}[\tau]$, on peut remplacer τ par $\overline{\tau}$, de sorte que l'on peut supposer que $\mathrm{Im}(\tau) > 0$; on peut aussi remplacer τ par $\tau + n$ (avec n dans $\mathbb{Z}$). On peut donc supposer que la partie réelle de τ est dans $[0, 1[$; comme $\tau + \overline{\tau} \in \mathbb{Z}$, on a $\tau + \overline{\tau} = 0$ ou 1. Cela nous ramène à étudier seulement le cas où τ est racine d'un polynôme $X^2 + b$, ou $X^2 - X + b$ (avec $b \in \mathbb{N}^*$). Dans le premier cas, $\tau = i\sqrt{b}$; dans le deuxième $\tau = \dfrac{1 + i\sqrt{4b - 1}}{2}$.
Le théorème s'applique donc uniquement dans les cinq cas suivants :

$$\tau \in \left\{ i, i\sqrt{2}, \frac{1 + i\sqrt{3}}{2}, \frac{1 + i\sqrt{7}}{2}, \frac{1 + i\sqrt{11}}{2} \right\}.$$

Commentaire. On peut démontrer relativement facilement (*cf.* exerc. 2.5) que dans tous les autres cas, l'anneau $\mathbb{Z}[\tau]$ n'est pas euclidien. Cependant, il y a quelques cas où $\mathbb{Z}[\tau]$ est quand même principal. Cela se produit pour $\tau = \dfrac{1 + i\sqrt{19}}{2}$. (*cf.* exerc. 2.7). Cependant, pour $b \geqslant 3$, l'anneau $\mathbb{Z}[i\sqrt{b}]$ n'est pas factoriel, donc il n'est pas principal (*cf.* exerc. 2.8).

L'équation diophantienne $x^2 + y^2 = z^2$. On cherche à trouver tous les triplets $(x, y, z) \in \mathbb{Z}^3$ tels que $x^2 + y^2 = z^2$. Si (x, y, z) est une solution et $k \in \mathbb{Z}$, alors (kx, ky, kz) est aussi une solution. On peut donc supposer que (x, y, z) sont premiers entre eux. Si d divise x et y, alors d^2 divise z^2, donc d divise z. On peut donc supposer que x et y sont premiers entre eux. Remarquons que x et y ne peuvent être tous deux impairs car alors $x^2 \equiv y^2 \equiv 1$ [4], donc $z^2 \equiv 2$ [4] ce qui est impossible. Donc l'un des deux est pair et l'autre impair.

Dans ce cas, l'idéal $J = (x + iy)\mathbb{Z}[i] + (x - iy)\mathbb{Z}[i]$ de $\mathbb{Z}[i]$ contient $(x + iy) + (x - iy) = 2x$, ainsi que $i\big((x - iy) - (x + iy)\big) = 2y$; écrivant une relation de Bézout (dans $\mathbb{Z}$) entre x et y, il vient $2 \in J$. Or il existe $q \in \mathbb{Z}[i]$ tel que $(x + iy) - 2q$ soit égal à 1 ou à i. Cela prouve que $(x + iy)$ et $(x - iy)$ sont premiers entre eux. Décomposons $z^2 = (x + iy)(x - iy)$ en éléments irréductibles dans $\mathbb{Z}[i]$; puisque c'est un carré, chacun figure un nombre pair de fois. Cela prouve que $x + iy$ est associé à un carré : il existe $(a, b) \in \mathbb{Z}$, tels que $x + iy$ soit associé à $(a + ib)^2$ c'est à dire $x + iy = \pm(a + ib)^2$ (si y est pair) ou $x + iy = \pm i(a + ib)^2$ (si x est pair). On en déduit que les solutions sont nécessairement de la forme $(k(a^2 - b^2), 2kab, k(a^2 + b^2))$ ou $(2kab, k(a^2 - b^2), k(a^2 + b^2))$ (avec $a, b, k \in \mathbb{Z}$).

Irréductibles. *On suppose que $\mathbb{Z}[\tau]$ est principal. Soit q un élément irréductible de $\mathbb{Z}[\tau]$. Alors deux cas sont possibles :*

- *il existe un nombre premier $p \in \mathbb{N}$ tel que $v(q) = p$;*
- *il existe un nombre premier $p \in \mathbb{N}$ tel que q soit associé à p (et l'on a $v(q) = p^2$).*

Démonstration. Décomposons $v(q) = q\overline{q}$ en facteurs premiers dans $\mathbb{Z}$. C'est une décomposition dans $\mathbb{Z}[\tau]$ qui ne peut donc avoir que un ou deux éléments : dans le premier cas $v(q)$ est premier ; dans le deuxième un des facteurs p est associé à q, donc $v(q) = v(p) = p^2$. □

Nous verrons en exercice (2.1) quels nombres premiers de $\mathbb{N}$ ne sont plus irréductibles dans $\mathbb{Z}[i]$.

2.5 Sous-corps

2.5.1 Caractéristique d'un corps ; sous-corps premier

Soit K un corps. Tout morphisme f d'anneaux de K dans un anneau non nul est injectif : si $x \in K^*$, alors $f(x^{-1})f(x) = 1$, donc $f(x) \neq 0$.

Soit K un corps et $f : \mathbb{Z} \to K$ l'unique homomorphisme d'anneaux (défini par $f(n) = n1_K$). Le noyau de f est un idéal $n\mathbb{Z}$ de $\mathbb{Z}$. L'image $f(\mathbb{Z})$ est un sous-anneau commutatif de $\mathbb{K}$ isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Puisque K est un corps, $f(\mathbb{Z})$ est un anneau intègre, donc ou bien n est premier, ou bien f est injective. Ce nombre n s'appelle la *caractéristique* de K.

- Lorsque la caractéristique p n'est pas nulle, l'image $f(\mathbb{Z})$ est un sous-corps de K isomorphe à $\mathbb{Z}/p\mathbb{Z}$.
- Lorsque f est injective, on peut étendre f en un homomorphisme $\tilde{f} : \mathbb{Q} \to K$ en posant $\tilde{f}\left(\dfrac{p}{q}\right) = f(p)f(q)^{-1}$ pour $p, q \in \mathbb{Z}$ avec $q \neq 0$. L'image $\tilde{f}(\mathbb{Q})$ est un sous-corps de K isomorphe à $\mathbb{Q}$.
- Le corps ainsi obtenu, isomorphe selon les cas à $\mathbb{Z}/p\mathbb{Z}$ ou à $\mathbb{Q}$ est le plus petit sous-corps de K. On l'appelle le *sous-corps premier* de K.

2.5.2 Corps des fractions d'un anneau intègre

Soit A un anneau commutatif intègre non nul. On définit un corps K contenant A. Sa construction est la généralisation de la construction de $\mathbb{Q}$ à partir de $\mathbb{Z}$. Les éléments de K sont des fractions $\dfrac{a}{b}$ où $a \in A$ et $b \in A - \{0\}$. On peut alors dire quand deux fractions sont égales, définir l'addition et la multiplication des fractions, et vérifier que l'on obtient ainsi un corps qui contient l'anneau A.

Pour formaliser cela, considérons la relation R sur $A \times (A - \{0\})$ définie par $(a, b)\, R\, (c, d)$ si $ad = bc$. On vérifie sans peine que R est une relation d'équivalence. Notons K l'ensemble quotient. La classe dans K d'un élément $(a, b) \in A \times (A - \{0\})$ se note $\dfrac{a}{b}$.

On définit la somme et le produit d'éléments de K en posant pour des éléments a, b, c, d de A avec b, d non nuls

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{et} \quad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}.$$

Ces opérations sont bien définies : si $(a, b)\, R\, (a', b')$ et $(c, d)\, R\, (c', d')$, alors $(ad + bc, bd)\, R\, (a'd' + b'c', b'd')$ et $(ac, bd)\, R\, (a'c', b'd')$. De plus, on a

$$\frac{a}{d} + \frac{c}{d} = \frac{a + c}{d}$$

ce qui permet de démontrer facilement les règles des opérations : K est bien un anneau commutatif. De plus K est un corps : l'inverse de $\dfrac{a}{b}$ est $\dfrac{b}{a}$ (pour $a, b \in A - \{0\}$).

Le corps K s'appelle le *corps de fractions* de A.

Enfin, on plonge A dans K au moyen de l'application $a \mapsto \dfrac{a}{1}$: cette application est un morphisme injectif qui plonge l'anneau A dans K.

2.29 Proposition. *Soit A un anneau commutatif intègre. Notons $K(A)$ son corps des fractions. Pour tout corps L et tout homomorphisme injectif $f : A \to L$, il existe un unique homomorphisme $\tilde{f} : K(A) \to L$ dont la restriction à $A \subset K(A)$ soit f*

2.5.3 Éléments algébriques, éléments transcendants

Soient L un corps commutatif et $K \subset L$ un sous-corps.

Soit $x \in L$. Considérons L comme espace vectoriel sur K et introduisons le sous-espace $K[x] \subset L$ engendré par les éléments x^n pour $n \in \mathbb{N}$. Cet espace est l'image de l'application $f : P \mapsto P(x)$ de $K[X]$ dans L. Cette application étant un homomorphisme d'anneaux, son noyau est un idéal de l'anneau principal $K[X]$. Il existe donc un polynôme $\varpi \in K[X]$ tel que $\ker f = \varpi K[X]$. Deux cas sont possibles :

a) Si $\varpi = 0$, l'application $f : P \mapsto P(x)$ est injective de $K[X]$ dans L. On dit alors que x est *transcendant* sur K.

b) Si $\varpi \neq 0$. Remarquons que f n'est pas l'application nulle, donc ϖ n'est pas inversible ; si $\varpi = PQ$, on trouve $P(x)Q(x) = 0$, ce qui implique que $P(x) = 0$ ou $Q(x) = 0$, *i.e.* l'un des deux est dans $\ker f$ donc multiple de ϖ. Il s'ensuit que ϖ est irréductible. On dit alors que x est *algébrique* sur K et le polynôme ϖ s'appelle le *polynôme minimal* de x.

Citons sans démonstration le résultat suivant (*cf.* exercice 2.9) :

2.30 Proposition. *Soient L un corps commutatif et $K \subset L$ un sous-corps. Les éléments de L algébriques sur K forment un sous-corps de L.*

Cela signifie que la somme, le produit, l'inverse d'éléments algébriques est algébrique.

2.31 Proposition. *Le corps des nombres complexes algébriques sur $\mathbb{Q}$ est dénombrable.*

En effet, les éléments algébriques sont les racines de polynômes à coefficients rationnels (non nuls). Or $\mathbb{Q}$ étant dénombrable, l'ensemble des polynômes à coefficients rationnels est dénombrable, et chacun a un nombre fini de racines

On déduit de ce résultat qu'il y a « bien plus » de nombres transcendants que de nombres algébriques. On peut démontrer que les nombres e et π sont transcendants, mais ce n'est pas si facile.

2.6 Exercices

2.1 Exercice. Soit $p \in \mathbb{N}$ un nombre premier. Démontrer que les assertions suivantes sont équivalentes :

(i) il existe $a, b \in \mathbb{Z}$ tels que $a^2 + b^2 = p$;

(ii) l'élément $p \in \mathbb{Z}[i]$ n'est pas irréductible dans $\mathbb{Z}[i]$;

(iii) -1 est un carré modulo p ;

(iv) $p \not\equiv 3$ [4].

2.2 Exercice. *Le groupe $\mathbb{F}_p^*$ est cyclique. (1)*

1. Soit G un groupe commutatif fini.
   a) Soient $a, b \in G$. On note k_a et k_b leurs ordres respectifs. On suppose que k_a et k_b sont premiers entre eux. Démontrer que l'ordre de ab est $k_a k_b$.
   b) Démontrer qu'il existe $n \in \mathbb{N}^*$ tel que $\{k \in \mathbb{Z};\ \forall x \in G;\ x^k = 1\} = n\mathbb{Z}$. Démontrer que n divise le cardinal de G.
   Le nombre n s'appelle l'*exposant* de G.

c) Ecrivons $n = \prod p_j^{m_j}$ la décomposition de n en nombres premiers distincts. Démontrer que pour tout j, il existe $x_j \in G$ d'ordre $p_j^{m_j}$.

d) En déduire qu'il existe $x \in G$ d'ordre n.

2. Soit K un corps commutatif et G un sous-groupe fini à N éléments de K^*. Soit n son exposant.

a) Démontrer que l'équation $x^n = 1$ a au plus n solutions dans K. En déduire que $N \leqslant n$.

b) Démontrer que G est cyclique.

2.3 Exercice. *Le groupe $\mathbb{F}_p^*$ est cyclique. (2)*

1. Soit $n \in \mathbb{N}^*$. On considère l'ensemble $A_n = \left\{ \frac{k}{n};\ k \in \mathbb{N},\ \ 0 \leqslant k < n \right\}$.

a) Soit d un diviseur de n. Combien d'éléments de A_n ont leur écriture irréductible de la forme $\frac{a}{d}$?

b) En déduire l'égalité $\sum_{d|n} \varphi(d) = n$.

2. Soit K un corps commutatif et G un sous-groupe fini à n éléments de K^*. Pour $d \in \mathbb{N}^*$, on note s_d le nombre d'éléments d'ordre d de G.

a) Démontrer que $\sum_{d|n} s_d = n$.

b) Soit $x \in G$; notons d son ordre et H le sous-groupe (cyclique) de G engendré par x. Démontrer que
- H a d éléments et $\varphi(d)$ éléments d'ordre d.
- Tout élément $y \in H$ vérifie $y^d = 1$.
- L'équation $y^d = 1$ a au plus d solutions dans K.
- Tout élément d'ordre d de G est dans H.

c) En déduire que si $s_d \neq 0$, alors $s_d = \varphi(d)$.

d) En déduire que pour tout diviseur d de n on a $s_d = \varphi(d)$, puis que G est cyclique.

2.4 Exercice. *Le groupe $(\mathbb{Z}/n\mathbb{Z})^*$ est-il cyclique ? (***)* Perrin, *Cours d'algèbre* p.24.

Cet exercice complète les précédents.

1. a) Soient G et H deux groupes commutatifs finis. Démontrer que $G \times H$ est cyclique si et seulement si G et H sont cycliques et que leurs ordres sont premiers entre eux.

b) Quels sont les nombres n tels que $\varphi(n)$ soit impair ?

c) Soient m et n deux nombres entiers premiers entre eux distincts de 1 et de 2. Démontrer que $(\mathbb{Z}/nm\mathbb{Z})^*$ n'est pas cyclique.

d) $\mathbb{Z}/8\mathbb{Z}^*$ est-il cyclique ?

2. Soient p un nombre premier distinct de 2 et $n \in \mathbb{N}$, $n \geqslant 2$.

a) Démontrer (par récurrence) que, pour tout $k \in \mathbb{N}$, $(1+p)^{p^k} \equiv 1 + p^{k+1} \ \ [p^{k+2}]$.

b) Quel est l'ordre de $1+p$ dans le groupe $\mathbb{Z}/p^n\mathbb{Z}^*$?

c) Soit $a \in \mathbb{Z}$ dont la classe dans $\mathbb{Z}/p\mathbb{Z}$ engendre $\mathbb{Z}/p\mathbb{Z}^*$, et soit $x \in \mathbb{Z}/p^n\mathbb{Z}^*$ la classe de a. Démontrer que l'ordre de x dans $\mathbb{Z}/p^n\mathbb{Z}^*$ est un multiple de $p-1$. En déduire qu'il existe dans $\mathbb{Z}/p\mathbb{Z}$ un élément d'ordre $p-1$.

d) Démontrer que $\mathbb{Z}/p^n\mathbb{Z}^*$ est cyclique. Démontrer que $\mathbb{Z}/2p^n\mathbb{Z}^*$ est aussi cyclique.

3. Quels sont les entiers n tels que $\mathbb{Z}/n\mathbb{Z}^*$ soit cyclique ?

2.5 Exercice. Soit $a \in \mathbb{N}^*$ et $\tau \in \mathbb{C}$ une racine du polynôme $X^2 + X + a$. On note $\mathbb{Z}[\tau]$ l'anneau $\mathbb{Z} + \tau\mathbb{Z}$.

1. a) Soit $x \in \mathbb{Z}[\tau]$ non nul. Démontrer que $\mathbb{Z}[\tau]/x\mathbb{Z}[\tau]$ est fini. Notons $v(x)$ le nombre de ses éléments.

   b) Soient $x, y \in \mathbb{Z}[\tau]$ non nuls. Donnons nous des représentants $r_1, \ldots, r_n$ des classes d'éléments de $\mathbb{Z}[\tau]$ modulo x et des représentants $s_1, \ldots, s_m$ des classes d'éléments de $\mathbb{Z}[\tau]$ modulo y. Démontrer que tout élément de $\mathbb{Z}[\tau]$ est congru modulo xy à un un et un seul élément de la forme $r_i + xs_j$. En déduire que $v(xy) = v(x)v(y)$.

   c) En calculant $v(k)$ pour $k \in \mathbb{Z}$, démontrer que, pour tout $x \in \mathbb{Z}[\tau]$ non nul, on a $v(x) = |x|^2$.

2. On suppose que $\mathbb{Z}[\tau]$ possède un stathme euclidien V.

   a) On suppose aussi que les seuls éléments inversibles de $\mathbb{Z}[\tau]$ sont ± 1. Soit $x \in \mathbb{Z}[\tau]$ non nul et non inversible de stathme minimal. Démontrer que tout élément de $\mathbb{Z}[\tau]$ est congru modulo x à $0, 1$ ou -1 ; en déduire que $v(x) \leqslant 3$.

   b) Démontrer que $\operatorname{Im} \tau \leqslant \sqrt{3}$.

2.6 Exercice. *Sous-groupes de* $\mathbb{Z}[\tau]$. Soit $\tau \in \mathbb{C}$ racine d'un polynôme $X^2 + X + a$ ou $X^2 + a$ avec $a \in \mathbb{N}^*$. Soit G un sous-groupe non nul de $\mathbb{Z}[\tau]$. Soit $\alpha \in G$ un élément non nul tel que $|\alpha|^2$ soit minimal dans $\{|x|^2;\ x \in G \setminus \{0\}\}$. (Un tel élément existe d'après le « principe de récurrence »- puisque $|x|^2 \in \mathbb{N}$ pour tout $x \in \mathbb{Z}[\tau]$).

1. Démontrer que $G \cap \mathbb{R}\alpha = \mathbb{Z}\alpha$.
   On suppose désormais que $G \not\subset \mathbb{R}\alpha$. Soit $\beta \in G \setminus \mathbb{Z}\alpha$ tel que $|\beta|^2$ soit minimal dans $\{|x|^2;\ x \in G \setminus \mathbb{Z}\alpha\}$. Quitte à remplacer β par $-\beta$, on peut supposer que $\operatorname{Im} \dfrac{\beta}{\alpha} > 0$.
2. Démontrer que $\left|\dfrac{\beta}{\alpha}\right| \geqslant 1$ et $\left|\operatorname{Re} \dfrac{\beta}{\alpha}\right| \leqslant \dfrac{1}{2}$.
3. Soit $x \in G$. Démontrer qu'il existe $m, n \in \mathbb{Z}$ tels que

$$\left|\operatorname{Im} \frac{x - n\beta}{\alpha}\right| \leqslant \frac{1}{2}\operatorname{Im} \frac{\beta}{\alpha} \quad \text{et} \quad \left|\operatorname{Re} \frac{x - (m\alpha + n\beta)}{\alpha}\right| \leqslant \frac{1}{2}.$$

   En déduire que $|x - (m\alpha + n\beta)| < |\beta|$, puis que $x = m\alpha + n\beta$.
   Il s'ensuit que $G = \alpha\mathbb{Z} + \beta\mathbb{Z}$.

2.7 Exercice. *Un anneau principal non euclidien*

Le but de cet exercice est de démontrer que pour $\tau = \dfrac{1 + i\sqrt{19}}{2}$, l'anneau $\mathbb{Z}[\tau]$ est principal mais n'est pas euclidien. Soit J un idéal non nul de $\mathbb{Z}[\tau]$. Puisque J est un sous-groupe de $\mathbb{Z}[\tau]$, non contenu dans un $a\mathbb{R}$ (il contient un élément non nul a et $a\tau$) il existe d'après l'exercice 2.6 $\alpha, \beta \in \mathbb{Z}[\tau]$ tels que

$$\operatorname{Im} \frac{\beta}{\alpha} > 0, \quad \left|\frac{\beta}{\alpha}\right| \geqslant 1, \quad \left|\operatorname{Re} \frac{\beta}{\alpha}\right| \leqslant \frac{1}{2} \quad \text{et} \quad J = \alpha\mathbb{Z} + \beta\mathbb{Z}$$

(remarquons que $\tau\alpha \in J$, donc $J \not\subset \mathbb{R}\alpha$).

1. Démontrer qu'il existe $a, b, c, d \in \mathbb{Z}$ tels que $\tau\alpha = a\alpha + b\beta$ et $\tau\beta = c\alpha + d\beta$.
2. En regardant les signes des parties imaginaires de τ et $\dfrac{\beta}{\alpha}$, démontrer que $b > 0$.
3. Quelles sont les valeurs propres et espaces propres de la matrice $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$? Démontrer que $a + d = 1$ et $ad - bc = 5$. En déduire que $ad \leqslant 0$, que ad est pair, que $bc < 0$, que b et c sont impairs et que $4bc + (a - d)^2 = -19$.

4. Posons $x = \dfrac{\beta}{\alpha}$. Démontrer que $\begin{vmatrix} a+bx & 1 \\ c+dx & x \end{vmatrix} = 0$. En déduire que
   a) x et $\overline{x}$ sont racines du polynôme $bX^2 + (a-d)X - c$,
   b) $|x|^2 = -\dfrac{c}{b}$ et $\operatorname{Re} x = \dfrac{d-a}{2b}$.
5. Démontrer que $|a-d| \leqslant b$ et $b \leqslant -c$. En déduire que $3b^2 \leqslant 19$, puis que $b = 1$.
6. En déduire que $(\alpha, \tau\alpha)$ est une $\mathbb{Z}$-base de J et conclure.

On démontre de même que pour $D \in \{19, 43, 67, 163\}$, l'anneau $\mathbb{Z}\left[\dfrac{1+i\sqrt{D}}{2}\right]$ est principal.

2.8 Exercice. 1. Dans $\mathbb{Z}[X]$, démontrer que l'idéal engendré par 2 et X n'est pas principal.

2. Démontrons que pour $\tau = i\sqrt{b}$ avec $b \geqslant 3$ et pour $\tau = \dfrac{1+i\sqrt{15}}{2}$, l'anneau $\mathbb{Z}[\tau]$ n'est pas factoriel (donc n'est pas principal). En utilisant les égalités :
   • pour $\tau = i\sqrt{3}$, on a $(1+\tau)(1+\overline{\tau}) = 4 = 2 \times 2$;
   • pour $\tau = 2i$ ou $\tau = \dfrac{1+i\sqrt{15}}{2}$, on a $\tau\overline{\tau} = 4 = 2 \times 2$;
   • pour $\tau = i\sqrt{5}$, on a $(1+\tau)(1+\overline{\tau}) = 6 = 2 \times 3$;
   démontrer que l'on n'a pas l'unicité dans la décomposition en éléments irréductibles. Pour $b \geqslant 5$, et $\tau = i\sqrt{b}$, écrire une égalité de ce style en discutant la parité de b. En déduire que $\mathbb{Z}[\tau]$ n'est pas principal.

2.9 Exercice. Soient L un corps commutatif et $K \subset L$ un sous-corps. Remarquons que L est un espace vectoriel sur K et que tout sous-anneau de L contenant K est un sous-K-espace vectoriel de L.

1. Soit K_1 un sous-corps de L contenant K. Démontrer que tout élément algébrique sur K est algébrique sur K_1.
2. Démontrer que pour $x \in L$ les conditions suivantes sont équivalentes :
   (i) x est algébrique sur K ;
   (ii) il existe un sous-anneau A de L contenant K et x et qui soit un espace vectoriel de dimension finie sur K ;
   (iii) il existe un sous-corps K_1 de L contenant K et x et qui soit un espace vectoriel de dimension finie sur K.
3. Soient K_1, K_2 des sous-corps de L tels que $K \subset K_1 \subset K_2$. Démontrer que K_2 est un K-espace vectoriel de dimension finie si et seulement si K_2 est un K_1-espace vectoriel de dimension finie et K_1 est un K-espace vectoriel de dimension finie, et que dans ce cas, on a $\dim_K(K_2) = \dim_{K_1}(K_2)\dim_K(K_1)$.
4. Soient $\alpha, \beta \in L$ des éléments algébriques sur K. Soit K_1 un sous-corps de L contenant K et α et de dimension finie sur K.
   a) On suppose que $\alpha \neq 0$. Démontrer que α^{-1} est algébrique sur K.
   b) Démontrer que $\alpha + \beta$ et $\alpha\beta$ sont algébriques sur K.
5. Démontrer que les éléments de L algébriques sur K forment un sous-corps K' de L. Démontrer que si $x \in L$ est algébrique sur K' alors $x \in K'$.

3 Polynômes et fractions rationnelles

3.1 Polynômes à une indéterminée sur un corps commutatif K

Soit K un corps commutatif. On sait très bien ce qu'est un polynôme à coefficients dans K : c'est une expression abstraite $P = \sum_{k=0}^{n} a_k X^k$ où les a_i sont des éléments de K appelés les coefficients de P. On sait ajouter et multiplier les polynômes, les multiplier par un scalaire : les polynômes forment une K-algèbre.

3.1 Quelques mots sur la définition de l'algèbre $K[X]$. Se donner un polynôme revient à se donner ses coefficients c'est à dire une suite $(a_k)_{k\in\mathbb{N}}$ d'éléments de K qui sont nuls pour k assez grand : il existe $n \in \mathbb{N}$ satisfaisant $a_k = 0$ pour $k > n$. On peut formaliser cela en définissant un polynôme comme la suite abstraite de ses coefficients : l'ensemble des polynômes est alors l'ensemble $K^{(\mathbb{N})}$ des suites $(a_k)_{k\in\mathbb{N}}$ telles qu'il existe $n \in \mathbb{N}$ satisfaisant $a_k = 0$ pour $k > n$. Dans cette vision, le $k^{\text{ème}}$ coefficient du polynôme X^k est égal à 1, et tous les autres sont nuls. L'ensemble $K^{(\mathbb{N})}$ est naturellement un K-espace vectoriel de dimension infinie et $(X^k)_{k\in\mathbb{N}}$ en est une base.

L'algèbre $K[X]$ est donc l'espace vectoriel $K^{(\mathbb{N})}$ muni de l'unique produit tel que $X^k X^\ell = X^{k+\ell}$ (pour tous $k, \ell \in \mathbb{N}$). Enfin, on identifie K avec l'ensemble des polynômes constants (au moyen de $a \mapsto aX^{(0)}$).

Soit $P \in K[X]$ un polynôme non nul. On appelle *degré* de P l'entier $\partial P = n \in \mathbb{N}$ tel que $a_n \neq 0$ et, $a_k = 0$ pour $k > n$ (où les a_k sont les coefficients de P). Le coefficient non nul de plus haut degré (a_n si $\partial P = n$) s'appelle le *coefficient directeur* de P. On dit que P est *unitaire* (ou *monique*) si son coefficient directeur est 1.

3.2 Proposition. *Pour $P, Q \in K[X]$ deux polynômes non nuls, on a $PQ \neq 0$, $\partial(PQ) = \partial P + \partial Q$, et le coefficient directeur de PQ est le produit des coefficients directeurs de P et de Q. En particulier, l'anneau $K[X]$ est intègre.*

L'anneau $K[X]$ est euclidien de stathme ∂. Plus précisément on a (où l'on a convenu $\partial 0 < 0$) :

3.3 Proposition : Division euclidienne dans $K[X]$. *Soient $A, B \in K[X]$ avec $B \neq 0$. Il existe un unique couple $Q, R \in K[X]$ tels que $A = BQ + R$ et $\partial R < \partial B$.*

On en déduit que $K[X]$ est principal, c'est-à-dire que tous les idéaux de $K[X]$ sont de la forme $AK[X]$. On peut alors définir le plus grand commun diviseur (PGCD) et plus petit commun multiple (PPCM) de deux polynômes, établir un théorème de Bézout, un algorithme d'Euclide qui permet de trouver le PGCD et une relation de Bézout ainsi que la décomposition unique d'un polynôme en facteurs irréductibles.

3.4 Exercices. a) Soient L un corps commutatif et K un sous-corps de L. Soient $A, B \in K[X]$; Démontrer que leur PGCD est le même qu'on les considère comme éléments de $K[X]$ ou de $L[X]$.

b) Calculer $PGCD(X^m - 1, X^n - 1)$.

De l'égalité $\partial(PQ) = \partial P + \partial Q$ on déduit :

3.5 Proposition. *a) Les éléments inversibles de $K[X]$ sont les polynômes non nuls de degré nul, i.e. les éléments de K.*

b) Tout polynôme de degré 1 est irréductible.

3.2 Fonctions polynômes

3.2.1 Racines

Soit K un corps. Si $x \in K$ et $P = \sum_{k=0}^{n} a_k X^k \in K[X]$, on pose $P(x) = \sum_{k=0}^{n} a_k x^k$. L'application $x \mapsto P(x)$ s'appelle la fonction polynôme associée à P. L'application $P \mapsto P(x)$ est un homomorphisme d'anneaux de $K[X]$ dans K. On dit que x est une *racine* de P si $P(x) = 0$.

3.6 Proposition. *Le reste de la division euclidienne de P par $X - a$ est $P(a)$. En particulier, $X - a$ divise P si et seulement si $P(a) = 0$.*

En effet, écrivons $P = (X - a)Q + R$ avec $\partial R < 0$, donc $R \in K$. Comme $(X - a)(a) = 0$, on trouve $P(a) = R$.

Cette proposition nous conduit à dire que a est une racine d'ordre k (au moins) si $(X - a)^k$ divise P et d'ordre exactement k si de plus $(X - a)^{k+1}$ ne divise pas P. Si $k = 2, 3$, on dira que a est racine double, triple... de P. Si $k \geqslant 2$ on dira que a est *racine multiple* de P

3.7 Proposition. *Soient $a_1, \ldots, a_k \in K$ des éléments deux à deux distincts et $m_1, \ldots, m_k \in \mathbb{N}$. Si un polynôme non nul P admet les racines a_j avec multiplicité m_j, il est divisible par $\prod_{j=1}^{k}(X - a_j)^{m_j}$. En particulier $\partial P \geqslant \sum m_j$ et si $\partial P = \sum m_j$, alors $P = a\prod_{j=1}^{k}(X - a_j)^{m_j}$ où $a \in K$ est le coefficient directeur de P.*

Les polynômes $X - a_j$ sont premiers entre eux deux à deux, donc il en va de même pour $(X - a_j)^{m_j}$. Si P admet les racines a_j avec multiplicité m_j, il est divisible par $(X - a_j)^{m_j}$, donc par leur produit.

3.8 Exemple. Soit p un nombre premier. D'après le (petit) théorème de Fermat, pour tout $x \in \mathbb{Z}/p\mathbb{Z}$, on a $x^p = x$. En d'autres termes, tout élément de $\mathbb{Z}/p\mathbb{Z}$ est racine du polynôme $X^p - X \in \mathbb{Z}/p\mathbb{Z}[X]$. On en déduit que $\prod_{x \in \mathbb{Z}/p\mathbb{Z}} (X - x) = X^p - X$.

3.9 Corollaire. *Si K est infini, l'homomorphisme qui à un polynôme P associe la fonction polynôme $x \mapsto P(x)$ de K dans K est injectif.*

En effet, un polynôme non nul ne peut avoir qu'un nombre fini de racines. Il ne peut s'annuler sur tout K.

A cause de ce corollaire, on confond souvent les polynômes avec les fonctions polynômes.

3.10 Remarque. Pour $K = \mathbb{Z}/p\mathbb{Z}$, le noyau de l'homomorphisme qui à un polynôme P associe la fonction polynôme $x \mapsto P(x)$ de K dans K est l'idéal engendré par $X^p - X$.

3.11 Exemple. Polynôme d'interpolation de Lagrange. Soient $x_1, x_2 \ldots, x_n$ des éléments distincts de K et $\lambda_1, \lambda_2, \ldots, \lambda_n$ des éléments de K. Il existe un unique polynôme P de degré au plus $n - 1$ tel que $P(x_i) = \lambda_i$ pour tout i.

Existence. Pour $i = 1, \ldots, n$, posons $Q_i = \prod_{1 \leqslant j \leqslant n;\ j \neq i} (X - x_j)$. On prend $P = \sum_{i=1}^{n} \frac{\lambda_i}{Q_i(x_i)} Q_i$.

Unicité. Si P et Q satisfont ces conditions alors $P - Q$ s'annule en les x_i ; comme $\partial(P - Q) < n$, il vient $P - Q = 0$.

3.2.2 Polynômes scindés ; relations entre coefficients et racines

On dit qu'un polynôme P est *scindé* s'il est produit de polynômes du premier degré. Alors P s'écrit $P = a\prod_{k=1}^{n}(X - x_k)$.

Soit $P = \prod_{k=1}^{n}(X - x_k)$ un polynôme unitaire scindé. Écrivons $P = X^n + \sum_{k=0}^{n-1} a_k X^k$. Alors on a

- somme des racines $\sum_{k=1}^{n} x_k = -a_{n-1}$;
- produit des racines $(-1)^n a_0 = \prod_{k=1}^{n} x_k$.
- Plus généralement, $(-1)^\ell a_{n-\ell} = \sum_{1\leqslant k_1<\ldots<k_\ell\leqslant n}\left(\prod_{j=1}^{\ell} x_{k_j}\right)$ est la somme de tous les produits de ℓ racines.
- Pour $n = 2$ on trouve $P = X^2 - sX + p$ où s est la somme et p le produit des racines.
- Pour $n = 3$ on trouve $P = X^3 - sX^2 + \sigma_2 X - p$, où s est la somme, p le produit des racines et $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$.

3.2.3 Dérivation des polynômes

Soit $P = \sum_{k=0}^{n} a_k X^k$. On définit sa dérivée : c'est le polynôme $P' = \sum_{k=1}^{n} k a_k X^{k-1}$.

3.12 Proposition. a) *Pour $P, Q \in K[X]$, on a $(PQ)' = P'Q + PQ'$.*

b) *Soient $P \in K[X]$ et $a \in K$ une racine de P. Alors a est une racine double de P si et seulement si $P'(a) = 0$.*

a) se vérifie pour $P = X^k$ et $Q = X^\ell$ et s'étend par linéarité.
Pour b), écrivons $P = (X-a)Q$ de sorte que (d'après a) $P' = Q+(X-a)Q'$, donc $Q(a) = P'(a)$. Alors a est racine double de P, si et seulement si c'est une racine de Q, *i.e.* si et seulement si $P'(a) = Q(a) = 0$.

3.13 Dérivées successives ; identité de Taylor. On définit aussi les dérivées successives en posant $P'' = (P')'$ *etc.* La dérivée k-ième se note $P^{(k)}$. On a $P^{(k)}(0) = k!a_k$, de sorte que, si K est de caractéristique nulle (et $\partial P \leqslant n$),

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(0)}{k!} X^k.$$

Plus généralement, soit $a \in K$. Les polynômes $(X - a)^k$ forment une base de $K[X]$ (car ils sont échelonnés). Posons $Q_k = \dfrac{(X-a)^k}{k!}$. On a $Q_k^{(j)} = Q_{k-j}$ si $k \geqslant j$ et $Q_k^{(j)} = 0$ si $k < j$. En particulier, $Q_k^{(j)}(a) = \delta_k^j$, et si P s'écrit $\sum_k b_k Q_k$, il vient $b_j = P^{(j)}(a)$, donc

$$P = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!}(X - a)^k.$$

3.2.4 Polynômes irréductibles sur $\mathbb{R}$ et $\mathbb{C}$

Donnons sans démonstration le théorème fondamental suivant :

3.14 Théorème de d'Alembert-Gauss. *Tout polynôme non constant à coefficients complexes admet au moins une racine dans* $\mathbb{C}$.

Tout polynôme non constant est donc divisible par un $X - a$. Il en résulte immédiatement que les polynômes irréductibles dans $\mathbb{C}[X]$ sont les polynômes du premier degré : tout polynôme à coefficients complexes est donc scindé.

Soit maintenant $P \in \mathbb{R}[X]$ un polynôme irréductible. Considérons le comme polynôme à coefficients complexes. Il a une racine $z \in \mathbb{C}$. Si $z \in \mathbb{R}$, P est du premier degré. Si $z = a + ib \notin \mathbb{R}$, alors écrivons $P = BQ + R$ la division euclidienne de P par $B = (X - z)(X - \overline{z}) = X^2 - 2aX + (a^2 + b^2)$ (dans $\mathbb{R}[X]$). Alors $R \in \mathbb{R}[X]$ est de degré au plus 1 et s'annule en z : c'est le polynôme nul.

On trouve :

3.15 Corollaire. *Les polynômes irréductibles de* $\mathbb{R}[X]$ *sont les polynômes du premier degré et ceux du deuxième degré de discriminant strictement négatif.*

3.2.5 Racines et extensions de corps

Soient K un corps commutatif et $P \in K[X]$. Si L est une extension de K, on peut considérer P comme polynôme à coefficients dans L : en d'autres termes on identifie $K[X]$ à un sous-anneau de $L[X]$. En particulier, on peut définir l'évaluation $P(x) \in L$ de P en un point $x \in L$ et donc la notion de racine de P dans L.

On note (P) l'idéal $PK[X]$ de $K[X]$. Puisque $K[X]$ est principal, tout idéal de $K[X]$ est de cette forme. Nous utiliserons le résultat suivant.

3.16 Proposition. *Soit* $P \in K[X]$ *un polynôme non nul. On a l'équivalence entre :*

(i) *Le polynôme* P *est irréductible ;*

(ii) *L'anneau quotient* $K[X]/(P)$ *est intègre ;*

(iii) *L'anneau quotient* $K[X]/(P)$ *est un corps.* □

Soit $P \in K[X]$ un polynôme irréductible. Notons $L = K[X]/(P)$ l'anneau quotient.

- On considère l'application $i : K \to L$ qui à un scalaire $a \in K$ associe la classe du polynôme constant $a \in K[X]$ dans le quotient. L'application i est un morphisme de corps (injectif) au moyen duquel on identifie K à un sous-corps de L et donc L à une extension de K.
- Notons aussi x la classe dans L du polynôme X dans le quotient $L = K[X]/(P)$. En d'autres termes, on a $x = \pi(X)$ où $\pi : K[X] \to L = K[X]/(P)$ est l'application quotient.
- Comme π est un homomorphisme d'anneaux, on a $\pi(X^2) = x^2$ et plus généralement $\pi(X^n) = x^n$.
- Pour $a \in K$, on a $\pi(aX^0) = i(a)$, en d'autres termes, avec les identifications de $K \subset K[X]$ et $K \subset L$, la restriction de π à K est l'identité.
- On a donc $\pi(\sum_{k=0}^{n} a_k X^k) = \sum_{k=0}^{n} a_k x^k$; autrement dit, pour tout polynôme $Q \in K[X]$, on a $\pi(Q) = Q(x)$.
- En particulier, puisque $P \in \ker \pi = (P)$, on a $P(x) = 0$.

On a démontré :

3.17 Théorème. *Soient* K *un corps et* $P \in K[X]$ *un polynôme irréductible sur* K. *Il existe une extension* L *de* K *dans laquelle* P *admet une racine.* □

3.18 Corollaire. *Soient* K *un corps et* $P \in K[X]$ *un polynôme non constant.*

a) Il existe une extension L *de* K *dans laquelle* P *admet une racine.*

b) Il existe une extension L *de* K *dans laquelle* P *est scindé.*

Démonstration. a) Soit $P_0 \in K[X]$ un polynôme irréductible dans K divisant P. Par le théorème ci-dessus, il existe une extension L de K dans laquelle P_0 admet une racine ; celle-ci sera une racine de P.

b) On procède par récurrence sur le degré de P. On démontre par récurrence sur n l'énoncé suivant : $S(n)$: 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 $n = 1$: tout polynôme de degré 1 est scindé donc $S(1)$ est vraie.
- Supposons $S(n)$ démontrée et soit P un polynôme de degré $n+1$ sur un corps commutatif K. Par (a), il existe une extension L_1 de K dans laquelle P admet une racine α. Alors P vu comme polynôme de $L_1[X]$ s'écrit $P = (X-\alpha)Q$ où $Q \in L_1[X]$ est de degré n. Puisque $S(n)$ est vraie (hypothèse de récurrence), il existe une extension L de L_1 dans laquelle le polynôme Q est scindé. Alors L est une extension de K et le polynôme $P = (X-\alpha)Q$ est scindé dans L. □

3.3 Fractions rationnelles sur un corps commutatif K

3.19 Définition. Le corps des fractions de $K[X]$ se note $K(X)$. Ses éléments s'appellent des *fractions rationnelles.*

Si A, B, D sont des polynômes avec $BD \neq 0$, on a $\dfrac{AD}{BD} = \dfrac{A}{B}$. Donc pour chaque fraction rationnelle F il existe des polynômes A, B premiers entre eux $B \neq 0$ tels que $F = \dfrac{A}{B}$. Une écriture de $F = \dfrac{A}{B}$ avec A, B premiers entre eux s'appelle une *forme irréductible* de F.

Soit F une fraction rationnelle et $F = \dfrac{A}{B}$ une forme irréductible. Les racines de A s'appellent les *zéros* ou *racines* de F ; les racines de B s'appellent les *pôles* de F. L'*ordre de multiplicité* d'un zéro (*resp.* pôle) a est l'ordre de multiplicité de la racine a de A (*resp.* B).

Soit $F \in K(X)$. Notons $\mathcal{P} \subset K$ l'ensemble de ses pôles. Soit $x \in K - \mathcal{P}$. Il existe une écriture $F = \dfrac{A}{B}$ telle que $B(x) \neq 0$. On pose alors $F(x) = A(x)B(x)^{-1}$. Cet élément de K ne dépend pas de l'écriture $F = \dfrac{A}{B}$ (avec $B(x) \neq 0$).
L'application $x \mapsto F(x)$ de $K - \mathcal{P}$ dans K s'appelle la *fonction rationnelle* associée à F.

Décomposition en éléments simples

On va peu à peu essayer de décomposer une fraction rationnelle en une somme de termes plus simples.

a) ***Partie entière.*** Le degré d'une fraction rationnelle $F = \dfrac{A}{B}$ est le nombre $\partial F = \partial A - \partial B (\in \mathbb{Z})$. Ce nombre est indépendant de l'écriture. On a $\partial(FG) = \partial F + \partial G$ et $\partial(F+G) \leqslant \max\{\partial F, \partial G\}$ (avec la convention $\partial 0 = -\infty$).
Soit $F = \dfrac{A}{B}$ une fraction rationnelle. Écrivons $A = BQ + R$ la division euclidienne de A par B. On trouve $F = Q + \dfrac{R}{B}$, où $Q \in K[X] \subset K(X)$ et $\dfrac{R}{B}$ est une fraction rationnelle de degré < 0 (ou nulle). Donc :
Toute fraction rationnelle $F \in K(X)$ se décompose de façon unique en une somme d'un polynôme Q et d'une fraction rationnelle F_1 de degré strictement négatif. Le polynôme Q de cette décomposition s'appelle la partie entière *de F.*

b) ***Parties primaires.*** Soit à présent $F = \dfrac{A}{B}$ une fraction rationnelle de degré < 0. Supposons que B s'écrive $B = B_1 B_2$ où B_1 et B_2 sont des polynômes premiers entre eux. D'après le théorème de Bézout, il existe des polynômes C_1 et C_2 tels que $A = B_1 C_2 + B_2 C_1$. Écrivons $C_1 = QB_1 + A_1$ la division euclidienne de C_1 par B_1 et posons $A_2 = C_2 + QB_2$, de sorte que $A = A_2 B_1 + A_1 B_2$ avec $\partial A_1 < \partial B_1$. Notons qu'alors $A_2 B_1 = A - A_1 B_2$, de sorte que $\partial(A_2 B_1) < \partial B$; il vient $\dfrac{A}{B} = \dfrac{A_1}{B_1} + \dfrac{A_2}{B_2}$ avec $\partial A_1 < \partial B_1$ et $\partial A_2 < \partial B_2$. On vérifie que cette décomposition est unique.

Décomposant B en produit $\displaystyle\prod_{i=1}^{k} P_i^{m_i}$ où les P_i sont des polynômes irréductibles distincts on obtient (par récurrence sur k) une décomposition unique

$$\frac{A}{B} = \sum_{i=1}^{k} \frac{A_i}{P_i^{m_i}}$$

avec $\partial A_i < m_i \partial P_i$.

c) ***Éléments simples.*** Considérons enfin le cas où $F = \dfrac{A}{P^m}$ où P est irréductible, $\partial A < m\partial P$. Supposons que $m \geqslant 2$, et notons $A = PQ + R$ la division euclidienne de A par P. On trouve $F = \dfrac{R}{P^m} + \dfrac{Q}{P^{m-1}}$. Par récurrence sur m, on trouve donc que F s'écrit

$$\sum_{k=1}^{m} \frac{R_k}{P^k}$$

avec $\partial R_k < \partial P$. Cette décomposition est encore unique.

d) Mettant tout cela ensemble, on trouve que toute fraction rationnelle $F = \dfrac{A}{B}$ s'écrit de façon unique sous la forme :

$$F = E + \sum_{i=1}^{k} \sum_{j=1}^{m_i} \frac{R_{i,j}}{P_i^j}$$

où $B = b \prod P_i^{m_i}$ est la décomposition de B en facteurs irréductibles (et $b \in K^*$), E et $R_{i,j}$ sont des polynômes avec $\partial R_{i,j} < \partial P_i$.
Cette décomposition s'appelle la *décomposition* de F *en éléments simples.*

Lorsque P_i est un polynôme du premier degré - c'est toujours le cas si $K = \mathbb{C}$ - les $R_{i,j}$ sont de degré nul, donc des éléments de K.

Dans le cas où $K = \mathbb{R}$, on peut avoir des P_i du deuxième degré ; on aura alors des termes du premier degré au numérateur.

3.4 Exercices

3.1 Exercice. *Racines rationnelles*
Soit $P = \displaystyle\sum_{k=0}^{n} a_k X^k$ un polynôme à coefficients entiers. Soit $x = \dfrac{p}{q}$ une racine rationnelle de P écrite sous forme irréductible. Démontrer que $p|a_0$ et $q|a_n$.

3.2 Exercice. Factoriser le polynôme $P = X^5 - 4X^4 + 9X^3 - 21X^2 + 20X - 5$ sachant qu'il s'écrit comme un produit de trois polynômes à coefficients entiers.

3.3 Exercice. Décomposer en éléments simples dans $\mathbb{R}[X]$ la fraction rationnelle $F = \dfrac{X^2+2}{X^3(X-1)^2}$.

En déduire une primitive de l'application $t \mapsto \dfrac{t^2+2}{t^3(t-1)^2}$.

3.4 Exercice. Trouver un polynôme $P \in K[X]$ de degré 3 tel que $P(0) = 1$, $P'(0) = 0$, $P(1) = 0$ et $P'(1) = 1$. Quels sont les polynômes $Q \in K[X]$ qui vérifient $Q(0) = 1$, $Q'(0) = 0$, $Q(1) = 0$ et $Q'(1) = 1$?

3.5 Exercice. Calculer des primitives des fonctions

a) $x \mapsto \dfrac{1}{x^4 - x^2 - 2}$; b) $x \mapsto \dfrac{x+1}{(x^2+1)^2}$; c) $x \mapsto \dfrac{x+1}{x(x-1)^6}$; d) $x \mapsto \dfrac{1}{\cos^3 x}$.

3.6 Exercice. Résoudre le système d'équations $\begin{cases} x+y+z=3 \\ xy+yz+zx=1 \\ x^3+y^3+z^3=15 \end{cases}$ d'inconnues $x, y, z \in \mathbb{C}$.

3.7 Exercice. Soit K un corps et $a, b \in \mathbb{N}$. On considère les polynômes $A = X^a - 1$ et $B = X^b - 1$ de $K[X]$.

1. On suppose $b \neq 0$. Quel est le reste de la division euclidienne de A par B ?
2. Quel est le PGCD D de A et B ?
3. Écrire une relation de Bézout $D = AU + BV$.
4. Autre méthode : décomposer A et B en facteurs irréductibles dans $\mathbb{C}$. Pourquoi cela donne-t-il le PGCD de A et B vus comme éléments de $\mathbb{Q}[X]$?

3.8 Exercice. Soit $P \in \mathbb{R}[X]$ un polynôme unitaire sans racines réelles.

1. Démontrer qu'il existe un polynôme $A \in \mathbb{C}[X]$ tel que $P = \overline{A}\,A$ et A et $\overline{A}$ soient premiers entre eux.

   Notons k le degré de A.
2. Démontrer qu'il existe un unique polynôme $J \in \mathbb{C}[X]$ de degré $< 2k$ tel que $J \equiv i\ [A]$ et $J \equiv -i\ [\overline{A}]$.
3. Démontrer que $J \in \mathbb{R}[X]$ et $J^2 \equiv -1\ [P]$.
4. Un espace vectoriel complexe peut être considéré comme $\mathbb{R}$-espace vectoriel. Inversement, soient E un $\mathbb{R}$-espace vectoriel et j un endomorphisme de E tel que $j^2 = -\mathrm{id}_E$.
   a) Démontrer qu'il existe une unique structure d'espace vectoriel sur E telle que, pour $s, t \in \mathbb{R}$ et $x \in E$ on ait $(s+it)x = sx + tj(x)$.
   b) Munissons E de cette structure. Démontrer que les endomorphismes du $\mathbb{C}$-espace vectoriel E sont les endomorphismes f du $\mathbb{R}$ espace vectoriel E tels que $j \circ f = f \circ j$.
5. Soit E un $\mathbb{R}$ espace vectoriel de dimension finie et f un endomorphisme de E sans valeurs propres réelles. Démontrer qu'il existe sur E une structure d'espace vectoriel complexe telle que f soit $\mathbb{C}$-linéaire.

3.9 Exercice. Soit $P \in K[X]$.

1. Décomposer $\dfrac{P'}{P}$ en éléments simples.
2. *Théorème de Lucas.* On suppose $K = \mathbb{C}$. Démontrer que l'ensemble des zéros de P' est inclus dans l'enveloppe convexe de l'ensemble des zéros de P.

3. *Ellipse de Steiner.* Soient $\alpha, \beta, \gamma \in \mathbb{C}$ les affixes de trois points non alignés et notons P le polynôme $P = (X-\alpha)(X-\beta)(X-\gamma)$. On veut démontrer qu'il existe une unique ellipse (appelée ellipse de Steiner) inscrite dans le triangle de sommets (α, β, γ) et tangente aux côtés du triangle en leur milieu dont les foyers sont les racines de P'.
   a) Démontrer qu'il existe une unique application affine (sur $\mathbb{R}$) $\ell : \mathbb{C} \to \mathbb{C}$ telle que $\ell(1) = \alpha$, $\ell(j) = \beta$, $\ell(j^2) = \gamma$ (où $j = e^{\frac{2i\pi}{3}}$). Démontrer qu'il existe $a, b, c \in \mathbb{C}^2$ tels que $\ell(z) = az + b\overline{z} + c$ pour tout $z \in \mathbb{C}$ et que l'on a $P = (X-c)^3 - 3ab(X-c) - a^3 - b^3$.
   b) Démontrer qu'il existe une unique ellipse qui soit tangente au milieu des trois côtés du triangle (α, β, γ). Démontrer que les affixes des foyers de cette ellipse sont les racines de P'.

3.10 Exercice. *Hyperbole et triangle équilatère.* Dans le plan affine euclidien on considère une hyperbole équilatère H. Notons O son centre de symétrie. Soient P un point de H, P' son symétrique par rapport à O et $\mathcal{C}$ le cercle de centre P et de rayon PP'.

1. Démontrer que $\mathcal{C}$ et H se coupent en quatre points (avec la possibilité que P' soit un point double).
2. On note A, B, C les trois autres points d'intersection de $\mathcal{C}$ avec H. Démontrer que le centre de gravité du triangle ABC est P ; en déduire que c'est un triangle équilatéral.

3.11 Exercice. *Polynômes à racines de module* 1
Soit P un polynôme unitaire à coefficients entiers. Notons $x_1, \ldots, x_n$ les racines de P (comptées avec leur multiplicité), de sorte que $P = \prod_{k=1}^{n} (X - x_k)$.

1. On suppose que pour tout k, on a $|x_k| = 1$.
   a) Soit $\ell \in \mathbb{N}$. Démontrer qu'il existe un polynôme unitaire P_ℓ à coefficients entiers dont les racines sont les x_k^ℓ - autrement dit que le polynôme $P_\ell = \prod_{k=1}^{n} (X - x_k^\ell)$ est à coefficients entiers.
   b) Soit $Q = X^n + \sum_{j=0}^{n-1} a_j X^j \in \mathbb{C}[X]$ un polynôme dont toutes les racines sont de module 1. Démontrer que $|a_j| \leqslant \binom{n}{j}$.
   c) En déduire qu'il existe ℓ et m tels que tels que $\ell \neq m$ et $P_\ell = P_m$.
   d) Démontrer qu'il existe une permutation $\sigma \in \mathfrak{S}_n$ telle que, pour tout k, on ait $x_k^\ell = x_{\sigma(k)}^m$.
   e) En déduire que pour tout $r \in \mathbb{N}$, on a $x_k^{\ell^r} = x_{\sigma^r(k)}^{m^r}$.
   f) Démontrer que toutes les racines de P sont des racines de 1.
2. On suppose que toutes les racines de P sont réelles comprises entre -2 et 2. Démontrer qu'elles sont de la forme $2\cos q\pi$ avec $q \in \mathbb{Q}$ (*Considérer un polynôme Q tel que $Q(x) = x^n P(x + 1/x)$*).
3. Soit A une matrice symétrique à coefficients entiers de norme $\leqslant 2$. Démontrer que les valeurs propres de A sont de la forme $2\cos q\pi$ avec $q \in \mathbb{Q}$.

3.12 Exercice. *Résultant de deux polynômes.* Soit K un corps. Pour $n \in \mathbb{N}$, notons E_n l'espace vectoriel des polynômes de degré $< n$.

Soient $A, B \in K[X]$ des polynômes non nuls. Posons $m = \partial A$ et $n = \partial B$ et écrivons $A = \sum_{k=0}^{m} a_k X^k$,

$B = \sum_{k=0}^{n} b_k X^k$. On considère l'application linéaire $f_{A,B} : E_n \times E_m \to E_{m+n}$ définie par $f_{A,B}(P,Q) = AP + BQ$. Pour $k = 0, \ldots, n-1$, notons C_k la matrice colonne à $n+m$ lignes :

$$C_0 = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_m \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad C_1 = \begin{pmatrix} 0 \\ a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_m \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots \quad C_k = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_m \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots \quad C_{n-1} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}.$$

De même, pour $k = 0, \ldots, m-1$, notons D_k la matrice colonne à $n+m$ lignes :

$$D_0 = \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_n \\ 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad D_1 = \begin{pmatrix} 0 \\ b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_n \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots \quad D_k = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_n \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots \quad D_{m-1} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

(La matrice-colonne C_k commence par k lignes nulles et se termine par $n-1-k$ lignes nulles ; la matrice D_k commence par k lignes nulles et se termine par $m-1-k$ lignes nulles.)

1. Établirer l'équivalence :
   (i) les polynômes A et B sont premiers entre eux (pour $K = \mathbb{C}$ les polynômes A et B n'ont pas de racine commune) ;
   (ii) l'application f est bijective ;
   (iii) le déterminant $\mathrm{Res}_{A,B}$ de la matrice carrée de colonnes $C_0, \ldots, C_{n-1}, D_0, \ldots, D_{m-1}$ n'est pas nul. Ce déterminant s'appelle le *résultant* de A et B.
2. Pour $K = \mathbb{C}$ écrire une relation nécessaire et suffisante pour qu'un polynôme A possède des racines multiples.
3. Applications : calculer le résultant de A et B dans les cas suivants :
   a) $A = aX^2 + bX + c$ et $B = A'$;
   b) $A = X^3 + pX + q$ et $B = A'$;
   c) A quelconque $B = X - b$.

   Le résultant de A et A' s'appelle le *discriminant* de A.
4. Quelques formules sur le résultant. Démontrer que l'on a :
   a) $\mathrm{Res}_{B,A} = (-1)^{mn}\mathrm{Res}_{A,B}$ pour $A \in K[X]$ de degré m et $B \in K[X]$ de degré n ;

b) $\mathrm{Res}_{A,bB} = b^m \mathrm{Res}_{A,B}$ pour $b \in K$;

c) $\mathrm{Res}_{A,B_1B_2} = \mathrm{Res}_{A,B_1}\mathrm{Res}_{A,B_2}$;

d) si $B = \prod_{i=1}^{n}(X - y_i)$, $\mathrm{Res}(A,B) = \prod_{i=1}^{n} A(y_i)$;

e) si $A = \prod_{i=1}^{m}(X - x_i)$, $\mathrm{Res}(A,B) = (-1)^{mn}\prod_{i=1}^{m} B(x_i)$;

f) si $A = \prod_{i=1}^{m}(X - x_i)$ et $B = \prod_{i=1}^{n}(X - y_i)$, $\mathrm{Res}(A,B) = \prod_{i,j}(x_j - y_i)$.

3.13 Exercice. On se propose de démontrer le

Théorème de Sturm. *Soit $P \in \mathbb{R}[X]$ un polynôme sans racines multiples dans $\mathbb{C}$. Posons $P_0 = P$, $P_1 = P'$ et pour $k \geqslant 2$, supposant P_{k-2} et P_{k-1} construits, on écrit la division euclidienne de P_{k-2} par P_{k-1} sous la forme $P_{k-2} = Q_k P_{k-1} - P_k$. On note P_m le dernier P_k non nul. Notons A l'ensemble des nombres réels qui sont racine d'un P_k (au moins) pour $0 \leqslant k \leqslant m$. Pour $x \in \mathbb{R} \setminus A$, notons $n(x)$ le nombre de changements de signes de la suite $P_0(x), P_1(x), \ldots, P_m(x)$, c'est-à-dire le nombre de $i \in \{1, \ldots, m\}$ tels que $P_i(x)$ et $P_{i-1}(x)$ soient de signes contraires. Pour tous $a, b \in \mathbb{R} \setminus A$ tels que $a < b$, le nombre de racines de P dans l'intervalle $[a, b]$ est $n(a) - n(b)$.*

1. Démontrer que, pour tout $k < m$, P_k et P_{k+1} sont premiers entre eux. Démontrer que P_m est constant et non nul.
2. Démontrer que l'application $x \mapsto n(x)$ est constante sur tout intervalle contenu dans le complémentaire de A.

   Pour $x \in A$, on note $n_g(x)$ la limite à gauche de n en x et $n_d(x)$ sa limite à droite.
3. Soit x une racine de P_k avec $k > 0$.
   a) Démontrer que P_{k-1} et P_{k+1} ne s'annulent pas en x et sont de signes contraires. Démontrer qu'il existe un intervalle ouvert J contenant x tel que, pour $y \in J \setminus \{x\}$, le nombre de changements de signe dans la suite $P_{k-1}(y), P_k(y), P_{k+1}(y)$ soit égal à 1.
   b) Démontrer que si $x \in A$ n'est pas racine de $P_0 = P$, alors $n_g(x) = n_d(x)$.
4. Soit x une racine de P. Démontrer que $n_g(x) = n_d(x) + 1$.

   Indication : Les polynômes P et P' ont le même signe à droite de x et des signes contraires à gauche de x.
5. Établir le théorème de Sturm.

3.14 Exercice. *Résolution des équations du quatrième degré*

1. Soit $P \in K[X]$ un polynôme scindé unitaire de degré 4. Notons z_1, z_2, z_3, z_4 ses racines. Trouver un polynôme de degré 3 dont les racines sont $u_1 = z_1z_2 + z_3z_4$, $u_2 = z_1z_3 + z_2z_4$, $u_3 = z_1z_4 + z_2z_3$.
2. Si on sait résoudre les équations du troisième degré, on peut trouver u_1, u_2, u_3. Comment trouver alors les z_i ?

3.15 Exercice. Soit p un nombre premier.

1. Démontrer que dans $\mathbb{F}_p[X]$ on a l'égalité $X^p - X = \prod_{x \in \mathbb{F}_p}(X - x)$.
2. Démontrer le *théorème de Wilson* : $(p-1)! + 1 \equiv 0 \ \ [p]$.

3.16 Exercice. [Contenu d'un polynôme]

1. Soient $A, B \in \mathbb{Z}[X]$.
   Écrivons $A = \sum_{k=0}^{m} a_k X^k$, $B = \sum_{k=0}^{n} b_k X^k$ et $AB = \sum_{k=0}^{m+n} c_k X^k$. Soit p un nombre premier. On suppose que p divise tous les c_k. Démontrer que p divise tous les a_k ou tous les b_k.
   On appelle *contenu* d'un polynôme $P = \sum_{k=0}^{n} p_k X^k$ à coefficients dans $\mathbb{Z}$ et on note $c(P)$ le PGCD de ses coefficients $p_0, \ldots, p_n$.
2. Soient $A, B \in \mathbb{Z}[X]$. Démontrer que si $c(A) = c(B) = 1$, alors $c(AB) = 1$. En déduire que l'on a toujours $c(AB) = c(A)c(B)$.
3. Soient $A, B \in \mathbb{Q}[X]$ non nuls tels que $AB \in \mathbb{Z}[X]$. Démontrer qu'il existe $q \in \mathbb{Q}$ non nul tel que $qA \in \mathbb{Z}[X]$ et $\frac{1}{q}B \in \mathbb{Z}[X]$
4. Soit $P \in \mathbb{Z}[X]$ un polynôme non constant. Démontrer que si P est irréductible dans $\mathbb{Z}[X]$ il est irréductible dans $\mathbb{Q}[X]$.

3.17 Exercice. [Critère d'Eisenstein] Soient P un polynôme non constant à coefficients entiers et p un nombre premier. On suppose que p divise tous les coefficients de P sauf le coefficient dominant - et que $P(0)$ n'est pas divisible par p^2. Démontrer que P est irréductible sur $\mathbb{Q}$.

Application. Démontrer que, pour tout nombre premier p, le polynôme $\Phi_p = \sum_{k=0}^{p-1} X^k$ est irréductible sur $\mathbb{Q}$.

3.18 Exercice. (**) *Comment trouver les racines d'un polynôme dans $\mathbb{F}_p$?*
On se donne $P \in K[X]$ dont on veut trouver les racines dans K.

1. Trouver une méthode pour isoler les racines multiples.
   Indication : On pourra utiliser la dérivée de P.
2. On suppose que $K = \mathbb{F}_p$ où p est un (grand !) nombre premier. Donner une méthode pour trouver un polynôme scindé à racines simples ayant les mêmes racines que P.
   Indication : Penser au polynôme $X^p - X$.
3. On suppose que P est scindé à racines simples.
   a) Ecrire $P = AB$ où les racines de A sont des carrés dans $\mathbb{F}_p$ et celles de B ne le sont pas.
   b) Soient a, b deux racines (qu'on ne connait pas). On veut les séparer, c'est à dire écrire $P = AB$ avec a racine de A et b de B. Pour cela, on cherche un polynôme Q dont a ou b est racine mais pas l'autre, puis on prend le PGCD de P et Q. (On dit que Q sépare a et b.) Soit $c \in \mathbb{F}_p$ - distinct de a et de b. On pose $Q = (X - c)^{\frac{p-1}{2}} - 1$. Démontrer que Q sépare a et b si et seulement si $\frac{c-a}{c-b}$ n'est pas un carré.
   En choisissant c au hasard, on a donc une chance sur 2 de séparer a et b.
   c) Esquisser une méthode qui va nous permettre de trouver toutes les racines de P (le degré de P est ici supposé petit par rapport à p).

3.19 Exercice. (****) *Polynômes irréductibles dans $\mathbb{F}_p[X]$.*

1. *Fonction de Moebius.* On définit la fonction de Moebius $\mu : \mathbb{N}^* \to \mathbb{Z}$ en posant $\mu(n) = 0$ si n a des facteurs carrés, $\mu(1) = 1$ et $\mu(p_1 p_2 \ldots p_n) = (-1)^n$ si les p_i sont des nombres premiers distincts.
   a) Démontrer que si m, n sont premiers entre eux, on a $\mu(mn) = \mu(m)\mu(n)$.

b) Soient $(a_n)_{n\in\mathbb{N}^*}$ et $(b_n)_{n\in\mathbb{N}^*}$ des suites de nombres réels. Démontrer que l'on a $a_n = \sum_{d|n} b_d$ pour tout n si et seulement si on a $b_n = \sum_{d|n} \mu(\frac{n}{d}) a_d$ pour tout n.

2. On note Q l'ensemble des polynômes unitaires à coefficients dans $\mathbb{F}_p$ et P l'ensemble des polynômes unitaires irréductibles. On note N_n le nombre de polynômes unitaires irréductibles de degré n.

a) Démontrer que pour $t \in]-1/p, 1/p[$ on a

$$\frac{1}{1-pt} = \sum_{A\in Q} t^{\partial A} = \prod_{R\in P} \frac{1}{1-t^{\partial R}} = \prod_{n=1}^{+\infty} (1-t^n)^{-N_n}.$$

b) Démontrer que $p^n = \sum_{d|n} dN_d$.

Indication : Prendre le logarithme - ou la dérivée logarithmique.

c) En déduire que $nN_n = \sum_{d|n} \mu(\frac{n}{d}) p^d$.

d) Remarquant que n a au plus $\frac{n}{2}$ diviseurs distincts de n tous $\leqslant \frac{n}{2}$, en déduire que $nN_n \geqslant p^{n/2}(p^{n/2} - n/2)$, puis que $N_n > 0$ pour tout $n > 0$.

e) En déduire l'existence d'un corps à p^n éléments.

Deuxième partie

Algèbre linéaire sur un sous-corps de $\mathbb{C}$

4 Définitions et généralités

4.1 Espaces vectoriels

4.1 Définition. Soit K un corps commutatif. Un *espace vectoriel* sur K (ou K-*espace vectoriel*) est un ensemble E muni
- d'une loi de composition interne notée $+$,
- d'une loi externe (action de K) $K \times E \to E$ notée $(\lambda, x) \mapsto \lambda x$,
  telles que
  * $(E, +)$ soit un groupe commutatif ;
  * pour tous $\lambda, \mu \in K$ et tous $x, y \in E$ on a :

$$\lambda(x+y) = \lambda x + \lambda y, \quad (\lambda+\mu)x = \lambda x + \mu x, \quad (\lambda\mu)x = \lambda(\mu x) \quad \text{et} \quad 1x = x.$$

Rappelons la notion suivante qui prend un sens grâce à l'associativité et la commutativité de la somme :

4.2 Définition. Soient E un K-espace vectoriel et A une partie de E. On appelle *combinaison linéaire* d'éléments de A un élément x de E qui s'écrit sous la forme $x = \sum_{k=1}^{n} \lambda_k x_k$ où $n \in \mathbb{N}$, $\lambda_1, \ldots, \lambda_n$ sont des éléments de K et $x_1, \ldots, x_n$ des éléments de A.

4.3 Exemples.
a) Muni de l'addition et de la multiplication de K, le corps K est un K-espace vectoriel.

b) Muni de l'addition des polynômes et du produit d'un polynôme par un scalaire, $K[X]$ est un K-espace vectoriel.

c) Sur K^n on considère l'addition et l'action de K données par les formules :
$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$ et $\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$.
Muni de ces opérations, K^n est un K-espace vectoriel.

d) Plus généralement, donnons nous un entier n et une famille $(E_1, \ldots, E_n)$ de K-espaces vectoriels. Notons $\mathcal{E}$ le produit $\prod_{k=1}^{n} E_k = E_1 \times \ldots \times E_n$ des E_k. Les éléments de $\mathcal{E}$ sont des suites $(x_1, \ldots, x_n)$ où $x_k \in E_k$. Sur $\mathcal{E}$ on considère l'addition et l'action de K données par les formules : $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$ et $\lambda(x_1, \ldots, x_n) = (\lambda x_1, \ldots, \lambda x_n)$. Muni de ces opérations, $\mathcal{E}$ est un K-espace vectoriel. Cet espace s'appelle l'*espace vectoriel produit* des E_i.

4.2 Sous-espaces vectoriels

4.4 Définition. Soit E un K-espace vectoriel. On appelle *sous-espace vectoriel* de E une partie F de E, qui est un sous-groupe de E pour $+$ et telle que pour tout $x \in F$ et tout $\lambda \in K$ on ait $\lambda x \in F$.

Pour vérifier que $F \subset E$ est un sous-espace vectoriel on doit vérifier :
- $0 \in F$ et $\forall \lambda \in K$, $x, y \in F$, on a $x + y \in F$ et $\lambda x \in F$;
  ou
- $F \neq \emptyset$ et $\forall \lambda, \mu \in K$, $x, y \in F$, on a $\lambda x + \mu y \in F$.

Plus généralement, un sous-espace vectoriel est stable par combinaisons linéaires :

4.5 Proposition. *Soient E un K-espace vectoriel et F un sous-espace vectoriel de E. Toute combinaison linéaire d'éléments de F est dans F.*

4.6 Proposition. *Soient E un K-espace vectoriel. L'intersection d'une famille de sous-espaces vectoriels de E est un sous-espace vectoriel de E.*

Autrement dit, si $(E_i)_{i\in I}$ est une famille de sous-espaces vectoriels de E, son intersection *i.e.* l'ensemble $\bigcap_{i\in I} E_i = \{x \in E;\ \forall i \in I,\ x \in E_i\}$ est un sous-espace vectoriel de E.

4.7 Exemples. Soit E un K-espace vectoriel.

a) Soit A une partie de E. Il existe un plus petit sous-espace vectoriel de E qui contient A : l'intersection de tous les sous-espaces de E contenant A.

b) Soit $(E_i)_{i\in I}$ une famille de sous-espaces de E. Il existe un plus petit sous-espace vectoriel de E qui contient tous les E_i : c'est le plus petit sous-espace de E contenant leur réunion $A = \bigcup_{i\in I} E_i$.

4.8 Définition. Soit E un K-espace vectoriel.

a) Soit A une partie de E. Le plus petit sous-espace vectoriel de E qui contient A s'appelle le *sous-espace vectoriel engendré* par A. Nous le noterons $\mathrm{Vect}(A)$.

b) Soit $(E_i)_{i\in I}$ une famille de sous-espaces vectoriels de E. Le plus petit sous-espace vectoriel de E qui contient tous les E_i s'appelle la *somme* des E_i et se note $\sum_{i\in I} E_i$. Si $I = \{1, \ldots, n\}$ cette somme se note aussi $E_1 + \cdots + E_n$.

4.9 Proposition. *Soit E un K-espace vectoriel.*

a) Soit A une partie de E. Le sous-espace engendré par une partie A de E est l'ensemble des combinaisons linéaires d'éléments de A.

b) Soit $(E_1, \ldots, E_n)$ des sous-espaces vectoriels de E. La somme $\sum_{i=1}^{n} E_i$ des E_i est l'ensemble $\Big\{ \sum_{k=1}^{n} x_k;\ (x_1, \ldots, x_n) \in E_1 \times \ldots \times E_n \Big\}$.

Pour établir cette proposition, on démontre que les combinaisons linéaires d'éléments de A (*resp.* des sommes d'éléments des E_k) forment un sous-espace vectoriel et on utilise la proposition 4.5 pour démontrer que c'est le plus petit.

4.10 Définition. Soit E un K-espace vectoriel.

a) Deux sous-espaces F, G de E sont dits *supplémentaires* si $F + G = E$ et $F \cap G = \{0\}$.

b) Soient $n \in \mathbb{N}$ ($n \geqslant 2$) et $(E_1, \ldots, E_n)$ des sous-espaces de E. On dit que les sous-espaces E_j sont *en somme directe* si l'application $(x_1, \ldots, x_n) \mapsto x_1 + \ldots + x_n$ est injective.

4.3 Applications linéaires

4.11 Définition. Soient E, F deux K-espaces vectoriels.

- Une application $f : E \to F$ est dite *linéaire* (ou *K-linéaire*) si $\forall x, y \in E$ et $\forall \lambda \in K$ on a $f(x+y) = f(x) + f(y)$ et $f(\lambda x) = \lambda f(x)$.
- Une application linéaire de E dans E s'appelle aussi un *endomorphisme* de E.
- On appelle *isomorphisme* (d'espaces vectoriels) une application linéaire bijective.

• On appelle *automorphisme* un endomorphisme bijectif.

4.12 Proposition. *a) La composée d'applications linéaires est linéaire.*

b) La réciproque d'un isomorphisme est linéaire : c'est un isomorphisme.

4.13 Exemple. Soient E un espace vectoriel et F, G deux sous-espaces supplémentaires de E. Pour tout $x \in E$, il existe un unique élément $y \in F$ tel que $x - y \in G$. Notons $P(x)$ cet unique élément. L'application $P : E \to E$ ainsi définie (d'image égale à F) est linéaire. On l'appelle le *projecteur sur F parallèlement à G*. Pour $y \in F$ et $z \in G$, on a $P(y + z) = y$. Remarquons que $P \circ P = P$: en d'autres termes P est idempotent.

Inversement, tout endomorphisme idempotent est de cette forme.

4.14 Proposition. *Soient E, F des espaces vectoriels et $f : E \to F$ une application linéaire. L'image $f(E_1)$ d'un sous-espace vectoriel E_1 de E est un sous-espace vectoriel de F ; l'image réciproque $f^{-1}(F_1)$ d'un sous-espace vectoriel F_1 de F est un sous-espace vectoriel de E.*

4.15 Définition. Soient E, F des espaces vectoriels et $f : E \to F$ une application linéaire. On appelle *image* de f et on note $\operatorname{im} f$ le sous-espace $f(E)$ de F ; on appelle *noyau* de f et on note $\ker f$ le sous-espace $f^{-1}(\{0\})$ de E.

4.16 Proposition. *Soient E, F des espaces vectoriels et $f : E \to F$ une application linéaire. L'application f est injective si et seulement si $\ker f = \{0\}$; l'application f est surjective si et seulement si $\operatorname{im} f = F$.*

4.17 Proposition. *Soient E, F des espaces vectoriels et $f : E \to F$ une application linéaire. Soit E_1 un supplémentaire de $\ker f$ dans E et notons $g : E_1 \to \operatorname{im} f$ l'application $x \mapsto f(x)$. Alors g est un isomorphisme.*

4.4 Ensembles d'applications linéaires

4.18 Proposition. *Soient E, F des K-espaces vectoriels.*

a) Soient f, g des applications linéaires de E dans F et $\lambda \in K$. Les applications $f + g : x \mapsto f(x) + g(x)$ et $\lambda f : x \mapsto \lambda f(x)$ (de E dans F) sont linéaires.

b) Muni de ces opérations, l'ensemble des application linéaires de E dans F est un K-espace vectoriel noté $L(E, F)$.

Lorsque $E = F$, l'espace $L(E, F)$ se note $L(E)$. Muni de l'addition et de la composition des applications linéaires, $L(E)$ est un anneau. De plus, les structures d'espace vectoriel et d'anneau sont compatibles au sens suivant : pour $g \in L(E)$, les applications $f \mapsto g \circ f$ et $f \circ g$ sont linéaires. En d'autres termes, $L(E)$ est une K-algèbre.

Rappelons pour mémoire la définition d'une K-algèbre [1] :

4.19 Définition. Une K-algèbre est un ensemble A muni de trois lois :
• une addition + (qui est une loi interne $A \times A \to A$) ;
• une multiplication $(a, b) \mapsto ab$ (interne) ;
• une loi externe $K \times A \to A$, notée $(\lambda, a) \mapsto \lambda a$.
Ces lois doivent satisfaire :

a) muni des lois internes (addition et multiplication) A est un anneau ;

b) muni de l'addition et de la loi externe A est un espace vectoriel ;

c) les multiplications interne et externe vérifient : $\forall a, b \in A$ et $\forall \lambda \in K$ on a $(\lambda a)b = \lambda(ab) = a(\lambda b)$.

1. Nos algèbres sont supposées associatives. Cette convention n'est pas prise par tous les ouvrages.

4.20 Proposition. *L'ensemble des automorphismes d'un K-espace vectoriel E est un groupe (pour la composition). On l'appelle* groupe linéaire *de E et on le note $GL(E)$.*

Pour démontrer que $GL(E)$ est un groupe, on démontre en fait que c'est un sous-groupe du groupe des bijections de E dans E : l'application identité id_E de E est linéaire, et on applique la proposition 4.12.

4.5 Familles libres, génératrices, bases

4.5.1 Familles, familles de vecteurs

Soient X et I des ensembles. On appelle *famille* d'éléments de X indicée par I une application de I dans X. Cependant, la notation est un peu modifiée. Si f est une famille d'éléments de X indicée par I, l'élément $f(i)$ (pour un point $i \in I$) se note avec i en indice, par exemple x_i. La famille f elle-même se note $(x_i)_{i\in I}$.

Soient $(x_i)_{i\in I}$ et $(y_j)_{j\in J}$ des familles d'éléments de X. On dira que $(x_i)_{i\in I}$ est une *sous-famille* de $(y_j)_{j\in J}$ (on dit parfois que $(y_j)_{j\in J}$ est une sur-famille de $(x_i)_{i\in I}$) si $I \subset J$ et, pour tout $i \in I$, on a $x_i = y_i$.

Soit E un K-espace vectoriel. Une *famille de vecteurs* (de E) est donc une application d'un ensemble I dans E notée $(x_i)_{i\in I}$. On parle aussi parfois de *système de vecteurs*. On s'intéressera ici surtout au cas des familles finies $(x_i)_{i\in I}$, c'est à dire au cas où I est un ensemble fini. Le plus souvent, on prendra $I = \{1, \ldots, n\}$.

4.21 Remarque. Une partie A de E détermine une famille de vecteurs : $(x)_{x\in A}$ (qui est l'application de A dans E qui à $x \in A$ associe $x \in E$).

4.5.2 Applications linéaires de K^I dans E

Fixons un ensemble fini I. Rappelons que K^I est le K-espace vectoriel des familles d'éléments de K indicées par I, *i.e.* des applications de I dans K Pour $i \in I$, notons $e_i \in K^I$ l'élément $(s_j)_{j\in I}$ déterminé par $s_i = 1$ et $s_j = 0$ pour $j \neq i$.

Remarquons qu'un élément $(\lambda_i)_{\in I}$ s'écrit alors $\displaystyle\sum_{i\in I} \lambda_i e_i$.

4.22 Proposition. *Soit E un K-espace vectoriel.*

a) Soit $(x_i)_{i\in I}$ une famille finie de vecteurs de E. L'application $f : (\lambda_i)_{i\in I} \mapsto \displaystyle\sum_{i\in I} \lambda_i x_i$ de K^I dans E est linéaire.

b) Toute application linéaire f de K^I dans E est de cette forme : il existe une unique famille $(x_i)_{i\in I}$ d'éléments de E telle que pour tout $(\lambda_i)_{i\in I} \in K^I$ on ait $f((\lambda_i)_{i\in I}) = \displaystyle\sum_{i\in I} \lambda_i x_i$.

On a $x_i = f(e_i)$ pour tout $i \in I$.

4.5.3 Familles libres, génératrices, bases

4.23 Définition. Soient E un K-espace vectoriel $(x_i)_{i\in I}$ une famille finie de vecteurs de E. Notons $f : K^I \to E$ l'application $(\lambda_i)_{i\in I} \mapsto \displaystyle\sum_{i\in I} \lambda_i x_i$.

- On dit que la famille $(x_i)_{i\in I}$ est *libre* si f est injective (sinon, on dit qu'elle est *liée*) ;
- on dit que la famille $(x_i)_{i\in I}$ est *génératrice* si f est surjective ;
- on dit que la famille $(x_i)_{i\in I}$ est une *base* de E si f est bijective.

4.24 Remarques. a) La famille $(x_i)_{i\in I}$ est libre si le noyau de f est réduit à $\{0\}$, c'est-à-dire si la condition $\sum_{i\in I} \lambda_i x_i = 0$ implique que tous les λ_i sont nuls.

b) L'image de l'application f est le sous-espace vectoriel de E engendré par $\{x_i;\ i \in I\}$; la famille $(x_i)_{i\in I}$ est génératrice si ce sous-espace est E.

c) La famille $(x_i)_{i\in I}$ est une base si elle est à la fois libre et génératrice.

4.25 Proposition. *a) Une sous-famille d'une famille libre est libre.*

b) Une sur-famille d'une famille génératrice est génératrice.

4.26 Généralisation. Soient E un K-espace vectoriel et $(x_i)_{i\in I}$ une famille quelconque de vecteurs de E.

a) La famille $(x_i)_{i\in I}$ est dite génératrice si le sous-espace engendré par $\{x_i;\ i \in I\}$ est E ;

b) la famille $(x_i)_{i\in I}$ est dite libre si toute sous-famille finie est libre ;

c) la famille $(x_i)_{i\in I}$ est une base si elle est à la fois libre et génératrice.

4.27 Proposition. *Soit $(x_i)_{i\in I}$ une famille de vecteurs de E. Les propriétés suivantes sont équivalentes.*

(i) *$(x_i)_{i\in I}$ est libre maximale : toute sur-famille libre de $(x_i)_{i\in I}$ est égale à $(x_i)_{i\in I}$;*

(ii) *$(x_i)_{i\in I}$ est génératrice minimale : toute sous-famille génératrice de $(x_i)_{i\in I}$ est égale à $(x_i)_{i\in I}$;*

(iii) *$(x_i)_{i\in I}$ est une base.*

4.6 Matrices

Soient I, J deux ensembles finis et K un corps. Une *matrice* de type $I \times J$ à coefficients dans K est une famille d'éléments de K indicée par $I \times J$. On la représente par un tableau dont les lignes sont indicées par I et les colonnes par J. On note $\mathcal{M}_{I,J}(K)$ l'espace des matrices de type $I \times J$ à coefficients dans K. Si $I = \{1, \dots, m\}$ et $J = \{1, \dots, n\}$, les matrices de type $I \times J$ s'appellent des matrices d'ordre m, n et on écrit $\mathcal{M}_{m,n}(K)$ plutôt que $\mathcal{M}_{I,J}(K)$. Enfin lorsque $I = J$ (ou $m = n$) on parle de matrices carrées de type I (ou d'ordre m). On note $\mathcal{M}_n(K)$ l'ensemble des matrices carrées d'ordre n.

4.6.1 Applications linéaires de K^J dans K^I

Soient I et J deux ensembles finis. Il résulte en particulier de la proposition 4.22 qu'une application K-linéaire f de K^J dans K^I est déterminée par une famille $(x_j)_{j\in J}$ d'éléments de K^I. Une telle famille est donnée par une matrice $(a_{i,j})_{(i,j)\in I\times J}$ à coefficients dans K, appelée *matrice de f*, et l'on a donc

- $f(e_j) = (a_{i,j})_{i\in I}$ pour tout $j \in J$;
- $f((\lambda_j)_{j\in J}) = (\mu_i)_{i\in I}$ avec $\mu_i = \sum_{j\in J} a_{i,j}\lambda_j$, pour tout $(\lambda_j)_{j\in J} \in K^J$.

4.6.2 Produit matriciel

Soient I, J, L trois ensembles finis, $f : K^L \to K^J$ et $g : K^J \to K^I$ des applications linéaires. Notons $A = (a_{j,\ell})_{(j,\ell)\in J\times L}$ et $B = (b_{i,j})_{(i,j)\in I\times J}$ leurs matrices respectives. La matrice de $g \circ f$ est $(c_{i,\ell})_{(i,\ell)\in I\times L}$ où $c_{i,\ell} = \sum_{j\in J} b_{i,j}a_{j,\ell}$. Cette matrice s'appelle le produit des matrices B et A et se note BA.

4.6.3 Matrices inversibles. Groupe $GL(n, K)$

Soit J un ensemble fini. La matrice de l'application identité de K^J dans lui même est la matrice carrée appelée matrice identité $(\delta_{i,j})_{(i,j)\in J\times J}$ telle que, pour tout $i, j \in I$ on ait $\delta_{i,j} = 1$ si $i = j$ et $\delta_{i,j} = 0$ si $i \neq j$. Convenons de noter 1_J cette matrice. Pour $J = \{1, \ldots, n\}$ on écrira plutôt 1_n ou I_n.

Une matrice $A \in \mathcal{M}_{I,J}(K)$ est dite inversible si elle représente un isomorphisme, *i.e.* s'il existe $B \in \mathcal{M}_{J,I}(K)$ telle que $AB = 1_I$ et $BA = 1_J$.

On appelle *groupe linéaire (d'ordre n)* et l'on note $GL(n, K)$ le groupe des matrices carrées d'ordre n inversibles.

4.7 Exercices

4.1 Exercice. Soit E un K-espace vectoriel.

1. Soient F, G deux sous-espaces vectoriels de E. Démontrer qu'ils sont supplémentaires si et seulement si l'application $s : (x, y) \mapsto x + y$ de $F \times G$ dans E est bijective.
2. Soient $n \in \mathbb{N}$ et $E_1, \ldots, E_n$ des sous-espaces de E. Démontrer que les espaces E_j sont en somme directe si et seulement si on a $(E_1 + \ldots + E_k) \cap E_{k+1} = \{0\}$ pour tout $k \in \{1, \ldots, n-1\}$.

Commentaire. Le fait que l'intersection deux à deux des espaces E_i est réduite à $\{0\}$ n'implique pas en général que leur somme est directe. Par exemple, la somme de trois droites distinctes d'un plan vectoriel n'est pas directe puisque le plan est engendré par deux d'entre elles.

4.2 Exercice. On note E l'ensemble des fonctions continues de $\mathbb{R}$ dans $\mathbb{R}$.

1. Démontrer que E est naturellement muni d'une structure de $\mathbb{R}$-espace vectoriel.
2. On note $P \subset E$ et $I \subset E$ les sous-ensembles formés des fonctions continues paires et impaires respectivement. Démontrer que P et I sont des sous-espaces vectoriels supplémentaires de E.
3. Donner quelques exemples de décomposition $f = p + i$ avec $f \in E$, $p \in P$ et $i \in I$.

4.3 Exercice. Soient F, G, H des sous-espaces vectoriels d'un espace vectoriel E. On suppose que $G \subset H$, $F \cap H \subset F \cap G$ et $F + H \subset F + G$. Démontrer que $G = H$.

4.4 Exercice.

1. Soient F, G des sous-espaces vectoriels d'un espace vectoriel E. On suppose que $F \cup G$ est un sous-espace vectoriel de E. Démontrer que l'on a $F \subset G$ ou $G \subset F$?
2. Soient $F_1, \ldots, F_n$ des sous-espaces vectoriels stricts ($F_j \neq E$) d'un K-espace vectoriel E.
   a) Soit $k \in \{1, \ldots, n-1\}$ et soient $x, y \in E$ tels que $x \notin \bigcup_{i=1}^{k} F_i$ et $y \notin F_{k+1}$. Démontrer que pour $j \in \{1, \ldots, k\}$ il existe au plus un $\lambda_j \in K$ tel que $y + \lambda_j x \in F_j$.
   b) On suppose que K est infini. Démontrer que $\bigcup_{i=1}^{n} F_i \neq E$.

4.5 Exercice. Soient E, F des espaces vectoriels et $f : E \to F$ une application. Démontrer que f est linéaire si et seulement si son graphe $G_f = \{(x, f(x));\ x \in E\}$ est un sous-espace vectoriel de l'espace vectoriel produit $E \times F$.

4.6 Exercice. Soient E, F, G des espaces vectoriels, $f : E \to F$ et $g : F \to G$ des applications linéaires. Démontrer que $\ker g \cap \operatorname{im} f = f(\ker g \circ f)$.

4.7 Exercice.

Soient $a, b \in K$. Notons $E \subset K^{\mathbb{N}}$ l'ensemble des suites $(x_n)_{n\in K}$ telles que, pour tout $n \geqslant 2$ on ait $x_n = ax_{n-1} + bx_{n-2}$.

1. Démontrer que E est un sous-espace vectoriel de $K^{\mathbb{N}}$.
2. Soit $(x_n)_{n\in\mathbb{N}}$ un élément de E tel que $x_0 = x_1 = 0$. Démontrer que l'on a $x_n = 0$ pour tout $n \in \mathbb{N}$.
3. Posons $A = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}$. Écrivons $A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} u_n \\ v_n \end{pmatrix}$. Démontrer que
   a) pour tout $n \in \mathbb{N}$ on a $v_{n+1} = u_n$;
   b) $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont des éléments de E ;
   c) $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ forment une base de E.
4. Posons $F = \{(x_n)_{n\in\mathbb{N}};\ x_0 = x_1 = 0\}$. Démontrer que E et F sont des sous-espaces supplémentaires de $K^{\mathbb{N}}$.

5 Théorie de la dimension

5.1 Espaces vectoriels de dimension finie

5.1 Définition. On dit qu'un K-espace vectoriel est de *dimension finie* s'il possède une famille génératrice finie.

Il sera ici plus commode de raisonner en termes de *parties* libres ou génératrices d'un espace vectoriel :

5.2 Remarque. Soit E un K-espace vectoriel. Une partie X de E détermine une famille $(x)_{x\in X}$ et l'on peut donc parler de parties libres ou génératrices. Soit$(x_i)_{i\in I}$ une famille de vecteurs de E. Posons $X = \{x_i;\ i \in I\}$. La famille $(x_i)_{i\in I}$ est une famille génératrice de E si et seulement si X est une partie génératrice de E ; la famille $(x_i)_{i\in I}$ est une famille libre de E si et seulement si X est une partie libre de E et l'application $i \mapsto x_i$ est injective.

5.3 Théorème de la base incomplète. *Soient E un K-espace vectoriel, $G \subset E$ une partie génératrice finie de E et $L \subset G$ une partie libre de E. Alors il existe une base B de E telle que $L \subset B \subset G$.*

L'ensemble $\mathcal{G} = \{X$ partie génératrice de $E;\ L \subset X \subset G\}$ n'est pas vide puisque $G \in \mathcal{G}$. Un élément B de $\mathcal{G}$ qui possède un nombre minimum d'éléments est une base de E.

5.4 Corollaire. *Soit E un K-espace vectoriel de dimension finie.*

a) Toute partie génératrice finie de E contient une base ;

b) toute partie libre finie est contenue dans une base.

Pour (a) on applique le théorème de la base incomplète à $L = \emptyset$; pour (b) si L est une partie libre finie et G_1 est une partie génératrice finie, on applique le théorème de la base incomplète à L et $G = L \cup G_1$.

5.2 Dimension d'un espace vectoriel

5.5 Lemme d'échange (Steinitz). *Soit $G \subset E$ une partie génératrice finie, $x \in G$ et $y \in E$. Écrivons $y = \sum_{z\in G} \lambda_z z$, et supposons que $\lambda_x \neq 0$. Alors $(G \setminus \{x\}) \cup \{y\}$ est génératrice.*

Écrivons $G_1 = G \setminus \{x\}$ et $G_2 = G_1 \cup \{y\}$. On a $x = \lambda_x^{-1}\left(y - \sum_{z\in G_1} \lambda_z z\right)$, donc $x \in \mathrm{Vect}(G_2)$. Il vient $G \subset \mathrm{Vect}(G_2)$, donc $E = \mathrm{Vect}(G) \subset \mathrm{Vect}(G_2)$.

5.6 Théorème. *Soient E un espace vectoriel, G une partie génératrice finie de E et L une partie libre de E. Alors L est finie et* $\mathrm{Card}(L) \leqslant \mathrm{Card}(G)$.

Supposons d'abord que L soit finie et démontrons que $\mathrm{Card}(L) \leqslant \mathrm{Card}(G)$.

On raisonne par récurrence sur le nombre N d'éléments de L qui ne sont pas dans G.

- Si $N = 0$, alors $L \subset G$, donc $\mathrm{Card}(L) \leqslant \mathrm{Card}(G)$.
- Soit $N \in \mathbb{N}$ et supposons que l'on ait démontré que si L et G sont deux parties finies de E avec L libre et G génératrice et $\mathrm{Card}(L \setminus G) = N$, alors $\mathrm{Card}(G) \geqslant \mathrm{Card}(L)$.
  Soient maintenant L une partie libre et G une partie génératrice de E telles que $\mathrm{Card}(L\setminus G) = N+1$. Posons $L_1 = (G \cap L)$. Soit $y \in L \setminus G$. Comme G est génératrice, on peut écrire $y = \sum_{z\in G} \lambda_z z$. Comme L est libre, il vient $y \notin \mathrm{Vect}(L_1)$, donc il existe $x \in G \setminus L_1$ tel que $\lambda_x \neq 0$. Par le lemme d'échange $G_1 = (G \setminus \{x\}) \cup \{y\}$ est génératrice et $L \setminus G_1$ a N éléments. Par l'hypothèse de récurrence, on a $\mathrm{Card}(L) \leqslant \mathrm{Card}(G_1) = \mathrm{Card}(G)$.

Enfin, une partie infinie T de E contient une partie finie de cardinal $\mathrm{Card}(G)+1$, qui ne peut être libre ; donc T n'est pas libre.

5.7 Corollaire. *Dans un espace vectoriel de dimension finie, toutes les bases sont finies et ont même nombre d'éléments.*

5.8 Définition. Soit E un espace vectoriel de dimension finie. On appelle *dimension* de E le nombre $\dim E$ d'éléments d'une base quelconque de E.

5.9 Théorème. *Soit E un espace vectoriel de dimension finie. Posons $n = \dim E$.*

a) Toutes les bases de E ont n éléments.

b) Toute famille libre de E a au plus n éléments ; une famille libre à n éléments est une base.

c) Toute famille génératrice de E a au moins n éléments ; une famille génératrice à n éléments est une base.

5.10 Théorème. *Soit E un espace vectoriel de dimension finie. Tout sous-espace vectoriel F de E est de dimension finie. On a $\dim F \leqslant \dim E$; si $\dim F = \dim E$, alors $F = E$.*

Toute partie libre de F est libre dans E donc a au plus n éléments. Notons $k(\leqslant n)$ le plus grand nombre d'éléments d'une partie libre de F et soit L une partie libre de F à k éléments. C'est une partie libre maximale, donc une base de F. Donc $\dim F = k \leqslant n$. Si $k = n$, alors L est une base de E, donc $F = E$.

5.11 Corollaire. *Tout sous-espace vectoriel d'un espace vectoriel de dimension finie possède un supplémentaire.*

En effet, soient E un espace vectoriel de dimension finie, F un sous-espace vectoriel de E et L une base de F. On peut la compléter en une base B de E. Le sous-espace vectoriel engendré par $B \setminus L$ est un supplémentaire de F.

5.12 Proposition. *Soient F, G des sous-espaces vectoriels de dimension finie d'un espace vectoriel E. Alors $F+G$ et $F \cap G$ sont de dimension finie et l'on a $\dim F + \dim G = \dim(F+G) + \dim(F \cap G)$.*

Supposons d'abord que $F \cap G = \{0\}$. On obtient une base de $F+G$ en réunissant une base de F avec une base de G : on a donc $\dim(F+G) = \dim F + \dim G$.

Dans le cas général, choisissons un supplémentaire G_1 de $F \cap G$ dans G. Alors G_1 est un supplémentaire de F dans $F+G$ et par le premier cas, on a $\dim G = \dim(F \cap G) + \dim G_1$, et $\dim(F+G) = \dim F + \dim G_1$.

5.3 Rang

5.13 Définition. a) Une famille $(x_i)_{i \in I}$ de vecteurs d'un espace vectoriel est dite de *rang fini* si l'espace vectoriel qu'elle engendre est de dimension finie. La dimension de cet espace s'appelle *rang* de la famille $(x_i)_{i \in I}$ et se note $\mathrm{rg}(x_i)_{i \in I}$.

b) Une application linéaire f est dite de *rang fini* si son image est de dimension finie. La dimension de $\mathrm{im}\, f$ s'appelle *rang* de f et se note $\mathrm{rg}(f)$.

c) Le *rang* d'une matrice d'ordre m, n est le rang de l'application linéaire de K^n dans K^m qu'elle représente.

5.14 Théorème du rang. *Soient E, F des espaces vectoriels et $f : E \to F$ une application linéaire. Si E est de dimension finie on a $\dim E = \dim(\ker f) + \mathrm{rg}(f)$.*

Cela résulte immédiatement de la proposition 4.17.

5.15 Théorème. *Soient E, F des espaces vectoriels de dimension finie et $f : E \to F$ une application linéaire.*

a) Si $\dim E < \dim F$, l'application f n'est pas surjective.

b) Si $\dim E > \dim F$, l'application f n'est pas injective.

c) Si $\dim E = \dim F$ et en particulier si $E = F$, i.e. si f est un endomorphisme, on a l'équivalence entre : (i) f est surjective ; (ii) f est injective ; (iii) f est bijective.

Pour vérifier qu'un endomorphisme d'un espace vectoriel de dimension finie est un automorphisme, il suffit de vérifier son injectivité ou sa surjectivité.

5.16 Théorème. *Deux K-espaces vectoriels de dimension finie sont isomorphes si et seulement s'ils ont même dimension.*

5.4 Exercices

5.1 Exercice. Soit E un espace vectoriel et $(x_1, \dots, x_n)$ une famille génératrice de E. Posons

$$I = \{i \in \{1, \dots n\};\ x_i \notin \mathrm{Vect}\{x_j;\ j < i\}\}.$$

1. Soit $(\lambda_j) \in K^n$ une famille non nulle telle que $\sum_{j=1}^{n} \lambda_j x_j = 0$. Soit i_0 le plus grand élément de $\{j \in \{1, \dots, n\};\ \lambda_j \neq 0\}$. Démontrer que $i_0 \notin I$.
2. Démontrer que, pour tout $j \in \{1, \dots, n\}$ on a $x_j \in \mathrm{Vect}\{x_i;\ i \in \{1, \dots j\} \cap I\}$.
3. Démontrer que $(x_i)_{i \in I}$ est une base de E.

5.2 Exercice. Soient E un espace vectoriel de dimension finie et F, G des sous-espaces vectoriels de E. Démontrer qu'il existe un automorphisme f de E tel que $f(F) = G$ si et seulement si F et G ont même dimension.

5.3 Exercice. Soit F un sous-espaces vectoriel d'un espace vectoriel E.

1. Soient G_1 et G_2 deux sous-espaces de E. On suppose qu'ils sont tous les deux supplémentaires de F. Démontrer que G_1 et G_2 sont isomorphes.
   On dit que F est de *codimension finie* dans E s'il admet un supplémentaire de dimension finie. On appelle alors *codimension* de F et l'on note $\mathrm{codim}\, F$ la dimension d'un tel supplémentaire.
2. On suppose que E est de dimension finie. Démontrer que la dimension et la codimension de F sont finies et que l'on a $\mathrm{codim}\, F = \dim E - \dim F$.
3. Démontrer que si F est un sous-espace de E de codimension finie, tout sous-espace de E contenant F est de codimension finie inférieure ou égale à celle de F.
4. Soit f une application linéaire de E dans un espace vectoriel G. Démontrer que f est de rang fini si et seulement si $\ker f$ est de codimension finie et que, dans ce cas on a $\mathrm{codim}(\ker f) = \mathrm{rg} f$.

5.4 Exercice. Soient E, F, G des espaces vectoriels $f : E \to F$ et $g : F \to G$ des applications linéaires.

1. On suppose que f est de rang fini. Démontrer que $g \circ f$ est de rang fini et que l'on a $\mathrm{rg}(g \circ f) \leqslant \mathrm{rg} f$. Plus précisément, démontrer que l'on a $\mathrm{rg}(g \circ f) = \mathrm{rg} f - \dim(\ker g \cap \mathrm{im}\, f)$.
2. On suppose que g est de rang fini. Démontrer que $g \circ f$ est de rang fini et que l'on a $\mathrm{rg}(g \circ f) \leqslant \mathrm{rg} g$. Plus précisément, démontrer que l'on a $\mathrm{rg}(g \circ f) = \mathrm{rg} g - \mathrm{codim}(\ker g + \mathrm{im}\, f)$.

5.5 Exercice. *Cet exercice m'a été proposé par Gentiana Danila et Catherine Gille.*

1. Soient p un nombre premier et $n \in \mathbb{N}^*$. Combien y a-t-il de droites dans $\mathbb{F}_p^n$? Et combien d'hyperplans (voir définition 6.20) ?
2. Combien y a-t-il de systèmes libres à k éléments dans $\mathbb{F}_p^n$? Combien y a-t-il de bases ?
3. Combien y a-t-il de sous-espaces de dimension k dans $\mathbb{F}_p^n$ (pour $0 \leqslant k \leqslant n$).
4. a) *Dîner avec le capitaine.* Nous sommes sur un bateau de croisière, au mois d'août. Il y a 31 passagers à bord et le capitaine décide d'en inviter chaque soir 6 au dîner selon la règle suivante : deux personnes doivent se trouver à la table du capitaine une et une seule fois. Aider le capitaine à organiser ses invitations.

   b) *Le jeu de Dobble* consiste en 57 cartes, chacune comportant 8 symboles, et chaque couple de cartes ayant un et un seul symbole en commun. Proposer un moyen de construction d'un tel jeu sur le même principe que le problème du capitaine. Remarquer que dans cette construction chaque symbole apparaît 8 fois (dans le vrai jeu cette règle n'est pas respectée...).

5.6 Exercice. 1. a) Soit E un sous-espace vectoriel de dimension 2 de K^4. On suppose que tout élément non nul de E a au moins 3 composantes non nulles. Démontrer que les applications $g : E \to K^2$ et $h : E \to K^2$ qui à $x \in E$ associent ses deux premières et ses deux dernières composantes respectivement sont bijectives. Démontrer que la matrice A_E de $h \circ g^{-1}$ est une matrice 2×2 inversible et à coefficients non nuls.

   b) Inversement démontrer que, pour toute matrice $A \in M_2(K)$ inversible et à coefficients non nuls, il existe un unique sous-espace vectoriel E de K^4 tel que tout élément non nul de E ait au moins 3 composantes non nulles et $A = A_E$.

2. On appelle sudoku une application $f : \mathbb{F}_3^4 \to \mathbb{F}_3^2$ telle que pour tous $x, y \in \mathbb{F}_3^4$ distincts, mais ayant leurs première et deuxième composante égale (x et y sont situés sur la même ligne dans une grille de sudoku) ou la troisième et quatrième (même colonne) ou la première et la troisième (même petit carré) on ait $f(x) \neq f(y)$. On appelle sudoku fort une application $f : \mathbb{F}_3^4 \to \mathbb{F}_3^2$ telle que pour tous $x, y \in \mathbb{F}_3^4$ distincts, mais ayant deux composantes égales on ait $f(x) \neq f(y)$.

   a) Démontrer qu'une application linéaire $f : \mathbb{F}_3^4 \to \mathbb{F}_3^2$ est un sudoku fort si et seulement si tout élément non nul de $\ker f$ a au moins trois composantes non nulles.

   b) Combien y a-t-il de sudokus forts linéaires ?

   c) Combien y a-t-il de sudokus linéaires ?

6 Matrices et bases

Dorénavant, (presque toutes) nos bases seront indicées par $\{1, \ldots, n\}$.

6.1 Matrice d'une application linéaire

6.1.1 Matrice d'une application linéaire entre espaces vectoriels munis de bases

Soient E, F des espaces vectoriels de dimension finie. Choisissons des bases $B = (e_1, \ldots, e_n)$ et $B' = (e'_1, \ldots, e'_m)$ de E et F respectivement. Par définition (*cf.* déf. 4.23), elles donnent lieu à des isomorphismes $p_B : K^n \to E$ et $p_{B'} : K^m \to F$. Soit $f : E \to F$ une application linéaire. On lui associe l'application linéaire $p_{B'}^{-1} \circ f \circ p_B : K^n \to K^m$. Notons $A = (a_{i,j})_{1 \leqslant i \leqslant m;\ 1 \leqslant j \leqslant n}$ la matrice de cette application. On a donc $f(e_j) = \sum_{i=1}^{m} a_{i,j} e'_i$.

6.1 Définition. La matrice ainsi définie s'appelle *matrice de f dans les bases B et B'*. On la note $M_{B',B}(f)$.

La matrice d'une composée est le produit des matrices :

6.2 Proposition. *Soient E, F, G des K espaces vectoriels de dimension finie munis de bases B, B', B'' respectivement. Soient $f : E \to F$ et $g : F \to G$ des applications linéaires. On a $M_{B'',B}(g \circ f) = M_{B'',B'}(g) M_{B',B}(f)$.*

6.1.2 Changements de base, matrices de passage

Donnons-nous à présent deux bases B et B_1 de E. Il est commode (usuel) d'appeler B l'« ancienne base » et B_1 la « nouvelle base ».

6.3 Définition. On appelle *matrice de passage* de la base B à la base B_1 la matrice dont les vecteurs-colonnes sont les coefficients des vecteurs de B_1 (la nouvelle base) dans la base B (l'ancienne base).

La matrice de passage P de B à B_1 est la matrice $M_{B,B_1}(\mathrm{id}_E)$ de l'identité de E allant de la base B_1 dans la base B. Soit $x \in E$; notons X (*resp.* X_1) le vecteur-colonne formé des composantes de x dans la base B (*resp.* B_1). On a $X = PX_1$.

6.4 Remarques. a) Une matrice de passage est inversible : la matrice de passage de B_1 à B est l'inverse de la matrice de passage de B à B_1.

b) Toute matrice inversible est la matrice de passage de B à une autre base : une matrice inversible P représente un automorphisme f de E dans la base B (*i.e.* $P = M_{B,B}(f)$). C'est aussi la matrice de passage de B à la base $f(B)$.

6.5 Formule de changement de base. *Soient E, F des K-espaces vectoriels de dimension finie. Donnons nous des bases B et B_1 de E et des bases B' et B'_1 de F. Notons P la matrice de passage de B à B_1 et Q la matrice de passage de B' à B'_1. Soit $f : E \to F$ une application linéaire. Les matrices M et M_1 de f dans les bases B, B' et B_1, B'_1 sont reliées par la formule $M_1 = Q^{-1} M P$.*

En effet, on écrit $M = M_{B',B}(f)$, $M_1 = M_{B'_1,B_1}(f)$, $P = M_{B,B_1}(\mathrm{id}_E)$ et $Q = M_{B',B'_1}(\mathrm{id}_F)$. Par la prop. 6.2, on a

$$QM_1 = M_{B',B'_1}(\mathrm{id}_F) M_{B'_1,B_1}(f) = M_{B',B_1}(f) = M_{B',B}(f) M_{B,B_1}(\mathrm{id}_E) = MP.$$

6.2 Matrices équivalentes, matrices semblables

6.2.1 Matrices équivalentes

6.6 Définition. Soient $m, n \in \mathbb{N}$. Deux matrices $A, B \in \mathcal{M}_{m,n}(K)$ sont dites *équivalentes* s'il existe des matrices inversibles $P \in \mathcal{M}_m(K)$ et $Q \in \mathcal{M}_n(K)$ telles que $B = P^{-1}AQ$.

Deux matrices sont donc équivalentes si elles représentent la même application linéaire (d'un espace vectoriel dans un autre) dans des bases différentes.

6.7 Proposition. *Deux matrices équivalentes ont le même rang.*

6.8 Proposition. *Soient E et F des espaces vectoriels et $f : E \to F$ une application linéaire. Notons r son rang. Il existe des bases B de E et B' de F telles que la matrice de f soit $(a_{i,j})$ avec $a_{i,j} = 1$ si $i = j \leqslant r$ et $a_{i,j} = 0$ sinon.*

En d'autres termes, $M_{B',B}(f)$ admet la décomposition par blocs $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.

Il suffit de prendre
- pour B une base $(e_1, \ldots, e_n)$ où $(e_1, \ldots, e_r)$ est la base d'un supplémentaire de $\ker f$ et $(e_{r+1}, \ldots, e_n)$ une base de $\ker f$;
- pour $j \leqslant r$ on pose $e'_j = f(e_j)$; d'après la proposition 4.17, la famille $(e'_1, \ldots, e'_r)$ est une base de $\operatorname{im} f$; on la complète en une base $B' = (e'_1, \ldots, e'_m)$ de F.

6.9 Théorème. *Deux matrices d'ordre m, n sont équivalentes si et seulement si elles ont le même rang.*

6.2.2 Transposée d'une matrice

6.10 Définition. Si $A = (a_{i,j})_{(i,j)\in I\times J}$ est une matrice de type $I \times J$, on appelle *transposée* de A la matrice ${}^tA = (b_{j,i})_{(j,i)\in J\times I}$ de type $J \times I$ donnée par $b_{j,i} = a_{i,j}$ pour tout $(j, i) \in J \times I$.

Regroupons dans la proposition suivante les principales propriétés de la transposée des matrices :

6.11 Proposition. *a) Soient I, J, L des ensembles finis. On a ${}^t1_I = 1_I$. Pour tout $A \in \mathcal{M}_{I,J}(K)$ et tout $B \in \mathcal{M}_{J,L}(K)$, on a ${}^t(AB) = {}^tB\,{}^tA$.*

b) La transposée d'une matrice carrée inversible est inversible.

c) Le rang d'une matrice est égal au rang de sa transposée.

6.2.3 Matrices extraites

6.12 Définition. Soient I, J des ensembles finis et $A = (a_{i,j})_{(i,j)\in I\times J} \in \mathcal{M}_{I,J}(K)$. Soient $I' \subset I$ et $J' \subset J$. La matrice $(a_{i,j})_{(i,j)\in I'\times J'} \in \mathcal{M}_{I',J'}(K)$ s'appelle une *matrice extraite* de A.

6.13 Exercice. Décrire l'application linéaire de $K^{J'}$ dans $K^{I'}$ associée à une matrice extraite. On sera amené à construire des applications linéaires $K^{J'} \to K^J$ et $K^I \to K^{I'}$.

6.14 Proposition. *a) Le rang d'une matrice extraite de A est inférieur ou égal à celui de A.*

b) Si le rang de A est $\geqslant r$, il existe une matrice carrée d'ordre r inversible extraite de A.

En d'autres termes, le rang de A est l'ordre de la plus grande matrice carrée inversible extraite de A.

Le (a) résulte... de l'exercice.

Pour (b), on sait que le rang de A est le rang de ses vecteurs-colonnes. Dans le système $(x_j)_{j\in J}$ qui engendre l'image de A qui est de dimension $\geqslant r$, on choisit une base $(x_j)_{j\in J_1}$ de cette image ; puisque J_1 a $\mathrm{rg}A$ éléments, on peut choisir une sous-famille $(x_j)_{j\in J'}$ a r éléments, qui sera donc libre. La matrice extraite B, de type $I \times J'$, est de rang r, donc sa transposée aussi. Raisonnant de même avec ${}^tB$, on trouve une partie $I' \subset I$ dans les colonnes de B à r éléments telle que la matrice extraite (carrée d'ordre r) soit de rang r.

6.2.4 Matrices d'endomorphismes

Dans le cas d'un endomorphisme f d'un espace vectoriel E, on va en général choisir la même base au départ et à l'arrivée, *i.e.* considérer la matrice $M_{B,B}(f)$ où B est une base de E.

6.15 Formule de changement de base. *Soient E un K-espace vectoriel de dimension finie et f un endomorphisme de E. Donnons nous des bases B et B_1 de E. Notons P la matrice de passage de B à B_1. Les matrices M et M_1 de f dans les bases B et B_1 sont reliées par la formule $M_1 = P^{-1}MP$.*

6.16 Définition. Soit $n \in \mathbb{N}$. Deux matrices $A, B \in \mathcal{M}_n(K)$ sont dites *semblables* s'il existe une matrice inversible $P \in \mathcal{M}_n(K)$ telle que $B = P^{-1}AP$.

Deux matrices sont donc semblables si elles représentent le même *endomorphisme* dans des bases différentes.

6.17 Définition. Soit $A = (a_{i,j}) \in \mathcal{M}_n(K)$ une matrice carrée. On appelle *trace* de A le nombre $\mathrm{Tr}(A) = \sum_{i=1}^{n} a_{i,i}$.

6.18 Proposition. *Soient $A \in \mathcal{M}_{m,n}(K)$ et $B \in \mathcal{M}_{n,m}(K)$ deux matrices. On a $\mathrm{Tr}\, AB = \mathrm{Tr}\, BA$.*

6.19 Corollaire. *Deux matrices semblables ont même trace.*

Cela nous permet de définir la trace d'un endomorphisme : c'est la trace de sa matrice dans n'importe quelle base.

Nous reviendrons plus longuement sur les endomorphismes au paragraphe 8.

6.3 Dualité, base duale

6.3.1 Formes linéaires ; dual d'un espace vectoriel

Soit E un K-espace vectoriel.

6.20 Définition. On appelle *hyperplan* de E un sous-espace vectoriel de codimension 1 de E. On appelle *forme linéaire* sur E une application linéaire de E à valeurs dans K. On appelle *dual* de E et l'on note E^* l'espace vectoriel $L(E, K)$ formé des formes linéaires sur E.

6.21 Proposition. *Le noyau d'une forme linéaire non nulle est un hyperplan. Inversement, tout hyperplan est noyau d'une forme linéaire.*

Soit H un hyperplan de E. Il existe donc une forme linéaire f, unique à un multiple scalaire près dont c'est le noyau. Soit $x \in E$. On a donc $x \in H \iff f(x) = 0$. On dit donc que l'équation $f(x) = 0$ est une *équation* de H.

Base duale

6.22 Proposition. *Soit E un espace vectoriel de dimension finie et soit $(e_1, \dots, e_n)$ une base de E.*

a) Pour tout $k \in \{1, \dots, n\}$, il existe une unique forme linéaire $e_k^* \in E^*$ telle que $e_k^*(e_j) = 0$ si $j \neq k$ et $e_k^*(e_k) = 1$.

b) La famille $(e_1^*, \dots, e_n^*)$ est une base de E^*.

En particulier, $\dim E^* = \dim E$.

6.23 Définition. La base $(e_1^*, \dots, e_n^*)$ de E^* s'appelle la *base duale* de $(e_1, \dots, e_n)$.

6.24 Proposition. *Soient E un espace vectoriel de dimension finie, F un sous-espace vectoriel et $x \in E \setminus F$. Il existe $f \in E^*$ telle que $F \subset \ker f$ et $x \notin \ker f$.*

Soit $(e_1, \dots e_k)$ une base de F. Posons $e_{k+1} = x$; puisque $x \notin F$, la famille $(e_1, \dots, e_{k+1})$ est libre. Complétons-la en une base $(e_1, \dots e_n)$. Il suffit alors de poser $f = e_{k+1}^*$.

6.25 Exemple. Soit $n \in \mathbb{N}$. Notons E_n le sous-espace vectoriel de $K[X]$ formé des polynômes de degré $< n$. C'est un espace vectoriel de dimension n. Soient $(x_1, \dots, x_n)$ des points distincts de K. Pour $k \in \{1, \dots, n\}$, notons f_k la forme linéaire $P \mapsto P(x_k)$. Considérons l'application linéaire $\varphi : E_n \to K^n$ définie par $\varphi(P) = (f_1(P), \dots, f_n(P))$

Si $P \in \ker \varphi$, alors P admet les racines $x_1 \dots, x_n$, donc P est le polynôme nul. L'application φ est donc injective ; puisque $\dim E_n = \dim K^n = n$, elle est bijective.

Pour $k \in \{1, \dots, n\}$, notons Q_k le polynôme $Q_k = \prod_{1 \leqslant j \leqslant n;\ j \neq k} (X - x_j)$ et posons $P_k = \dfrac{1}{Q_k(x_k)} Q_k$. La famille $(P_1, \dots, P_n)$ est une base de E_n. Sa base duale est $(f_1, \dots, f_n)$.

En particulier, si $\lambda_1, \dots, \lambda_n$ sont des éléments de K, il existe un et un seul polynôme de degré $< n$ tel que $P(x_k) = \lambda_k$ pour tout k : ce polynôme est $\sum_{k=1}^{n} \lambda_k P_k$ (*formule d'interpolation de Lagrange*).

Transposée d'une application linéaire

6.26 Définition. Soient E, F des espaces vectoriels et $\varphi : E \to F$ une application linéaire. On appelle *transposée* de φ l'application linéaire ${}^t\varphi : f \mapsto f \circ \varphi$ de F^* dans E^*.

Supposons que E et F soient des espaces vectoriels de dimension finie. Soient B et B' des bases de E et F respectivement. La matrice $M_{B^*,(B')^*}({}^t\varphi)$ de ${}^t\varphi$ de la base duale de B' dans la base duale de B est la transposée de la matrice $M_{B',B}(\varphi)$ de φ dans de la base B dans la base B'. En particulier, on a $\mathrm{rg}\, {}^t\varphi = \mathrm{rg}\, \varphi$.

6.3.2 Espaces vectoriels en dualité

Le point de vue que nous adoptons pour ce qui concerne l'orthogonalité est celui de deux espaces « en dualité ». Cela nous permet

- de traiter de façon symétrique un espace et son dual ;
- de traiter en même temps le cas d'un espace muni d'une forme bilinéaire symétrique non dégénérée comme un espace euclidien.

Soient E, F des espaces vectoriels. Il revient au même de se donner

∗ une forme bilinéaire $b : E \times F \to K$;

∗ une application linéaire $\varphi : E \to F^*$;

$*$ une application linéaire $\psi : F \to E^*$.
Ces applications sont reliées par la formule $b(x, y) = \varphi(x)(y) = \psi(y)(x)$.

Lorsqu'on s'est donné de telles applications, on dit que E et F sont des espaces vectoriels *en dualité*.

Cette généralité permet de recouvrir deux cas particuliers fondamentaux :
- $F = E^*$ et $\psi = \mathrm{id}_F$;
- $F = E$ et b est une forme bilinéaire symétrique (*i.e.* $\varphi = \psi$) voire antisymétrique (*i.e.* $\varphi = -\psi$).

Choisissons des bases $B = (e_1, \ldots, e_m)$ et $B' = (e'_1, \ldots, e'_n)$ de E et F respectivement. On appelle *matrice de la forme bilinéaire* b la matrice $A = (a_{i,j}) \in \mathcal{M}_{m,n}(K)$ définie par $a_{i,j} = b(e_i, e'_j)$. C'est la matrice $M_{B^*,B'}(\psi)$ de ψ de la base B' dans la base duale de B et la transposée de la matrice $M_{(B')^*,B}(\varphi)$ de φ dans de la base B dans la base duale de B'. On en déduit :

6.27 Proposition. *Soient E, F des espaces vectoriels de* dimension finie *en dualité. On a* $\mathrm{rg}\varphi = \mathrm{rg}\psi$. *En particulier, φ est un isomorphisme si et seulement si ψ est un isomorphisme.*

6.28 Exemple. Supposons que $F = E^*$ et $\psi = \mathrm{id}_F$. Alors $\varphi : E \to (E^*)^*$ est une application linéaire appelée *homomorphisme canonique* de E dans son *bidual* que l'on note E^{**} caractérisé par l'égalité $\varphi(x)(f) = f(x)$ pour $x \in E$ et $f \in E^*$. Lorsque E est de dimension finie, φ est un isomorphisme appelé *isomorphisme canonique*.

6.3.3 Orthogonalité

6.29 Définition. Soient E et F des espaces vectoriels en dualité. Des vecteurs $x \in E$ et $y \in F$ sont dits *orthogonaux* si $b(x, y) = 0$. L'*orthogonal* d'une partie A de E (*resp.* d'une partie B de F) est l'ensemble $A^\perp = \{y \in F;\ \forall x \in A;\ b(x, y) = 0\}$ (*resp.* l'ensemble $B^o = \{x \in E;\ \forall y \in B;\ b(x, y) = 0\}$).

Regroupons dans le prochain énoncé les principales propriétés de l'orthogonalité.

6.30 Proposition. *Soient E et F des espaces vectoriels en dualité.*

a) Pour toute partie $A \subset E$ (resp. $B \subset F$), l'ensemble $A^\perp$ (resp. B^o) est un sous-espace vectoriel de E (resp. de F). Si $A_1 \subset A_2$, on a $A_2^\perp \subset A_1^\perp$ (resp. si $B_1 \subset B_2$, on a $B_2^o \subset B_1^o$).

On suppose de plus que E et F sont de dimension finie, et que φ et ψ sont des isomorphismes.

b) Pour toute partie $A \subset E$ (resp. $B \subset F$) l'espace $(A^\perp)^o$ (resp. $(A^o)^\perp$) est le sous-espace de E (resp. F) engendré par A (resp. B).

c) L'application $E_1 \mapsto E_1^\perp$ est une bijection décroissante de l'ensemble des sous-espaces vectoriels de E sur l'ensemble des sous-espaces vectoriels de F ; la bijection réciproque est $F_1 \mapsto F_1^o$.

d) Pour tout sous-espace vectoriel E_1 de E (resp. F_1 de F), on a $\dim E_1^\perp = \dim E - \dim E_1$ *(resp.* $\dim F_1^o = \dim F - \dim F_1$*).*

e) Soient E_1, E_2 (resp. F_1, F_2) des sous-espaces vectoriels de E (resp. F). On a $(E_1+E_2)^\perp = E_1^\perp \cap E_2^\perp$ et $(E_1 \cap E_2)^\perp = E_1^\perp + E_2^\perp$ (resp. $(F_1 + F_2)^o = F_1^o \cap F_2^o$ et $(F_1 \cap F_2)^o = F_1^o + F_2^o$).

Notons que les assertions « *resp.* » se déduisent des autres en échangeant les rôles de E et F et en remplaçant b par l'application $b' : (y, x) \mapsto b(x, y)$ de $F \times E$ dans K.

6.4 Exercices

6.1 Exercice. Soit A une matrice décomposée par blocs $A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$. On suppose que A_1 est une matrice carrée d'ordre r inversible. Démontrer que $\mathrm{rg}A = r \iff A_4 = A_3 A_1^{-1} A_2$.

6.2 Exercice. Soit E un espace vectoriel de dimension finie B, B' deux bases de E. Notons P la matrice de passage de B à B'. Quelle est la matrice de passage de la base duale B^* de B à la base duale $(B')^*$ de B'.

6.3 Exercice. Soit E un K espace vectoriel.

1. Démontrer que deux formes linéaires sur E dont les noyaux sont égaux sont proportionnelles.
2. Soient $f_1, \dots, f_k$ des formes linéaires sur E et $f \in E^*$. Démontrer que $f \in \mathrm{Vect}\{f_1, \dots, f_k\}$ si et seulement si $\bigcap_{j=1}^{k} \ker f_j \subset \ker f$.

6.4 Exercice. Soit E un espace vectoriel de dimension finie. Soit $(f_1, \dots, f_n)$ une famille d'éléments de E^*. Notons $\varphi : E \to K^n$ l'application $x \mapsto (f_1(x), \dots, f_n(x))$.

1. On suppose que la famille $(f_1, \dots, f_n)$ est une base de E^*.
   a) Démontrer que φ est injective. En déduire qu'elle est bijective.
   b) Démontrer qu'il existe une base B de E telle que $\varphi(B)$ soit la base canonique de K^n.
2. En déduire que toute base de E^* est duale d'une base de E.
3. Démontrer que l'on a les équivalences suivantes :
   φ est injective si et seulement si la famille $(f_1, \dots, f_n)$ est génératrice ;
   φ est surjective si et seulement si la famille $(f_1, \dots, f_n)$ est libre.

6.5 Exercice. Soient E et F des espaces vectoriels de dimension finie et f une application linéaire de E dans F.

1. Démontrer que ${}^t f$ est injective si et seulement si f est surjective et ${}^t f$ est surjective si et seulement si f est injective.
2. Démontrer que $\ker {}^t f = (\mathrm{im}\, f)^\perp$ et $\mathrm{im}\, {}^t f = (\ker f)^\perp$.

6.6 Exercice. Soient E et F deux espaces vectoriels de dimension finie en dualité. Démontrer que $\ker \varphi = F^o$ et $\ker \psi = E^\perp$.

Notons $b : \mathcal{M}_n(K) \times \mathcal{M}_n(K) \to K$ l'application $(A, B) \mapsto \mathrm{Tr}(AB)$.

1. Démontrer que b est une forme bilinéaire symétrique non dégénérée (ces termes sont définis page 81).
2. On suppose que $n \geqslant 2$. Démontrer que tout hyperplan de $\mathcal{M}_n(K)$ contient une matrice inversible.
3. On suppose que $K = \mathbb{R}$. Quelle est la signature de b ?

6.7 Exercice. Soient a et b deux points distincts de K. Sur le K espace vectoriel E des polynômes de degré $\leqslant 3$, on considère les formes linéaires $f_1 : P \mapsto P(a)$, $f_2 : P \mapsto P'(a)$, $f_3 : P \mapsto P(b)$, $f_4 : P \mapsto P'(b)$.

1. Calculer $\{f_1, f_2, f_3, f_4\}^o$.
2. Démontrer que (f_1, f_2, f_3, f_4) est une base de E^*.
3. Quelle est la base de E dont (f_1, f_2, f_3, f_4) est la base duale ?

6.8 Exercice. On se propose de donner deux démonstration du
Lemme de Schur. *Un endomorphisme u d'un espace vectoriel E de dimension finie qui laisse stable tout hyperplan est une homothétie.*

1. Rappel : Démontrer qu'un endomorphisme qui laisse invariante toute droite vectorielle est une homothétie.
2. *Première méthode.*
   a) Démontrer que la transposée de u laisse fixe toute droite - donc c'est est une homothétie.
   b) En déduire que u est une homothétie.
3. *Deuxième méthode.* Démontrer que u laisse stable toute droite - donc c'est une homothétie.

6.9 Exercice. [Dual d'un espace vectoriel complexe] Remarquons que tout espace vectoriel complexe est naturellement un espace vectoriel réel. Soit E un espace vectoriel complexe. Notons $E^*_{\mathbb{C}}$ son dual et $E^*_{\mathbb{R}}$ le dual de E considéré comme espace vectoriel réel. Pour $\ell \in E^*_{\mathbb{C}}$, notons $\mathrm{Re}(\ell)$ l'application $x \mapsto \mathrm{Re}(\ell(x))$.

1. Démontrer que $\ell \mapsto \mathrm{Re}(\ell)$ est une bijection de $E^*_{\mathbb{C}}$ sur $E^*_{\mathbb{R}}$.
2. En particulier, $E^*_{\mathbb{R}}$ s'identifie à l'espace vectoriel complexe $E^*_{\mathbb{C}}$. Décrire directement la structure d'espace vectoriel complexe sur $E^*_{\mathbb{R}}$, *i.e.* la multiplication d'un élément de $E_{\mathbb{R}}$ par un nombre complexe.

6.10 Exercice. Soient E un espace vectoriel de dimension finie sur un corps K et f un endomorphisme de E.

1. Démontrer qu'un sous-espace F de E est stable par f si et seulement son orthogonal $F^\perp$ est stable par ${}^t f$.
2. Démontrer que f possède une valeur propre (dans K) si et seulement s'il existe un hyperplan de E stable par f.

On en déduit par récurrence sur $\dim E$ que si le polynôme caractéristique de f est scindé, alors f est trigonalisable - *cf.* fin de la démonstration du théorème 8.7.

6.11 Exercice. Soient L un corps commutatif, $K \subset L$ in sous-corps de L.

1. Démontrer que toute matrice $A \in M_{m,n}(K)$ a même rang considérée comme matrice à coefficients dans K ou dans L. dans K et dans L.
2. En déduire qu'un système de vecteurs dans K^n libre sur K implique est libre sur L.
3. Soit $M \in \mathcal{M}_n(K)$. Démontrer que le polynôme minimal de M est le même sur K et sur L

6.12 Exercice. 1. Soit $A \in M_k(\mathbb{Q})$. Pour $K = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, notons $f_K : K^k \to K^k$ l'application linéaire de matrice A. Démontrer que $\ker f_{\mathbb{R}} = \overline{\ker f_{\mathbb{Q}}}$ et $\ker f_{\mathbb{C}} = \{x+iy;\ x, y \in \ker f_{\mathbb{R}}\}$. Démontrer que $\mathrm{im}\, f_{\mathbb{R}} = \overline{\mathrm{im}\, f_{\mathbb{Q}}}$ et $\mathrm{im}\, f_{\mathbb{C}} = \{x + iy;\ x, y \in \mathrm{im}\, f_{\mathbb{R}}\}$.

2. Soient $A, B \in M_n(\mathbb{Q})$. Posons $E_{\mathbb{Q}} = \{M \in M_n(\mathbb{Q});\ AM = MB\}$, $E_{\mathbb{R}} = \{M \in M_n(\mathbb{R});\ AM = MB\}$ et $E_{\mathbb{C}} = \{M \in M_n(\mathbb{C});\ AM = MB\}$.
   a) Démonter que $E_{\mathbb{Q}}$ est dense dans $E_{\mathbb{R}}$ et que $E_{\mathbb{C}} = \{M + iN;\ M, N \in E_{\mathbb{R}}\}$.
   b) En déduire que A et B sont semblables sur $\mathbb{Q}$ si et seulement si elles le sont sur $\mathbb{C}$.

7 Systèmes d'équations linéaires, déterminants

7.1 Systèmes d'équations linéaires

Dans un sens, l'algèbre linéaire consiste à expliquer la structure des systèmes linéaires. Inversement, les questions d'algèbre linéaire se résolvent à l'aide de systèmes.

Un système linéaire de m équations aux inconnues $(x_1, \dots, x_n)$ est de la forme

$$\begin{cases} a_{1,1}x_1 & + & a_{1,2}x_2 & + & \dots & + & a_{1,n}x_n & = & b_1 \\ a_{2,1}x_1 & + & a_{2,2}x_2 & + & \dots & + & a_{2,n}x_n & = & b_2 \\ \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ a_{m,1}x_1 & + & a_{m,2}x_2 & + & \dots & + & a_{m,n}x_n & = & b_m \end{cases}$$

On dit qu'on a résolu ce système si on a décrit l'ensemble des n-uplets $(x_1, \dots, x_n)$ qui satisfont les m égalités ci-dessus.

Ce système est équivalent à l'équation matricielle $AX = B$ où A est la matrice $A = (a_{i,j}) \in \mathcal{M}_{m,n}(K)$, X est la matrice colonne inconnue $(x_j) \in K^n$ et B est la matrice colonne $(b_i) \in K^m$. Le rang de la matrice A s'appelle aussi le *rang du système.*

7.1 Définition. Un système d'équations linéaires est dit *de Cramer* s'il s'écrit de façon matricielle $AX = B$ où A est une matrice inversible. Un système de Cramer a une et une seule solution : $X = A^{-1}B$.

Nous verrons plus loin (au paragraphe 7.3) comment résoudre *en pratique* un système linéaire.

Résolution théorique. Notons r le rang de A. Par la proposition 6.14, on peut choisir $I \subset \{1, \dots, m\}$ et $J \subset \{1, \dots, n\}$ tels que la matrice extraite $(a_{i,j})_{(i,j)\in I\times J}$ soit carrée d'ordre r et inversible. Les x_j pour $j \in J$ s'appellent alors les *inconnues principales*, et les équations d'indice $i \in I$ s'appellent les *équations principales.*

Quitte à échanger l'ordre des équations et des inconnues, nous allons supposer que $I = J = \{1, \dots, r\}$. Décomposons A par blocs $A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$ (où A_1 est inversible d'ordre r).

7.2 Proposition. *Soit A une matrice d'ordre (m, n) de rang r ; supposons qu'elle admette une décomposition par blocs $A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$ où A_1 est inversible d'ordre r. Soit $B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$. L'équation $AX = B$ en les inconnues $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ admet des solutions si et seulement si $\begin{pmatrix} b_{r+1} \\ \vdots \\ b_m \end{pmatrix} = A_3A_1^{-1} \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}$; dans ce cas l'ensemble des solutions est $\{X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} ; \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix} = A_1^{-1} \left(\begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix} - A_2 \begin{pmatrix} x_{r+1} \\ \vdots \\ x_n \end{pmatrix} \right) ; x_{r+1}, \dots, x_n \in K\}$.*

La matrice carrée $U = \begin{pmatrix} A_1 & 0 \\ A_3 & I_{m-r} \end{pmatrix}$ d'ordre m est inversible d'inverse $U^{-1} = \begin{pmatrix} A_1^{-1} & 0 \\ -A_3A_1^{-1} & I_{m-r} \end{pmatrix}$. Le système est donc équivalent à $U^{-1}AX = U^{-1}B$. Or $U^{-1}A$ est de la forme $\begin{pmatrix} I_r & A_1^{-1}A_2 \\ 0 & C_4 \end{pmatrix}$, et puisque $\mathrm{rg}U^{-1}A = \mathrm{rg}A = r$, il vient $C_4 = 0$. Le système devient $\begin{pmatrix} I_r & A_1^{-1}A_2 \\ 0 & 0 \end{pmatrix} X = U^{-1}B$, soit

$$0 = \begin{pmatrix} -A_3A_1^{-1} & I_{m-r} \end{pmatrix} B \quad \text{et} \quad \begin{pmatrix} I_r & A_1^{-1}A_2 \end{pmatrix} X = \begin{pmatrix} A_1^{-1} & 0 \end{pmatrix} B.$$

Écrivons enfin $X = \begin{pmatrix} X_1 \\ X_2 \end{pmatrix}$ et $B = \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$ où B_1 et X_1 sont des matrices-colonne à r lignes. Le système devient :

$$B_2 = A_3 A_1^{-1} B_1 \quad \text{et} \quad X_1 + A_1^{-1} A_2 X_2 = A_1^{-1} B_1.$$

Quelques applications

1. Soient E, F des espaces vectoriels de dimension finie, f une application linéaire et A sa matrice dans des bases données. La résolution du système $AX = B$ donne :
   - Des équations de l'image, *i.e.* l'ensemble des B pour lesquels ce système admet des solutions (on dit qu'il est *compatible*) : pour $i > r$, (ou plus généralement pour $i \in \{1, \dots, n\} \setminus I$ où I est l'ensemble des équations principales) on obtient une équation du type $b_i = \sum \alpha_{i,k} b_k$ la somme étant prise de 1 à r (sur J dans le cas général). Les $\alpha_{i,k}$ sont les coefficients de la matrice $A_3 A_1^{-1}$.
   - Une base de l'image : les vecteurs-colonne d'indice $j \in \{1, \dots, r\}$ ($j \in J$ dans le cas général).
   - Pour chaque élément b de l'image, une paramétrisation (par x_j, $j > r$ - ou $j \notin J$ dans le cas général) de l'ensemble des $x \in E$ tels que $f(x) = b$.
   - En particulier, on obtient une base du noyau indexée par $j \in \{r+1, \dots, n\}$ (en considérant le système $AX = 0$, *i.e.* en prenant les b_i tous nuls) : elle est formée par les vecteurs-colonne de la matrice $\begin{pmatrix} -A_1^{-1} A_2 \\ I_{n-r} \end{pmatrix}$.
2. ***Applications « géométriques »***
   Soient E un espace vectoriel de dimension finie et F un sous-espace vectoriel (*resp.* affine) de E. Une *représentation paramétrique* de F est donnée par une application linéaire (*resp.* affine) f de $\mathbb{R}^k$ dans E d'image F. Une telle représentation paramétrique sera minimale si f est injective.

   Un *système d'équations cartésiennes* (ou *représentation cartésienne*) de F est donné par une application linéaire $g : E \to \mathbb{R}^\ell$ telle que $F = \ker g$ (*resp.* $F = g^{-1}(B)$ où B est un point de $\mathbb{R}^\ell$). Une telle représentation cartésienne sera minimale si g est surjective.

   La proposition 7.2 nous permet de passer d'une représentation à l'autre : elle donne une représentation paramétrique minimale de l'ensemble des solutions de l'équation $g(X) = B$; elle donne un système minimal d'équations cartésiennes de l'ensemble des X tels que le système $f(Y) = X$ admet des solutions.

   En particulier, si F et G sont des sous-espaces vectoriels de E donnés par des représentations cartésiennes, on a immédiatement un système d'équations cartésiennes de $F \cap G$; on peut de même facilement donner une représentation paramétrique de $F + G$ si F et G sont donnés par une représentation paramétrique. La résolution de systèmes nous permet donc de donner des équations cartésiennes et paramétriques d'une intersection et d'une somme de sous-espaces.

7.2 Déterminants

7.2.1 Formes multilinéaires alternées ; déterminant relatif à une base

7.3 Définition. Soient E, F des K-espaces vectoriels et $n \in \mathbb{N}$. Une application $D : E^n \to F$ est appelée *multilinéaire* ou *n-linéaire* si elle est linéaire par rapport à chacune des variables. Une application multilinéaire $D : E^n \to F$ est dite *alternée* si $D(x_1, \dots, x_n) = 0$ dès que deux x_i sont égaux, *i.e.* dès qu'il existe $i, j \in \{1, \dots, n\}$ avec $i \neq j$ et $x_i = x_j$. Lorsque $F = K$ on parle de *forme multilinéaire* et de *forme multilinéaire alternée.*

L'ensemble des formes n-linéaires alternées est naturellement muni d'une structure d'espace vectoriel (sous-espace vectoriel de l'espace vectoriel F^{E^n} de toutes les applications de E^n dans F).

Soit D une application n-linéaire alternée. Soient $x_1, \dots, x_n \in E$. On a

$$0 = D(x_1 + x_2, x_1 + x_2, x_3, \dots, x_n) = D(x_1, x_2, x_3, \dots, x_n) + D(x_2, x_1, x_3, \dots, x_n),$$

donc $D(x_2, x_1, x_3, \dots, x_n) = -D(x_1, x_2, x_3, \dots, x_n)$. Plus généralement, si i, j sont deux éléments distincts de $\{1, \dots, n\}$, on a $D(\dots, x_i, \dots, x_j, \dots) = -D(\dots, x_j, \dots, x_i, \dots)$.

Puisque $\mathfrak{S}_n$ est engendré par les transpositions, on en déduit que pour toute permutation $\sigma \in \mathfrak{S}_n$ on a $D(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = \varepsilon(\sigma) D(x_1, x_2, \dots, x_n)$ où ε est la signature.

7.4 Théorème. *Soient E un K-espace vectoriel de dimension n et $B = (e_1, \dots, e_n)$ une base de E. Il existe une unique forme n-linéaire alternée $\det_B : E^n \to K$ telle que $\det_B(e_1, \dots, e_n) = 1$.*

Notons $(e_1^*, \dots, e_n^*)$ la base duale de $(e_1, \dots, e_n)$.

Existence. Démontrons que l'application D définie par $D(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{j=1}^{n} e_{\sigma(j)}^*(x_j)$ convient.

- Pour chaque $\sigma \in \mathfrak{S}_n$ posons $L_\sigma : (x_1, \dots, x_n) \mapsto \prod_{j=1}^{n} e_{\sigma(j)}^*(x_j) = \prod_{i=1}^{n} e_i^*(x_{\sigma^{-1}(i)})$. Pour tout $\sigma \in \mathfrak{S}$, tout $(x_1, \dots, x_n) \in E^n$ et tout $i \in \{1, \dots, n\}$ l'application $\Big(\prod_{j \neq i} e_{\sigma(j)}^*(x_j)\Big) e_{\sigma(i)}^*$ est une forme linéaire, donc l'application L_σ est multilinéaire. On en déduit que $D = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) L_\sigma$ est *multilinéaire.*
- Démontrons qu'elle est *alternée.* Soient $i, j \in \{1, \dots, n\}$ et $(x_1, \dots, x_n) \in E^n$ tels que $i \neq j$ et $x_i = x_j$. Notons τ la transposition (i, j) et remarquons que $L_{\tau \circ \sigma}(x_1, \dots, x_n) = L_\sigma(x_1, \dots, x_n)$. L'application $\sigma \mapsto \tau \circ \sigma$ est une bijection du groupe alterné $\mathfrak{A}_n$ sur son complémentaire $\mathfrak{S}_n \setminus \mathfrak{A}_n$, de sorte que

$$\sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) L_\sigma(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{A}_n} \Big(L_\sigma(x_1, \dots, x_n) - L_{\tau \circ \sigma}(x_1, \dots, x_n) \Big) = 0.$$

- Enfin, on a $L_{\mathrm{id}}(B) = 1$ et, pour $\sigma \in \mathfrak{S} \setminus \{\mathrm{id}\}$, on a $L_\sigma(B) = 0$; donc $D(B) = 1$.

Unicité. Par multilinéarité, pour connaître une forme n-linéaire $D : E^n \to K$, il suffit de la connaître sur les vecteurs de la base, *i.e.* de connaître les nombres $D(e_{s(1)}, \dots, e_{s(n)})$ pour toute application $s : \{1, \dots, n\} \to \{1, \dots, n\}$. On aura $D(x_1, \dots, x_n) = \sum_s D(e_{s(1)}, \dots, e_{s(n)}) \prod_{j=1}^{n} e_{s(j)}^*(x_j)$ où la somme est prise sur l'ensemble de toutes les applications $s : \{1, \dots, n\} \to \{1, \dots, n\}$, puisqu'on a $x_j = \sum_{i=1}^{n} e_i^*(x_j) e_i$.

Si D est alternée, alors $D(e_{s(1)}, \dots, e_{s(n)}) = 0$ si s n'est pas injective. De plus, pour tout $\sigma \in \mathfrak{S}_n$, on a $D(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = \varepsilon(\sigma) D(e_1, \dots, e_n)$. En d'autres termes, l'application $D \mapsto D(e_1, \dots, e_n)$ est injective.

L'application $\det_B$ s'appelle le *déterminant associé à la base B.*

7.5 Proposition. *Soient B, B' deux bases d'un espace vectoriel E de dimension finie. Posons $n = \dim E$. Pour tout $(x_1, \dots, x_n) \in E^n$, on a $\det_B(x_1, \dots, x_n) = \det_B(B') \det_{B'}(x_1, \dots, x_n)$.*

En effet, il résulte (de la démonstration) du théorème 7.4 que l'application $D \mapsto D(B')$ est une bijection de l'espace vectoriel des applications n-linéaires alternées sur K. Les applications n-linéaires alternées $\det_B$ et $\det_B(B') \det_{B'}$ qui coïncident en B' sont égales.

7.6 Proposition. *Soit B une base d'un espace vectoriel E de dimension finie. Posons $n = \dim E$. Pour tout $(x_1, \ldots, x_n) \in E^n$, on a $\det_B(x_1, \ldots, x_n) \neq 0$ si et seulement si $(x_1, \ldots, x_n)$ est une base de E.*

Posons $B' = (x_1, \ldots, x_n)$. Si B' est une base de E, on a $1 = \det_B(B) = \det_B(B')\det_{B'}(B)$ d'après la prop. 7.5, donc $\det_B(B') \neq 0$.

Puisque $\det_B$ est n-linéaire et alternée, le nombre $\det_B(x_1, \ldots, x_n)$ ne change pas lorsque on ajoute à un x_k une combinaison linéaire des autres - sans changer les autres x_j. Si la famille $(x_1, \ldots, x_n)$ n'est pas libre, par une telle opération, on peut changer un x_k en 0, donc $\det_B(x_1, \ldots, x_n) = 0$.

7.7 Formules de Cramer. Soit $B = (e_1, \ldots, e_n)$ une base de E. Soit $v \in E$. Écrivons $v = \sum_{k=1}^{n} \lambda_k e_k$.

On a $\det_B(e_1, \ldots, e_{k-1}, v, e_{k+1}, \ldots, e_n) = \lambda_k$.

Soit maintenant $(u_1, \ldots, u_n) = B'$ une autre base de E. L'équation $x_1u_1 + \ldots + x_nu_n = v$ en les inconnues $x_1, \ldots, x_n \in K$ admet une et une seule solution donnée par

$$x_k = \det_{B'}(u_1, \ldots, u_{k-1}, v, u_{k+1}, \ldots, u_n) = \frac{\det_B(u_1, \ldots, u_{k-1}, v, u_{k+1}, \ldots, u_n)}{\det_B(u_1, \ldots, u_n)}.$$

7.2.2 Déterminant d'un endomorphisme

7.8 Proposition. *Soient E un espace vectoriel de dimension finie et soit $f \in L(E)$ un endomorphisme de E. Il existe un unique élément de K appelé* déterminant de l'endomorphisme f *et noté* $\det f$ *tel que pour toute forme n-linéaire alternée D sur E et tout $(x_1, \ldots, x_n) \in E$ on ait $D(f(x_1), \ldots, f(x_n)) = (\det f)\, D(x_1, \ldots, x_n)$.*

Soit $B = (e_1, \ldots, e_n)$ une base de E. L'application $D_0 : (x_1, \ldots, x_n) \mapsto \det_B(f(x_1), \ldots, f(x_n))$ est une forme n-linéaire alternée sur E. On a donc $D_0 = D_0(B)\det_B$. Soit D une forme n-linéaire alternée sur E ; il existe $\lambda \in K$ tel que $D = \lambda\det_B$; notons D_f l'application $D_f : (x_1, \ldots, x_n) \mapsto D(f(x_1), \ldots, f(x_n)) = \lambda\det_B(f(x_1), \ldots, f(x_n))$. Il vient $D_f = \lambda D_0 = \lambda D_0(B)\det_B = D_0(B)D$.
Il suffit donc de poser $\det f = D_0(B)$.

Si $B = (e_1, \ldots, e_n)$ est une base de E, on a $\det f = \det_B(f(e_1), \ldots, f(e_n))$.

Donnons les principales propriétés du déterminant des endomorphismes.

7.9 Théorème. *Soient E un espace vectoriel de dimension finie et $f, g \in L(E)$.*

a) On a $\det f \neq 0$ si et seulement si f est inversible.

b) On a $\det(g \circ f) = \det f \det g$.

a) Soit $B = (e_1, \ldots, e_n)$ une base de E. On a $\det f = \det_B(f(e_1), \ldots, f(e_n))$; donc $\det f \neq 0$ si et seulement si $(f(e_1), \ldots, f(e_n))$ est une base de E, *i.e.* si et seulement si f est inversible.

b) Si D est une forme n-linéaire alternée sur E et $h \in L(E)$, notons D_h la forme n-linéaire alternée $D_h : (x_1, \ldots, x_n) \mapsto D(h(x_1), \ldots, h(x_n))$. Par la proposition ci-dessus, on a $D_h = (\det h)D$. On trouve $\det(g \circ f)\, D = D_{g\circ f} = (D_g)_f = (\det f)\, D_g = (\det f)(\det g)\, D$. Il suffit de choisir D non nulle pour conclure.

Il résulte de ce théorème que $f \mapsto \det f$ est un homomorphisme de groupes de $GL(E)$ dans K^*. Son noyau $\{f \in L(E);\ \det f = 1\}$ s'appelle le *groupe spécial linéaire* de E et se note $SL(E)$.

7.2.3 Déterminant d'une matrice carrée

Soit $n \in \mathbb{N}$. L'espace vectoriel des vecteurs-colonnes $\mathcal{M}_{n,1}(K)$ est naturellement muni d'une base B dite « canonique » formée des vecteurs-colonnes e_j ayant un 1 dans la $j^{\text{ème}}$ ligne et toutes les autres lignes nulles.

7.10 Définition. Le *déterminant d'une matrice* carrée $A \in \mathcal{M}_n(K)$ est le déterminant de ses vecteurs-colonnes relativement à la base canonique. C'est le déterminant de l'endomorphisme $X \mapsto AX$ de $\mathcal{M}_{n,1}(K)$ défini par A.

De la formule donnée dans le théorème 7.4, il résulte que si $A = (a_{i,j})$, on a $\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{j=1}^{n} a_{\sigma(j),j}$.

7.11 Remarque. Si K est juste un anneau *commutatif*, cette formule garde un sens et permet de définir le déterminant d'une matrice à coefficients dans K.

Si $\varphi : K_1 \to K_2$ est un homomorphisme d'anneaux et $A = (a_{i,j}) \in \mathcal{M}_n(K_1)$ est une matrice à coefficients dans K_1, notons $\varphi(A) \in \mathcal{M}_n(K_2)$ la matrice $(\varphi(a_{i,j}))$. On a $\det(\varphi(A)) = \varphi(\det(A))$.

Si P est la matrice de passage d'une base B à une base B', on a $\det(P) = \det_B(B')$.

Donnons les principales propriétés du déterminant des matrices carrées.

7.12 Théorème. *Soient $P, Q \in \mathcal{M}_n(K)$.*

a) On a $\det(P) \neq 0$ si et seulement si P est inversible.

b) On a $\det(PQ) = \det P \det Q$.

c) On a $\det({}^tP) = \det(P)$.

a) et b) résultent du théorème 7.9.

Ecrivons $P = (a_{i,j})$. On a $\det({}^tP) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{j=1}^{n} a_{j,\sigma(j)}$.

Puisque le produit dans K est associatif et commutatif, pour $\sigma \in \mathfrak{S}_n$ et $(\lambda_1, \ldots, \lambda_n) \in K^n$, on a $\prod_{j=1}^{n} \lambda_{\sigma(j)} = \prod_{j=1}^{n} \lambda_j$. En particulier, posant $\lambda_j = a_{j,\sigma^{-1}(j)}$, on trouve $\prod_{j=1}^{n} a_{j,\sigma^{-1}(j)} = \prod_{j=1}^{n} a_{\sigma(j),j}$. Donc $\det(P) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{j=1}^{n} a_{j,\sigma^{-1}(j)}$. Notons que $\sigma \mapsto \sigma^{-1}$ est une bijection de $\mathfrak{S}_n$ dans lui-même. Il vient $\det(P) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma^{-1}) \prod_{j=1}^{n} a_{j,\sigma(j)} = \det({}^tP)$, puisque $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$.

Il résulte de ce théorème que $P \mapsto \det(P)$ est un homomorphisme de groupes de $GL_n(K)$ dans K^*. Son noyau $\{P \in \mathcal{M}_n(K);\ \det P = 1\}$ s'appelle le *groupe spécial linéaire* et se note $SL_n(K)$.

7.13 Formules de Cramer. Soient $A \in \mathcal{M}_n(K)$ une matrice inversible et $B \in \mathcal{M}_{n,1}(K)$ une matrice-colonne. Écrivons $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. D'après 7.7, la solution du système $AX = B$ est donnée par $x_j = \dfrac{\Delta_j}{\Delta}$ où $\Delta = \det(A)$ et Δ_j est le déterminant de la matrice obtenue en remplaçant la $j^{\text{ème}}$ colonne de A par la colonne B.

Mineurs. Soit $A \in \mathcal{M}_{m,n}(K)$. On appelle *mineurs* de A les déterminants des matrices carrées extraites de A.

La proposition 6.14 s'énonce :

7.14 Proposition. *Le rang d'une matrice est l'ordre de son plus grand mineur non nul.*

Coffacteurs. Soient $A \in \mathcal{M}_n(K)$ une matrice carrée et $i, j \in \{1, \dots, n\}$. On note $A_{i,j} \in \mathcal{M}_{n-1}(K)$ la matrice obtenue en enlevant de A sa $i^{\text{ème}}$ ligne et sa $j^{\text{ème}}$ colonne.

7.15 Lemme. *Soient $A = (a_{k,\ell}) \in \mathcal{M}_n(K)$ une matrice carrée et $i, j \in \{1, \dots, n\}$. On suppose que $a_{i,j} = 1$ et que pour $k \neq i$, on a $a_{k,j} = 0$. Alors* $\det A = (-1)^{i+j} \det A_{i,j}$.

Supposons d'abord que $i = j = n$. Dans la somme $\det A = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{k=1}^{n} a_{\sigma(k),k}$ les seuls termes non nuls sont obtenus par les $\sigma \in \mathfrak{S}_n$ tels que $\sigma(n) = n$. Identifions avec $\mathfrak{S}_{n-1}$ l'ensemble de ces permutations. On a $\det A = \sum_{\sigma \in \mathfrak{S}_{n-1}} \varepsilon(\sigma) a_{n,n} \prod_{k=1}^{n-1} a_{\sigma(k),k} = \det(A_{n,n})$.

Pour le cas général, considérons les permutations $c_i = (i, i+1, \dots, n)$ et $c_j = (j, j+1, \dots, n)$ et P_{c_i} les matrices de permutation associées. La matrice $B = P_{c_i}^{-1} A P_{c_j}$ s'écrit par blocs $B = \begin{pmatrix} A_{i,j} & 0 \\ * & 1 \end{pmatrix}$, donc par le cas $i = j = n$, on a $\det B = \det A_{i,j}$. Or c_i étant un cycle de longueur $n - i + 1$, on a $\det(P_{c_i}) = \varepsilon(c_i) = (-1)^{n-i}$ et $\det(P_{c_j}) = (-1)^{n-j}$, d'où le résultat.

7.16 Proposition: développement relativement à une colonne ou une ligne.
Soit $A = (a_{i,j}) \in \mathcal{M}_n(K)$ une matrice carrée.

a) Pour tout $j \in \{1, \dots, n\}$, on a $\det A = \sum_{i=1}^{n} (-1)^{i+j} a_{i,j} \det A_{i,j}$.

b) Pour tout $i \in \{1, \dots, n\}$, on a $\det A = \sum_{j=1}^{n} (-1)^{i+j} a_{i,j} \det A_{i,j}$.

Pour $i, j \in \{1, \dots, n\}$, notons $B_{i,j} \in \mathcal{M}_n(K)$ la matrice qui a les mêmes colonnes que A sauf la $j^{\text{ème}}$ qui est égale à e_i. Par linéarité en la $j^{\text{ème}}$ colonne, on a $\det A = \sum_{i=1}^{n} a_{i,j} \det B_{i,j}$. L'assertion (a) résulte donc du lemme 7.15. En remplaçant A par sa matrice transposée, on en déduit (b).

Comatrice

7.17 Définition. Soit $A = (a_{i,j}) \in \mathcal{M}_n(K)$ une matrice carrée. On appelle *coffacteur* associé à (i, j) pour $i, j \in \{1, \dots, n\}$ le terme $(-1)^{i+j} \det A_{i,j}$. On appelle *comatrice* de A la matrice $\mathrm{com}(A)$ de terme général $(-1)^{i+j} \det A_{i,j}$.

7.18 Proposition. *Soit $A \in \mathcal{M}_n(K)$ une matrice carrée. On a $A\,{}^t\mathrm{com}(A) = {}^t\mathrm{com}(A) A = \det(A) I_n$. En particulier, si A est inversible, on a $A^{-1} = (\det A)^{-1}\,{}^t\mathrm{com}(A)$.*

Remarquons que cette formule pour l'inverse de A est très peu praticable - sauf en dimension 2... Si $ad - bc \neq 0$, l'inverse de $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est $\frac{1}{ad-bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

7.2.4 Interprétation du déterminant lorsque le corps de base est $\mathbb{R}$

Supposons que le corps de base soit $\mathbb{R}$.

Signe du déterminant et *orientation.* On dit que deux bases B et B' ont *même orientation* si $\det_B(B') \in \mathbb{R}_+^*$; on dit sinon qu'elles ont une *orientation opposée*. La relation « avoir même orientation » est une relation d'équivalence. Ainsi, les bases de E se séparent en deux classes d'équivalence. Choisir une orientation de l'espace c'est choisir une de ces deux classes.

Valeur absolue du déterminant et *volume.* Pour fixer une mesure des volumes sur E - c'est à dire une mesure de Lebesgue sur E, choisissons une base $B = (e_1, \dots, e_n)$ et normalisons le volume en décidant que le volume du « cube » $\{\sum_{i=1}^{n} t_i e_i;\ (t_1, \dots, t_n) \in [0,1]^n\}$ est 1. Si $(x_1, \dots, x_n)$ est une famille de vecteurs, le volume du parallélépipède $\{\sum_{i=1}^{n} t_i x_i;\ (t_1, \dots, t_n) \in [0,1]^n\}$ est $|\det_B(x_1, \dots, x_n)|$.

Un endomorphisme f de E multiplie le volume par $|\det f|$: si $A \subset E$ est une partie « mesurable » on a $vol(f(A)) = |\det f|\, vol(A)$.

Plus généralement, la formule de changement de variable d'une intégrale multiple pour un difféomorphisme fait aussi intervenir la valeur absolue d'un déterminant : si U et V sont des ouverts de $\mathbb{R}^n$ et $f : U \to V$ est un difféomorphisme de classe C^1, pour toute fonction intégrable $g : V \to \mathbb{R}$ on a

$$\int_V g(x_1, \dots, x_n)\, dx_1 \dots dx_n = \int_U g \circ f(x_1, \dots, x_n) \left|J_f(x_1, \dots, x_n)\right| dx_1 \dots dx_n$$

où J_f est le déterminant de la matrice jacobienne.

7.3 Opérations élémentaires sur les matrices

Nous expliquons à présent comment de façon algorithmique
- calculer le rang et le déterminant d'une matrice ;
- trouver l'inverse d'une matrice inversible ;
- résoudre un système d'équations linéaires...

7.3.1 Matrices élémentaires

On fixe un corps commutatif K et $n \in \mathbb{N}$ ($n \geqslant 2$). Pour $i, j \in \{1, \dots n\}$, notons $E_{i,j} \in \mathcal{M}_n(K)$ la matrice dont tous les coefficients sont nuls sauf celui d'indice (i, j) (i-ième ligne, j-ième colonne) qui vaut 1. Les $E_{i,j}$ forment une base de $\mathcal{M}_n(K)$.

On appelle matrices élémentaires trois types de matrices carrées :

Transvections. Soient $i, j \in \{1, \dots, n\}$ avec $i \neq j$ et soit $\lambda \in K^*$. Posons $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$. Cette matrice a donc tous ses coefficients diagonaux égaux à 1, ses coefficients hors-diagonaux nuls sauf celui d'indice (i, j) qui vaut λ.

Les matrices $T_{i,j}(\lambda)$ s'appellent des *matrices de transvection.*

Dilatations. Soit $i \in \{1, \dots, n\}$ et soit $\lambda \in K^*$, $\lambda \neq 1$. Posons $D_i(\lambda) = I_n + (\lambda - 1)E_{i,i} \in \mathcal{M}_n(K)$. Cette matrice a donc tous ses coefficients hors-diagonaux nuls, ses coefficients diagonaux égaux à 1 sauf celui d'indice (i, i) qui vaut λ.

Les matrices $D_i(\lambda)$ s'appellent des *matrices de dilatation.*

Transpositions. Soient $i, j \in \{1, \ldots, n\}$ avec $i \neq j$. Posons $P_{i,j} = I_n - E_{i,i} - E_{j,j} + E_{i,j} + E_{j,i}$.

Cette matrice a donc tous ses coefficients diagonaux égaux à 1 sauf ceux d'indice (i,i) et (j,j) qui sont nuls, et ses coefficients hors-diagonaux nuls sauf ceux d'indice (i,j) et (j,i) qui valent 1.

Les matrices $P_{i,j}$ s'appellent des *matrices de transposition.*

Les matrices de transposition sont des cas particuliers des matrices de permutation : soit $\sigma \in \mathfrak{S}_n$ une permutation ; on appelle matrice de permutation associée la matrice $P_\sigma = (a_{k,\ell}) \in \mathcal{M}_n(K)$ telle que

- $a_{k,\ell} = 1$ si $k = \sigma(\ell)$;
- $a_{k,\ell} = 0$ si $k \neq \sigma(\ell)$.

Remarquons que $\sigma \mapsto P_\sigma$ est un homomorphisme de groupes de $\mathfrak{S}_n$ dans $GL_n(K)$.

Les matrices élémentaires sont inversibles : on a $T_{i,j}(\lambda)^{-1} = T_{i,j}(-\lambda)$, $D_i(\lambda)^{-1} = D_i(1/\lambda)$ et $P_{i,j}^{-1} = P_{i,j}$.

7.3.2 Opérations sur les lignes et les colonnes

Soit $A \in M_{m,n}(K)$ une matrice. On appelle *opération élémentaire sur les lignes* de A une opération d'un des trois types suivants :

(L1) Ajouter à une ligne un multiple d'une autre ligne.

(L2) Multiplier une ligne par un scalaire non nul.

(L3) Intervertir deux lignes.

Ces opérations reviennent à multiplier A à gauche par une matrice élémentaire. Ainsi

1. la matrice $T_{i,j}(\lambda)A$ s'obtient à partir de A en ajoutant à la $i^{\text{ème}}$ ligne λ fois la $j^{\text{ème}}$ ligne.
2. la matrice $D_i(\lambda)A$ s'obtient à partir de A en multipliant la $i^{\text{ème}}$ ligne par λ.
3. la matrice $P_{i,j}A$ s'obtient à partir de A en intervertissant la $i^{\text{ème}}$ et la $j^{\text{ème}}$ lignes.

De même, on appelle *opération élémentaire sur les colonnes* de A une opération d'un des trois types suivants :

(C1) Ajouter à une colonne un multiple d'une autre colonne.

(C2) Multiplier une colonne par un scalaire non nul.

(C3) Intervertir deux colonnes.

Ces opérations reviennent à multiplier A à droite par une matrice élémentaire.

7.3.3 Opérations sur les lignes : Algorithme de Gauss

Soit $A \in \mathcal{M}_{m,n}(K)$.

L'algorithme de Gauss consiste à effectuer des opérations élémentaires sur les lignes d'une matrice jusqu'à ce qu'elle obtienne une forme « simple ». Commençons par définir ces matrices simples. Notons $(E_1, \ldots E_m)$ la base canonique de l'espace vectoriel $\mathcal{M}_{m,1}(K)$ des matrices-colonnes à m lignes.

7.19 Définition. Convenons d'appeler *matrice échelonnée réduite* ou *matrice à pivots* une matrice $A \in M_{m,n}(K)$, telle qu'il existe $r \in \{0, \ldots m\}$ et une application strictement croissante $k \mapsto j(k)$ de $\{1, \ldots, r\}$ dans $\{1, \ldots, n\}$ satisfaisant :

- pour $k \in \{1, \ldots, r\}$, la colonne d'ordre $j(k)$ de A est égale à E_k ;
- pour $i \in \{1, \ldots, r\}$ et $j < j(i)$ on a $a_{i,j} = 0$;
- pour $i \in \{r+1, \ldots, m\}$ et tout $j \in \{1, \ldots n\}$ on a $a_{i,j} = 0$.

Au bout du k-ième pas de l'algorithme de Gauss on aura choisi $j(k)$ et les $j(k)$ premières colonnes de $A^{(k)}$ formeront une matrice échelonnée réduite (qui ne changera plus dans la suite).

L'algorithme de Gauss est le suivant :

- On pose $A^{(0)} = A$ et on construit successivement des matrices $A^{(k)} = (a_{i,j}^{(k)})$ pour $1 \leqslant k \leqslant m$.
- Soit $k \in \{1, \dots, m\}$ et supposons $A^{(k-1)}$ construit.
  Si les $m - k + 1$ dernières lignes sont nulles, la matrice $A^{(k-1)}$ est échelonnée réduite.
  S'il existe $i \geqslant k$ et j tels que $a_{i,j}^{(k-1)} \neq 0$, on note $j(k)$ le plus petit j tel qu'il existe $i \geqslant k$ avec $a_{i,j}^{(k-1)} \neq 0$ et on choisit $i(k) \geqslant k$ tel que $a_{i(k),j(k)}^{(k-1)} \neq 0$. Le couple $(i(k), j(k))$ ainsi choisi s'appelle un *pivot*.
  Maintenant on fait subir à $A^{(k-1)}$ successivement les opérations élémentaires suivantes :
  (E1) on divise la ligne d'ordre $i(k)$ par $a_{i(k),j(k)}^{(k-1)}$; (opération de type (L2))
  (E2) on intervertit la ligne d'ordre k et la ligne d'ordre $i(k)$; (opération de type (L3))
  (E3) maintenant $a_{k,j(k)} = 1$. On annule tous les autres termes de la colonne $j(k)$ ([2]) : pour $i \neq k$ on retranche $a_{i,j(k)}$ fois la ligne d'ordre k à la ligne d'ordre i. (opérations de type (L1))
- Lorsque $k = m$ ou lorsque toutes les lignes d'ordre $i \geqslant k + 1$ de $A^{(k)}$ sont nulles, on a obtenu une matrice échelonnée réduite : on arrête l'algorithme.

7.20 Remarque. Remarquons que dans la k-ième étape, lorsque $k < m$, on peut utiliser uniquement des opérations de type (L1). En effet,

a) si $a_{k,j(k)}^{(k-1)} = 1$ on effectue directement l'étape (E3) qui n'utilise que les opérations (L1) ;

b) si un coefficient $i > k$ est non nul, en ajoutant un multiple convenable de la i-ième ligne à la k-ième on arrive à $a_{k,j(k)} = 1$;

c) si $a_{k,j(k)} \neq 1$ et $a_{i,j(k)} = 0$ pour tout $i > k$, on commence par ajouter la k-ième ligne à la suivante (on peut puisque $k < m$), et on est ramené au cas (b).

7.3.4 Applications

Résolution pratique de systèmes linéaires

On veut résoudre un système d'équations $AX = B$, où $A \in \mathcal{M}_{m,n}(K)$. On crée une matrice $C = (A\ B)$ à m lignes et $n + 1$ colonnes. En lui appliquant l'algorithme de Gauss *sur les lignes*, on obtient une matrice échelonnée réduite $C' = (A'\ B')$ avec $A' = UA$ et $B' = UB$ où U est une matrice inversible, donc un système $A'X = B'$ équivalent à celui du départ.

Notons r le rang de C. Deux cas sont possibles :

a) On a $j(r) = n + 1$, c'est-à-dire $\operatorname{rg} A = r - 1 < r = \operatorname{rg}(A\ B)$ et l'équation d'ordre r du système $A'X = B'$ est $0 = 1$: il n'y a pas des solutions.

b) On a $j(r) \leqslant n$, *i.e.* $\operatorname{rg} A = \operatorname{rg} C$ et le système admet des solutions qui sont très facilement paramétrées par les x_j pour j qui n'est pas de la forme $j(k)$.

Inversion de matrices carrées

Soit A une matrice carrée d'ordre n inversible. Lorsqu'on fait subir à A l'algorithme de Gauss *sur les lignes*, on obtient nécessairement une échelonnée réduite inversible. La seule telle matrice est I_n.

2. Souvent, on ne fait pas complètement la dernière étape de cette transformation : on n'annule que les coefficients $a_{i,j(k)}$ pour $i > k$. On obtient ainsi une matrice échelonnée « non réduite ». On a toujours des « pivots » qui sont des 1 en position $(k, j(k))$, avec des 0 à gauche et en dessous, mais on n'impose pas qu'il ait aussi des 0 au dessus.

Inverser la matrice A, revient à résoudre un système $AX = B$ pour toute matrice B. Si on pose $B = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ et que l'on résout le système $AX = B$ *i.e.* on fait subir à $(A\ B)$ l'algorithme de Gauss, la solution sera donnée sous la forme $X = A^{-1}B$.

Une autre façon d'effectuer le même calcul est la suivante : il suffit d'opérer l'algorithme de Gauss aux ***lignes*** de la matrice $(A\, I_n)$ $(\in \mathcal{M}_{n,2n}(K))$. À la fin de l'algorithme on aura la matrice $(I_n\, A^{-1})$.

Génération de $GL(n, K)$ et $SL(n, K)$

Si $A \in GL(n, K)$, on a démontré que l'on peut la multiplier par des matrices élémentaires et obtenir I_n. En particulier, A^{-1} est produit de matrices élémentaires. On en déduit immédiatement :

7.21 Proposition. *$GL(n, K)$ est engendré par les matrices élémentaires.*

Grâce à la remarque 7.20, on peut faire mieux :

7.22 Théorème. *a) $SL(n, K)$ est engendré par les transvections.*
b) $GL(n, K)$ est engendré par les transvections et les dilatations.

Calculs de rang, de déterminants

Pour calculer le rang d'une matrice A, on peut simplement lui faire subir l'algorithme de Gauss. Par contre, comme on ne change pas le rang en multipliant à gauche ou à droite par une matrice inversible, on peut utiliser à loisir les opérations à la fois sur les lignes et sur les colonnes.

On peut calculer le déterminant d'une matrice carrée A en utilisant les opérations sur les lignes et les colonnes. La seule chose à retenir est :

- Lorsqu'on ajoute à une ligne (*resp.* colonne) un multiple d'une ligne (*resp.* colonne) on ne change pas le déterminant.
- Lorsqu'on multiplie une ligne (ou une colonne) par un scalaire on multiplie le déterminant par ce scalaire.
- Lorsqu'on intervertit deux lignes ou deux colonnes on multiplie le déterminant par -1.

7.23 Remarques. a) Lorsqu'on effectue des calculs de manière approchée, on ne pourra jamais démontrer que le rang est strictement inférieur à $\min(m, n)$. En effet, l'ensemble des matrices de rang $\min(m, n)$ est dense. Par contre, on arrivera à *minorer le rang* puisque les matrices de rang $\geqslant k$ forment un ouvert, par exemple, si on arrive à démontrer qu'un déterminant extrait d'ordre k est égal à D à ε près et que $0 \notin]D - \varepsilon, D + \varepsilon[$.

b) On peut effectuer de façon très efficace des opérations élémentaires sur les matrices à coefficients entiers - et plus généralement sur un anneau euclidien A. Dans ce cas, les seules dilatations « autorisées » sont les $D_i(\lambda)$ avec λ inversible dans A. La division euclidienne est après tout l'opération élémentaire $\begin{pmatrix} a \\ b \end{pmatrix} \to \begin{pmatrix} a - bq \\ b \end{pmatrix}$. L'algorithme d'Euclide nous dit que par opérations élémentaires on peut passer de $\begin{pmatrix} a \\ b \end{pmatrix}$ à $\begin{pmatrix} d \\ 0 \end{pmatrix}$ où d est le PGCD de a et b.

Nous ne pousserons pas plus loin ces considérations - qui sont hors programme - mais signalons juste que l'on démontre ainsi que pour un anneau euclidien A :

- $SL_n(A)$ est engendré par les matrices de transvection ;
- toute matrice de $M_{m,n}(A)$ est équivalente à une matrice $\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}$ où D est une matrice carrée d'ordre r diagonale $D = \mathrm{diag}(d_i)$ avec $d_1 | d_2 | \ldots | d_r$.

7.4 Exercices

7.4.1 Calculs de déterminants

7.1 Exercice. Soient $A \in \mathcal{M}_p(K)$, $B \in \mathcal{M}_{p,q}(K)$ et $C \in \mathcal{M}_q(K)$. Notons $M \in \mathcal{M}_{p+q}(K)$ la matrice qui admet la décomposition par blocs $M = \begin{pmatrix} A & B \\ 0_{q,p} & C \end{pmatrix}$. Démontrer que l'on a $\det M = \det A \det C$.

Indication : Distinguer le cas où A est inversible et celui où elle ne l'est pas.

Par récurrence, on en déduit que si M est une matrice triangulaire par blocs et si l'on note $A_1, \ldots, A_k$ ses blocs diagonaux, alors $\det M = \det A_1 \ldots \det A_k$.

7.2 Exercice. Soient $a_1, \ldots, a_n \in K$. Considérons le déterminant

$$\Delta_n(a_1, \ldots, a_n) = \begin{vmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} \\ 1 & a_3 & a_3^2 & \ldots & a_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{vmatrix}$$

appelé *déterminant de Vandermonde.*

1. Calculer $\Delta_2(a_1, a_2)$.
2. En considérant $\Delta_n(a_1, \ldots, a_n)$ comme polynôme en a_n, établir l'égalité
$$\Delta_n(a_1, \ldots, a_n) = \Delta_{n-1}(a_1, \ldots, a_{n-1}) \prod_{k=1}^{n-1} (a_n - a_k).$$
3. En déduire que $\Delta_n(a_1, \ldots, a_n) = \displaystyle\prod_{1 \leqslant j < k \leqslant n} (a_k - a_j)$.
4. Pouvait-on prévoir dès le départ que si les a_i sont distincts $\Delta_n(a_1, \ldots, a_n) \neq 0$? Quelle application linéaire représente cette matrice ?

7.3 Exercice. Soit $P = \displaystyle\sum_{k=0}^{n} a_k X^k \in K[X]$ un polynôme unitaire ($a_n = 1$). En développant relativement à une ligne ou une colonne, démontrer que l'on a

$$\begin{vmatrix} \lambda & 0 & 0 & \ldots & 0 & a_0 \\ -1 & \lambda & 0 & \ldots & 0 & a_1 \\ 0 & -1 & \lambda & \ddots & 0 & a_2 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \lambda & a_{n-2} \\ 0 & 0 & 0 & \ldots & -1 & \lambda + a_{n-1} \end{vmatrix} = P(\lambda).$$

7.4 Exercice. Soient K un corps commutatif et $n \in \mathbb{N}^*$. Soit $P = X^n + \displaystyle\sum_{k=0}^{n-1} a_k X^k$ un polynôme unitaire de degré n. Notons E_n l'espace vectoriel des polynômes de degré $< n$. Soit $T \in L(E_n)$ l'application linéaire qui à $Q \in E_n$ associe le reste de la division euclidienne de XQ par P.

1. Quelle est la matrice de T dans la base $(1, X, \ldots, X^{n-1})$ de E ?
2. Calculer $\det T$.

3. Quelle est la matrice de $T - \lambda \mathrm{id}_{E_n}$ dans la base $(1, X - \lambda, \ldots, (X - \lambda)^{n-1})$.
4. Calculer $\det(T - \lambda \mathrm{id}_{E_n})$.

7.5 Exercice. *Déterminant de Cauchy.* Soient $x_1, \ldots x_n, y_1 \ldots, y_n \in K$. On suppose que pour tout i, j, on a $x_i + y_j \neq 0$. Calculer le déterminant de la matrice $\left(\dfrac{1}{x_i + y_j}\right)$.

7.6 Exercice. Pour $n \in \mathbb{N}^*$, calculer la différence entre le nombre de dérangements pairs et le nombre des dérangements impairs.

7.7 Exercice. [Semi-continuité du rang] Soit $m, n, r \in \mathbb{N}$. Démontrer que les matrices de rang $\leqslant r$ forment un fermé de $\mathcal{M}_{m,n}(\mathbb{K})$ (pour $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$). On suppose que $r \leqslant \min(m, n)$. Quelle est l'adhérence de l'ensemble des matrices de rang r ?

7.4.2 Opérations élémentaires

Il est certainement utile de faire un certain nombre d'exercices pratiques de résolution de systèmes linéaires - que l'on trouve dans de nombreux ouvrages. On ne présente ici que quelques exercices un peu plus théoriques.

7.8 Exercice. Calculer le déterminant de Vandermonde par opérations élémentaires.

Indication : On commence par retrancher la première ligne de toutes les autres - et on développe par la première colonne ; puis on met un terme en facteur dans toutes les lignes obtenues ; enfin on retranche chaque colonne à la suivante.

7.9 Exercice. Soient $A \in \mathcal{M}_{m,n}(K)$ une matrice et U une matrice carrée d'ordre m inversible. Posons $A' = UA$. Notons $C_1, \ldots, C_n$ les colonnes de A, r son rang, et $C'_1, \ldots, C'_n$ les colonnes de A' et r' son rang.

1. Démontrer que $r = r'$ et que pour toute partie J de $\{1, \ldots n\}$, on a $\mathrm{rg}\{C_j;\ j \in J\} = \mathrm{rg}\{C'_j;\ j \in J\}$. On suppose que $A' = UA$ est échelonnée réduite.
2. Pour $k = 1, \ldots, r$, notons $j(k)$ la place du $k^{\text{ème}}$ pivot de A'. Démontrer que
$$j(k) = \inf\{j;\ \mathrm{rg}(C_1, \ldots, C_j) = k\}.$$
3. Écrivons $A' = (a'_{i,j})$. Démontrer que l'on a $C_j = \sum_{k=1}^{r} a'_{k,j} C_{j(k)}$.
4. En déduire que pour toute matrice A il existe une et une seule matrice échelonnée réduite qui s'écrive $A' = UA$ avec U inversible.
   En ce sens, les matrices échelonnée réduite représentent les classes de l'action de $GL(n)$ par multiplication à gauche sur $M_{n,p}$.

7.10 Exercice.
1. Démontrer que $SL(n, K)$ est le sous-groupe des commutateurs de $GL(n, K)$ (sauf pour $n = 2$ et $K = \mathbb{F}_2$).
2. Démontrer que $SL(n, \mathbb{R})$ et $SL(n, \mathbb{C})$ sont connexes. En déduire que $GL(n, \mathbb{R})$ a deux composantes connexes et $GL(n, \mathbb{C})$ est connexe.

7.11 Exercice. (Décomposition LU.)

7.12 Exercice. (****) Soient $p \in \mathbb{N}$ et E un K-espace vectoriel de dimension finie. Notons Λ_p l'espace vectoriel des formes p-linéaires alternées $D : E^p \to K$.

1. Soient F un espace vectoriel de dimension p, $f : E \to F$ une application linéaire et B une base de F. Démontrer que l'application $(x_1, \ldots, x_p) \mapsto \det_B(f(x_1), \ldots, f(x_p))$ est un élément de Λ_p.
2. Fixons une base $(e_1, \ldots, e_n)$ de E. Notons J_p l'ensemble des applications strictement croissantes $s : \{1, \ldots, p\} \to \{1, \ldots, n\}$. Démontrer que l'application $\Phi : \Lambda_p \to K^{J_p}$ définie par $\Phi(D)(s) = D(e_{s(1)}, e_{s(2)}, \ldots, e_{s(p)})$ est linéaire et bijective.
3. En déduire que pour $p \leqslant n$, l'espace vectoriel Λ_p est de dimension $\binom{n}{p}$, et que, pour $p > n$, l'espace vectoriel des formes p-linéaires alternées est réduit à 0.

8 Réduction des endomorphismes

Nous énonçons ici les définitions, propriétés, résultats en termes d'endomorphismes. Ils peuvent bien sûr être aussi énoncés en termes de similitude de matrices carrés. On peut en effet identifier une matrice carrée $A \in \mathcal{M}_n(K)$ avec l'endomorphisme $X \mapsto AX$ de $\mathcal{M}_{n,1}(K)$ qu'elle définit.

8.1 Vecteurs propres et valeurs propres

8.1.1 Sous-espaces stables par un endomorphisme

8.1 Définition. Soit u un endomorphisme d'un espace vectoriel E. Un sous-espace vectoriel F est dit *stable* par u si $u(F) \subset F$. L'application $x \mapsto u(x)$ de F dans F est un endomorphisme de f appelé *endomorphisme* de F *induit* par u.

Soit E un espace vectoriel de dimension finie, u un endomorphisme de E et F un sous-espace vectoriel de E. Soit $(e_1, \ldots, e_k)$ une base de F que l'on complète en une base $B = (e_1, \ldots, e_n)$ de E. Alors F est stable par u si et seulement si la matrice de u dans la base B est de la forme $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$.

8.2 Proposition. *Si les endomorphismes u et v commutent, alors* $\operatorname{im} u$ *et* $\ker u$ *sont stables par v.*

8.1.2 Vecteurs propres et valeurs propres

On cherche à présent les espaces stables de dimension 1.

8.3 Définition. Soient E un K-espace vectoriel et u un endomorphisme de E.

a) Soient $\lambda \in K$ et x un vecteur non nul de E. On dit que λ et x sont une *valeur propre et un vecteur propre associés* si $u(x) = \lambda x$.

b) Soit $\lambda \in K$. On dit que λ est une *valeur propre* de u s'il existe un vecteur $x \in E$ non nul tel que $u(x) = \lambda x$.

c) Soit $x \in E$ un vecteur non nul. On dit que x est *vecteur propre* de u si $u(x)$ est proportionnel à x.

d) Soit $\lambda \in K$ une valeur propre de u. L'espace propre associé est $\ker(u - \lambda \mathrm{id}_E) = \{x \in E;\ u(x) = \lambda x\}$. On le note $E_\lambda(u)$.

Il est parfois commode de poser $E_\lambda(u) = \ker(u - \lambda \mathrm{id}_E)$ même lorsque λ n'est pas une valeur propre de u. Dans ce cas, on a $E_\lambda(u) = \{0\}$.

8.4 Proposition. *Les espaces propres d'un endomorphisme sont en somme directe.*

On doit démontrer que pour tout N et tout n-uplet $(\lambda_1, \ldots, \lambda_N)$ de valeurs propres distinctes de u les espaces propres $E_{\lambda_1}, \ldots, E_{\lambda_N}$ sont en somme directe.

- Pour $n = 1$, il n'y a rien à démontrer.
- Soit $N \geqslant 2$ et $\lambda_1, \ldots, \lambda_N$ des valeurs propres distinctes de u. Supposons que les espaces propres $E_{\lambda_1}, \ldots, E_{\lambda_{N-1}}$ soient en somme directe. Soient $x_i \in E_{\lambda_i}$ tels que $\sum_{i=1}^{N} x_i = 0$. Alors $0 = u(\sum_{i=1}^{N} x_i) = \sum_{i=1}^{N} \lambda_i x_i$, donc $\sum_{i=1}^{N-1} (\lambda_N - \lambda_i) x_i = \lambda_N \sum_{i=1}^{N} x_i - \sum_{i=1}^{N} \lambda_i x_i = 0$. Puisque $E_{\lambda_1}, \ldots, E_{\lambda_{N-1}}$ sont en somme directe, il vient $(\lambda_N - \lambda_1)x_1 = \ldots = (\lambda_N - \lambda_{N-1})x_{N-1} = 0$ et puisque les λ_i sont distincts, il vient $x_1 = \ldots = x_{N-1} = 0$. Enfin l'égalité $\sum_{i=1}^{N} x_i = 0$ permet de conclure que $x_N = 0$ aussi.

8.1.3 Polynôme caractéristique

Soient E un K-espace vectoriel de dimension finie et u un endomorphisme de E. Notons $A = (a_{i,j}) \in \mathcal{M}_n(K)$ la matrice de u dans une base B de E. Notons $M = (m_{i,j}) \in \mathcal{M}_n(K[X])$ la matrice définie par $m_{i,j} = a_{i,j}$ si $i \neq j$ et $m_{i,i} = a_{i,i} - X$. On pose $\chi_u^B = \det(M) \in K[X]$) (*cf.* remarque 7.11).

Soit B_1 une autre base de E, notons $P \in \mathcal{M}_n(K)$ la matrice de passage de B à B_1 et $A_1 = P^{-1}AP$ la matrice de l'endomorphisme u dans la base B_1. On plonge K dans le corps $K(X)$ des fractions rationnelles sur K. Par définition, $\chi_u^B = \det(A - XI_n)$ et $\chi_u^{B_1} = \det(A_1 - XI_n) = \det(P^{-1}(A - XI_n)P) = \det(P^{-1})\chi_u^B \det P$. En d'autres termes, on a démontré que le polynôme χ_u^B ne dépend pas de la base B.

8.5 Définition. Soient E un K-espace vectoriel de dimension finie et u un endomorphisme de E. On appelle *polynôme caractéristique* de l'endomorphisme u et l'on note χ_u le polynôme χ_u^B pour n'importe quelle base B de E.

Pour tout $\lambda \in K$, on a donc $\det(u - \lambda \mathrm{id}_E) = \chi_u(\lambda)$ (on applique la remarque 7.11 à l'homomorphisme $P \mapsto P(\lambda)$ de $K[X]$ dans K). Remarquons que cette égalité définit le polynôme caractéristique si K est infini.

On a immédiatement :

8.6 Proposition. *Soient E un K-espace vectoriel de dimension finie et u un endomorphisme de E. Les valeurs propres de u sont les racines de χ_u.*

8.1.4 Triangulation d'un endomorphisme

Une matrice carrée $A = (a_{i,j} \in \mathcal{M}_n(K)$ est dite *triangulaire supérieure* (*resp. inférieure*) si pour $i > j$ (*resp.* $i < j$) on a $a_{i,j} = 0$.

On dit qu'un endomorphisme u d'un espace vectoriel de dimension finie E est *triangulable* ou *trigonalisable* s'il existe une base de E dans laquelle la matrice de u est triangulaire. On dit qu'une matrice carrée M est *triangulable* ou *trigonalisable* si c'est la matrice d'un endomorphisme trigonalisable, *i.e.* s'il existe une matrice inversible P telle que $P^{-1}MP$ soit triangulaire.

8.7 Théorème. *Un endomorphisme (une matrice carrée) est trigonalisable si et seulement si son polynôme caractéristique est scindé.*

Le polynôme caractéristique d'une matrice triangulaire $A = (a_{i,j})$ est $\prod_{i=1}^{n}(a_{i,i} - X)$. Il est scindé. Si un endomorphisme (une matrice carrée) est trigonalisable, son polynôme caractéristique est égal au polynôme caractéristique d'une matrice triangulaire : il est scindé.

Démontrons la réciproque par récurrence sur la dimension de l'espace :

Si $n = 1$, il n'y a rien à démontrer : toute matrice est triangulaire ! !

Soit $n > 1$. Supposons que tout endomorphisme d'un espace vectoriel de dimension $n-1$ (toute matrice carrée d'ordre $n-1$) à polynôme caractéristique scindé soit trigonalisable. Soit E un espace vectoriel de dimension n et u un endomorphisme dont le polynôme caractéristique χ_u s'écrit $\chi_u = \prod_{i=1}^{n}(\lambda_i - X)$. Comme λ_1 est une valeur propre de E, il existe un vecteur propre e_1 associé à la valeur propre λ_1. Complétons e_1 en une base B de E. La matrice de u dans la base B est de la forme $M = \begin{pmatrix} \lambda_1 & L \\ 0 & N \end{pmatrix}$.

On a $\chi_M = \chi_u = (\lambda_1 - X)\chi_N$, donc $\chi_N = \prod_{i=2}^{n}(\lambda_i - X)$. D'après l'hypothèse de récurrence, N est

trigonalisable : il existe une matrice carrée inversible Q d'ordre $n-1$ telle que $Q^{-1}NQ$ soit triangulaire supérieure. Posons alors $P = \begin{pmatrix} 1 & 0 \\ 0 & Q \end{pmatrix}$. C'est une matrice inversible (d'inverse $\begin{pmatrix} 1 & 0 \\ 0 & Q^{-1} \end{pmatrix}$). La matrice $P^{-1}MP = \begin{pmatrix} \lambda_1 & LQ \\ 0 & Q^{-1}NQ \end{pmatrix}$ est triangulaire, d'où le résultat.

D'après la preuve ci-dessus, si u est un endomorphisme dont le polynôme caractéristique est $\chi_u = \prod_{i=1}^{n}(\lambda_i - X)$ on peut choisir une base dans laquelle la matrice de u sera triangulaire de diagonale $(\lambda_1, \ldots, \lambda_n)$, c'est-à-dire : on peut choisir l'ordre dans lequel apparaissent les éléments diagonaux.

8.1.5 Diagonalisation d'un endomorphisme

On dit qu'un endomorphisme d'un espace vectoriel de dimension finie E est *diagonalisable* s'il existe une base de E dans laquelle la matrice de E est diagonale. On dit qu'une matrice carrée M est *diagonalisable* si c'est la matrice d'un endomorphisme diagonalisable, *i.e.* s'il existe une matrice inversible P telle que $P^{-1}MP$ soit diagonale.

8.8 Proposition. *Soit u un endomorphisme d'un espace vectoriel de dimension finie E. Soit λ une valeur propre de E. Alors* $\dim E_\lambda$ *est inférieure ou égale à l'ordre de multiplicité de la racine λ dans le polynôme caractéristique χ_u.*

Soit $(e_1, \ldots, e_k)$ une base de E_λ. Complétons-la en une base de E. Dans cette base, la matrice de u est de la forme $M = \begin{pmatrix} \lambda I_k & * \\ 0 & N \end{pmatrix}$, donc $\chi_u = (\lambda - X)^k \chi_N$.

8.9 Théorème. *Soit u un endomorphisme d'un espace vectoriel de dimension finie E. Alors u est diagonalisable si et seulement si son polynôme caractéristique est scindé et la dimension de tout sous-espace propre est égale à l'ordre de multiplicité de la valeur propre associée.*

Si la matrice de u dans une base est la matrice diagonale $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, la dimension de l'espace propre associé à une valeur propre λ est égale au nombre de j tels que $\lambda_j = \lambda$ qui est lui-même égal à la multiplicité de la racine λ de $\chi_u = \prod_{j=1}^{n}(\lambda_j - X)$.

Inversement, si χ_u est scindé et la dimension de tout sous-espace propre est égale à l'ordre de multiplicité de la valeur propre associée, en mettant ensemble des bases des espaces propres, on obtient une famille libre d'après la prop. 8.4. Le nombre d'éléments de cette famille libre est $\sum_\lambda \dim E_\lambda = \sum_\lambda \mathrm{ordre}(\lambda) = \partial\chi_u = \dim E$: c'est donc une base. La matrice de u dans cette base est diagonale.

Remarquons que toute racine λ de χ_u est une valeur propre de u : on a donc $1 \leqslant \dim E_\lambda \leqslant \mathrm{ordre}(\lambda)$. En particulier, si λ est racine simple de χ_u on aura $\dim E_\lambda = \mathrm{ordre}(\lambda)$. Pour voir si u est diagonalisable, on ne doit donc se préoccuper que des racines multiples de χ_u.

8.10 Corollaire. *Un endomorphisme dont le polynôme caractéristique est scindé à racines simples est diagonalisable.*

8.2 Polynômes d'endomorphismes

8.2.1 Polynômes annulateurs, polynôme minimal

Soient E un espace vectoriel et u un endomorphisme de E. Pour un polynôme $P = \sum_{k=0}^{N} a_k X^k$, on pose $P(u) = \sum_{k=0}^{N} a_k u^k$. L'application $P \mapsto P(u)$ est un homomorphisme d'algèbres de $K[X]$ dans $L(E)$.

Si E est de dimension finie, cet homomorphisme n'est pas injectif. Son noyau est un idéal de l'anneau principal $K[X]$.

8.11 Définition. Un polynôme P est dit *annulateur* pour u si $P(u) = 0$. On appelle *polynôme minimal* de u l'unique polynôme unitaire ϖ_u qui engendre l'idéal formé par les polynômes annulateurs pour u.

En d'autres termes, les polynômes annulateurs sont les multiples du polynôme minimal. Pour $P \in K[X]$, on a donc $P(u) = 0 \iff \varpi_u | P$.

8.2.2 Le théorème de Cayley-Hamilton

8.12 Théorème de Cayley-Hamilton. *Soient E un espace vectoriel de dimension finie et u un endomorphisme de E. On a $\chi_u(u) = 0$.*

En d'autres termes ϖ_u divise χ_u.

Il y a de nombreuses démonstrations de ce théorème. En voici une relativement simple basée sur les matrices compagnon.

Soit $x \in E$ un vecteur non nul. Soit k le plus petit entier tel que $u^k(x)$ soit contenu dans le sous-espace engendré par les $u^j(x)$ pour $0 \leqslant j < k$. Écrivons $u^k(x) = \sum_{j=0}^{k-1} a_j u^j(x)$. Pour $j = 1, \ldots, k$, posons $e_j = u^{j-1}(x)$. Par définition de k, la famille $(e_1, \ldots, e_k)$ est libre. Complétons-la en une base $(e_1, \ldots, e_n)$ de E. Dans cette base, la matrice de u est sous la forme $\begin{pmatrix} C & D \\ 0 & N \end{pmatrix}$ où C est la matrice carrée d'ordre k (appelée matrice compagnon) : $C = \begin{pmatrix} 0 & 0 & \ldots & 0 & a_0 \\ 1 & 0 & \ldots & 0 & a_1 \\ 0 & 1 & \ldots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & a_{k-1} \end{pmatrix}$. Il en résulte que $\chi_u = \chi_C \chi_N$.

Or $(-1)^k \chi_C = X^k - \sum_{j=0}^{k-1} a_j X^j$ (*cf.* exerc. .7.3). On a donc $(-1)^k \chi_C(u)(x) = u^k(x) - \sum_{j=0}^{k-1} a_j u^j(x) = 0$. Il vient $\chi_u(u)(x) = \chi_N(u) \circ \chi_C(u)(x) = 0$. Cela étant vrai pour tout x, il vient $\chi_u(u) = 0$.

8.2.3 Théorème de décomposition des noyaux

8.13 Théorème de décomposition des noyaux. *Soient $P_1, \ldots, P_k$ des polynômes premiers entre eux deux à deux. Posons $P = \prod_{j=1}^{k} P_j$. Soient E un espace vectoriel et u un endomorphisme de E.*

a) On a $\ker P(u) = \bigoplus_{j=1}^{k} \ker(P_j(u))$.

b) En particulier, si P est un polynôme annulateur de u, on a $E = \bigoplus_{j=1}^{k} \ker(P_j(u))$. De plus, pour tout j, le projecteur d'image $\ker P_j(u)$ et de noyau $\bigoplus_{i\neq j} \ker(P_i(u))$ est un polynôme en u (i.e. un élément de l'algèbre $K[u]$).

Pour $j \in \{1, \ldots, k\}$, posons $Q_j = P/P_j = \prod_{i\neq j} P_i$. Comme P_j et Q_j sont premiers entre eux, il existe un polynôme R_j tel que $R_jQ_j \equiv 1 \quad [P_j]$. Posons enfin $S_j = R_jQ_j$. Pour $i \neq j$, P_i divise S_j, donc $\sum_{i=1}^{k} S_i \equiv 1 \quad [P_j]$. Alors $1 - \sum_{i=1}^{k} S_i$ est divisible par les P_j, donc par leur PPCM, c'est-à-dire P. Remarquons aussi que, pour tout j, P divise P_jS_j.

- Puisque $P = Q_jP_j$, on a $P(u) = Q_j(u) \circ P_j(u)$, donc $\ker P_j(u) \subset \ker P(u)$. Il vient $\sum_{j=1}^{k} \ker P_j(u) \subset \ker P(u)$.
- Soit $x \in \ker P(u)$. Comme P divise P_jS_j, on a $P_j(u) \circ S_j(u)(x) = 0$, donc $S_j(u)(x) \in \ker P_j(u)$. Comme P divise $1 - \sum_{i=1}^{k} S_i$, si $x \in \ker P(u)$, alors $x = \sum_{j=1}^{k} S_j(u)(x)$. Donc $\ker P(u) \subset \sum_{i=1}^{k} \ker P_j(u)$.
- Donnons-nous des x_j pour $j = 1, \ldots, n$ avec $x_j \in \ker P_j(u)$ tels que $\sum_{j=1}^{k} x_j = 0$. Comme P_j divise $1 - S_j$, alors $S_j(u)(x_j) = x_j$; pour $i \neq j$, P_i divise S_j, donc $S_j(u)(x_i) = 0$. Il vient $x_j = S_j(u)(\sum_{i=1}^{k} x_i) = 0$. Donc les $\ker P_j(u)$ sont en somme directe.

L'assertion (b) résulte aussi des calculs ci-dessus : le projecteur d'image $\ker P_j(u)$ et de noyau $\sum_{i\neq j} \ker(P_i(u))$ est $S_j(u)$.

8.2.4 Endomorphismes diagonalisables

8.14 Proposition. *Soient E un espace vectoriel de dimension finie et u un endomorphisme de E. Les propriétés suivantes sont équivalentes :*

(i) *u est diagonalisable ;*

(ii) *u admet un polynôme annulateur scindé à racines simples ;*

(iii) *le polynôme minimal de u est scindé à racines simples.*

Tout diviseur d'un polynôme scindé à racines simples est scindé à racines simples ; donc $(ii) \iff (iii)$.

Soient $\lambda_1, \ldots, \lambda_k$ les valeurs propres de u et posons $P = \prod_{i=1}^{k} (X - \lambda_i)$. Si u est diagonalisable, il admet une base B de vecteurs propres. L'endomorphisme $P(u)$ est nul sur la base B, donc il est nul. Le polynôme P est donc un polynôme annulateur.

Inversement, s'il existe un polynôme annulateur scindé à racines simples $P = \prod_{i=1}^{k} (X - \lambda_i)$, alors $E = \bigoplus_{i=1}^{k} \ker(u - \lambda_i \mathrm{id}_E)$ d'après le « lemme des noyaux » (théorème 8.13).

8.15 Corollaire. *Soient E un espace vectoriel de dimension finie et u un endomorphisme diagonalisable de E. La restriction de u à tout sous-espace de E stable par u est diagonalisable.*

8.16 Proposition. *Soient E un espace vectoriel et $(u_i)_{i\in I}$ une famille d'endomorphismes de E. On suppose que tous les u_i sont diagonalisables et que pour tout $i, j \in I$, on a $u_i \circ u_j = u_j \circ u_i$. Alors il existe une base $(e_1, \ldots, e_n)$ de E dans laquelle tous les u_i sont diagonaux.*

Procédons une récurrence « forte » sur $\dim E$. Si $\dim E$ est 1, il n'y a rien à démontrer, de même que si tous les u_i sont des homothéties.

Supposons donc que u_{i_0} n'est pas une homothétie. Alors $E = \bigoplus_{k=1}^{m} E_k$ où les E_k sont les espaces propres de u_{i_0} ; chacun de ces espaces est invariant par tous les u_i, et les restrictions des u_i à ces espaces sont diagonalisables et deux à deux permutables. Par l'hypothèse de récurrence, il existe une base de chacun des E_k qui diagonalise toutes les restrictions des u_i. Mettant ensemble toutes ces bases, on trouve une base de E qui diagonalise les u_i.

8.2.5 Sous-espaces caractéristiques

8.17 Définition. Soient E un espace vectoriel de dimension finie, u un endomorphisme de E et λ une valeur propre de u. Soit r l'ordre de multiplicité de λ dans χ_u. On appelle *sous-espace caractéristique* de u associé à la valeur propre λ le noyau de $(\lambda \mathrm{id}_E - u)^r$.

8.18 Proposition. *Soient E un espace vectoriel de dimension finie et u un endomorphisme de E. On suppose que le polynôme caractéristique de u est scindé. Alors E est somme directe des sous-espaces caractéristiques de u.*

Cette proposition résulte du lemme de décomposition des noyaux (théorème 8.13) à l'aide du théorème de Cayley-Hamilton.

8.19 Définition. Soit E un espace vectoriel. Un endomorphisme u de E est dit *nilpotent* s'il existe $p \in \mathbb{N}$ tel que $u^p = 0$.

Si n est nilpotent, toute valeur propre de u est nulle. En fait $\chi_u = (-X)^{\dim E}$ (*cf.* exerc. 8.7).

8.20 Théorème: Décomposition de Dunford. *Soient E un espace vectoriel de dimension finie et u un endomorphisme de E. On suppose que le polynôme caractéristique de u est scindé. Il existe un unique couple (d, n) d'endomorphismes tels que $u = d + n$ avec d diagonalisable n nilpotent et satisfaisant $d \circ n = n \circ d$.*

Existence. Soient $(\lambda_1, \ldots, \lambda_k)$ les valeurs propres distinctes de u. Pour tout j, notons N_j l'espace caractéristique associé à λ_j. D'après le théorème de décomposition des noyaux, $E = \bigoplus_{j=1}^{k} N_j$. Notons p_j le projecteur d'image N_j et de noyau $\bigoplus_{i\neq j} N_i$. Posons $d = \sum_{j=1}^{n} \lambda_j p_j$. Il est diagonalisable : son espace propre pour la valeur propre λ_j est N_j. Posons $n = u - d$. Chaque N_j est stable par n et l'endomorphisme de N_j induit par n coïncide avec $u - \lambda_j \mathrm{id}_E$. Il est nilpotent. On en déduit que n est nilpotent. Enfin, les p_j sont des polynômes en u, donc d et n sont des polynômes en u : ils commutent.

Unicité. Soient (d, n) le couple construit dans la partie existence, et (d', n') un autre couple satisfaisant les conditions ci-dessus. Alors d' commute à u, donc à tout polynôme en u. Il commute avec d. D'après la prop. 8.16, d et d' sont simultanément diagonalisables. De même, n' et n commutent. On en déduit (d'après la formule du binôme) que $n' - n$ est nilpotent. Or $d - d' = n' - n$. Cet endomorphisme est diagonalisable et nilpotent : ces valeurs propres sont toutes nulles. Il est nul.

8.3 Applications ; considérations topologiques dans le cas où le corps K est $\mathbb{R}$ ou $\mathbb{C}$

8.3.1 Puissances de matrices ; suites récurrentes

Donnons-nous une suite (X_k) de vecteurs-colonne définie par une relation de récurrence $X_{k+1} = AX_k$ où A est une matrice carrée donnée. Il vient immédiatement $X_k = A^k X_0$, d'où la nécessité de calculer les puissances de A.

Une telle formule de récurrence peut être un peu plus cachée : fixons $a_0, \dots, a_{n-1} \in K$ et considérons une suite $(x_k)_{k\in\mathbb{N}}$ vérifiant pour tout $k \in \mathbb{N}$, $x_{k+n} = \sum_{j=0}^{n-1} a_j x_{k+j}$. On pose alors $X_k = \begin{pmatrix} x_k \\ x_{k+1} \\ \vdots \\ x_{k+n-1} \end{pmatrix}$. La suite X_k vérifie la relation de récurrence $X_{k+1} = AX_k$ où $A = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ a_0 & a_1 & a_2 & \dots & a_{n-1} \end{pmatrix}$ est (la transposée d')une matrice compagnon.

Il est bien plus facile de calculer les puissances d'une matrice si elle est sous forme diagonale ! Si A est diagonalisable, elle s'écrit $A = PDP^{-1}$ avec $D = \mathrm{diag}(\lambda_1, \dots, \lambda_n)$ diagonale. Alors, on a $A^k = PD^kP^{-1}$ et $D^k = \mathrm{diag}(\lambda_1^k, \dots, \lambda_n^k)$.

Faisons quelques remarques dans le cas où $K = \mathbb{R}$ ou $K = \mathbb{C}$. Rappelons que, sur un espace vectoriel réel ou complexe de dimension finie, toutes les normes sont équivalentes et définissent donc la même topologie, en particulier la même notion de convergence des suites, de continuité, différentiabilité, *etc.*

1. Si $K = \mathbb{R}$, il peut être utile de considérer une matrice $A \in \mathcal{M}_n(\mathbb{R})$ comme matrice à coefficients complexes et de la diagonaliser sur $\mathbb{C}$.
2. Si $A \in \mathcal{M}_n(\mathbb{C})$ n'est pas diagonalisable, on peut utiliser la décomposition de Dunford : $A = D+N$ avec $DN = ND$ où A est diagonalisable et N est nilpotente. Comme $N^n = 0$, la formule du binôme qui calcule $(D+N)^k$ (pour k grand) n'a que n termes.
3. On peut étudier le comportement à l'infini d'une suite $X_k = A^k X_0$. Par les deux remarques précédentes, l'étude d'une telle suite se ramène (presque) à une étude de suites géométriques.

Un exemple : nombre de chemins de longueur n dans un graphe. Un graphe (orienté) est donné par deux ensembles X, Y et deux applications s et b de Y dans X. Les éléments de l'ensemble X s'appellent les *sommets* du graphe ; ceux de l'ensemble Y les *arêtes* (orientées). Une arête y va du sommet $s(y)$ *source* de y, au sommet $b(y)$ *but* de y. On dit que le graphe est fini si les ensembles X et Y sont finis.

Un graphe non orienté est donné par un graphe orienté (X, Y, s, b) avec une application $\tau : Y \to Y$ (de retournement des arêtes) satisfaisant $\tau \circ \tau = \mathrm{id}_Y$ et $s \circ \tau = b$ (donc $b \circ \tau = s$).

La matrice d'adjacence d'un graphe fini (X, Y, s, b) est la matrice carrée A dont les lignes et les colonnes sont indexées par X dont le coefficient $a_{x,x'}$ est le nombre d'arêtes de source x et de but x'. Remarquons que la matrice d'adjacence d'un graphe non orienté est symétrique.

Pour $n \in \mathbb{N}$, un chemin de longueur n dans le graphe (X, Y, s, b) est une suite $(y_1, y_2, \dots, y_n)$ d'arêtes telles que pour $j = 1, \dots, n-1$ on ait $s(y_{j+1}) = b(y_j)$; la source d'un tel chemin est $s(y_1)$ et son but est $b(y_n)$.

Pour calculer le nombre $a_{x,x'}^{(n)}$ de chemins de longueur n de source x et de but x', remarquons qu'un tel chemin est donné par un élément $z \in X$, un chemin $(y_1, \ldots, y_{n-1})$ de longueur $n-1$ de source x et de but z et un chemin y_n de source z et de but x'. En d'autres termes, on a $a_{x,x'}^{(n)} = \sum_{z \in X} a_{x,z}^{(n-1)} a_{z,x'}$.

Par récurrence sur n, on en déduit que la matrice $(a_{x,x'}^{(n)})_{x,x'}$ est la puissance n-ième A^n de la matrice A. On trouvera dans l'exercice 8.18 quelques calculs de nombre de chemins dans un graphe à l'aide de puissances de matrices.

Matrices de transition. On peut aussi affecter chaque arête du graphe d'un poids. Un exemple typique de cette situation est le cas où les sommets du graphe représentent des *états* d'un système évoluant dans le temps et les coefficients des arêtes représentent la *probabilité de transition* d'un état à un autre en une unité de temps. Un exemple « pratique » est donnée dans l'exercice 8.19 ci-dessous. On trouvera d'autres exemples dans Dantzer p. 411 avec des enfants jouant à la balle, dans Escoffier 1.14 p. 29 avec des particules se déplaçant dans un triangle...

On se donne donc N états possibles d'un système qui évolue dans temps. On suppose que la probabilité $p_{i,j}$ de passer de l'état i au temps n à l'état j au temps $n+1$ ne dépend que de i et de j mais :
- pas du temps n ;
- et pas non plus de ce qui s'est passé avant.

On obtient ainsi une matrice $M = (p_{i,j})$ carrée de taille N. Alors, les coefficients de la matrice $M^k = (p_{i,j}^{(k)})$ représentent la probabilité de passer de l'état i au temps n à l'état j au temps $n+k$. D'où l'utilité encore de réduire M afin de pouvoir calculer ses puissances.

Remarquons que, pour tout i, on a $\sum_{j=1}^{N} p_{i,j} = 1$ en d'autres termes $LM = L$ où L est la matrice-ligne dont tous les coefficients sont égaux à 1. Donc 1 est valeur propre de ${}^tM$, donc de M. De plus, les $p_{i,j}$ étant des probabilités on a $p_{i,j} \geqslant 0$ pour tous i, j. On entre ainsi dans le monde des matrices à coefficients positifs... On sait alors trouver un vecteur propre C avec des coefficients positifs associé à la valeur propre 1. On normalise C en supposant que la somme de ses coefficients vaut 1, (*i.e.* $LC = 1$). Toutes les autres valeurs propres (dans $\mathbb{C}$) de M sont de module $\leqslant 1$. Si pour n assez grand tous les coefficients de M^n sont strictement positifs (c'est-à-dire s'il est possible en n étapes de passer de n'importe quel état à n'importe quel état), alors cette valeur propre est simple et M^n converge vers le projecteur spectral CL correspondant quand $n \to \infty$. La convergence est géométrique de raison le module de la plus grande valeur propre.

8.3.2 Exponentielles de matrices et applications

8.21 Proposition. *Soit E un espace vectoriel réel ou complexe de dimension finie.*

a) Soit $u \in L(E)$. La série de terme général $\dfrac{u^n}{n!}$ est convergente.

On pose $\exp(u) = \sum_{n=0}^{+\infty} \dfrac{u^n}{n!}$.

b) Soit $u, v \in L(E)$ tels que $u \circ v = v \circ u$. On a $\exp(u+v) = \exp(u)\exp(v)$.

c) Soit $u \in L(E)$. L'équation différentielle $x'(t) = u\,x(t)$ admet comme solution $x(t) = \exp(tu)x_0$.

Considérons le système différentiel $x'(t) = ux(t) + b(t)$, où b est une fonction continue définie sur un intervalle ouvert I à valeurs dans E. Cherchons la solution sous la forme $x(t) = \exp(tu)y(t)$. Le système devient $\exp(tu)y'(t) = b(t)$, soit $y(t) = y(t_0) + \int_{t_0}^{t} \exp(-tu)b(t)\,dt$.

Encore une fois, il est bien plus facile de calculer l'exponentielle d'une matrice si elle est diagonalisée : remarquons que $\exp(PDP^{-1}) = P\exp(D)\,P^{-1}$. Si l'endomorphisme u n'est pas diagonalisable, on utilisera sa décomposition de Dunford pour calculer $\exp(tu)$. Remarquons que si n est un endomorphisme nilpotent, $\exp(tn)$ est polynomiale en t.

8.3.3 Exemples de parties denses de $L(E)$

8.22 Proposition. *On suppose que $K = \mathbb{R}$ ou $\mathbb{C}$. Soit E un K-espace vectoriel de dimension finie.*

a) $GL(E)$ est ouvert et dense dans $L(E)$.

b) Si $K = \mathbb{C}$, l'ensemble des endomorphismes diagonalisables est dense dans $L(E)$.

Démonstration. a) L'application déterminant est polynomiale donc continue, donc $GL(E)$ image inverse par det de l'ouvert K^* de K est ouvert dans $L(E)$. Soit $u \in L(E)$. Comme χ_u a un nombre fini de racines, il y a un nombre fini de $k \in \mathbb{N}$ tels que $u_k = u - (1+k)^{-1}\mathrm{id}_E$ soit non inversible. Donc pour k assez grand, $u_k \in GL(E)$, et la suite u_k converge vers u, donc u est dans l'adhérence de $GL(E)$: donc $GL(E)$ est dense dans $L(E)$.

b) On peut trianguler u dans une base $(e_1, \dots, e_n)$ de E. Notons v l'endomorphisme de E tel que $ve_j = je_j$ pour $j \in \{1, \dots, n\}$. Soit $k \in \mathbb{N}^*$ un nombre tel que $\dfrac{n-1}{k}$ soit strictement inférieur à $\inf|\lambda_i - \lambda_j|$, cet « inf » étant pris sur tous les couples de valeurs propres distinctes. Alors les nombres $\lambda_j + \dfrac{j}{k}$ sont deux à deux distincts, donc $u + k^{-1}v$ a toutes ses valeurs propres distinctes : il est diagonalisable. □

8.4 Exercices

8.1 Exercice. Soit E un espace vectoriel de dimension finie. Soit $(E_1, \dots, E_k)$ une famille de sous-espaces vectoriels de E telle que $E = \bigoplus_{j=1}^{k} E_j$. Choisissons une base de E formée de bases de E_j. Caractériser les matrices des endomorphismes pour lesquels les sous-espaces E_j sont stables.

8.2 Exercice. Soient $a_0, \dots, a_n$ des nombres complexes. On définit les matrices $A, J \in M_n(\mathbb{C})$ en posant

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \dots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{pmatrix} \qquad \text{et} \qquad J = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

1. Démontrer que $A = \sum_{k=0}^{n-1} a_k J^k$.
2. Calculer le polynôme minimal et le polynôme caractéristique de J.
3. Diagonaliser J puis A.

Endomorphismes trigonalisables

8.3 Exercice. Soit E un espace vectoriel de dimension finie. Posons $n = \dim E$. Un *drapeau* de E est une suite $(E_k)_{0 \leqslant k \leqslant n}$ de sous-espaces de E telle que pour tout k on ait $E_k \subset E_{k+1}$ et $\dim E_k = k$. Une base $(e_1, \dots, e_n)$ est dite *adaptée* au drapeau $(E_k)_{0 \leqslant k \leqslant n}$ si pour tout k, on a $e_k \in E_k$.

1. Démontrer que toute base de E est adaptée à un et un seul drapeau de E. Démontrer que tout drapeau possède des bases adaptées.
2. Soient $(E_k)_{0\leqslant k\leqslant n}$ un drapeau, $(e_1,\dots,e_n)$ une base adaptée et u un endomorphisme de E. Démontrer que le drapeau $(E_k)_{0\leqslant k\leqslant n}$ est stable par u (*i.e.* tous les E_k sont stables par u) si et seulement si la matrice de u dans la base $(e_1,\dots,e_n)$ est triangulaire supérieure.
3. Soient u un endomorphisme de E et $(E_k)_{0\leqslant k\leqslant n}$ un drapeau stable par u. Notons $\lambda_1,\dots,\lambda_n$ les éléments diagonaux de la matrice de u dans une base $(e_1,\dots,e_n)$ adaptée à $(E_k)_{0\leqslant k\leqslant n}$. Démontrer que $(u-\lambda_k\mathrm{id}_E)(E_k)\subset E_{k-1}$. En déduire une démonstration du théorème de Cayley-Hamilton pour les endomorphismes triangulables.

8.4 Exercice.
1. Soient E un espace euclidien et u un endomorphisme trigonalisable de E. Démontrer qu'il existe une base orthonormale de E dans laquelle la matrice de u est triangulaire.
2. En déduire que l'ensemble des matrices trigonalisables est fermé dans $M_n(\mathbb{R})$.
3. Quelle est l'adhérence de l'ensemble des matrices diagonalisables réelles ?
4. Démontrer que l'intérieur de l'ensemble des matrices diagonalisables est formé des matrices diagonalisables à valeurs propres distinctes.

8.5 Exercice.
1. Soit $A\in M_n(K)$ une matrice carrée. On suppose que son polynôme caractéristique est scindé : $\chi_A=\prod_{k=1}^{n}(\lambda_k-X)$. Soit $Q\in K[X]$. Démontrer que $\chi_{Q(A)}=\prod_{k=1}^{n}(Q(\lambda_k)-X)$.
2. Soit P un polynôme unitaire à coefficients entiers. Soient $\lambda_1,\dots,\lambda_n$ ses racines dans $\mathbb{C}$ comptées avec leur multiplicité. Démontrer que pour tout entier $q\in\mathbb{N}$, le polynôme $\prod_{k=1}^{n}(X-\lambda_k^q)$ est à coefficients entiers.

   Indication : Utiliser une matrice compagnon.

8.6 Exercice. Démontrer qu'un endomorphisme d'un espace vectoriel de dimension finie est trigonalisable si et seulement s'il admet un polynôme annulateur scindé.

8.7 Exercice. Endomorphismes nilpotents. Soient E un espace vectoriel de dimension finie non nulle et u un endomorphisme nilpotent de E. Notons m le plus petit entier tel que $u^m=0$.
1. Quel est le polynôme minimal de u ?
2. Démontrer que u n'est pas surjective.
3. Démontrer que $\operatorname{im} u$ est stable par u. En déduire par récurrence sur $\dim E$ que u est triangulable. Quel est le polynôme caractéristique de u ?
4. Pour $k=0,\dots,m$, posons $N_k=\ker u^k$ et $I_k=\operatorname{im} u^k$ (on a $N_0=\{0\}=I_m$ et $N_m=E=I_0$). Démontrer que la suite (N_k) est croissante et la suite (I_k) est décroissante.
5. Démontrer que la suite $(\dim I_k-\dim I_{k+1})=(\dim N_{k+1}-\dim N_k)$ est décroissante.

Endomorphismes cycliques

8.8 Exercice. Soient E un espace vectoriel de dimension finie et u un endomorphisme de E.
1. Soit $x_0\in E$. Pour $k\in\mathbb{N}^*$, on pose $x_k=u^k(x_0)$. Soit $k\in\mathbb{N}^*$ tel que $x_k\in\operatorname{Vect}(x_0,\dots,x_{k-1})$. Démontrer que $\operatorname{Vect}(x_0,\dots,x_{k-1})$ est stable par u ; en déduire que pour tout $\ell\in\mathbb{N}$, on a $x_\ell\in\operatorname{Vect}(x_0,\dots,x_{k-1})$.

2. Un vecteur $x \in E$ est dit *cyclique pour l'endomorphisme* u si $(x, u(x), u^2(x), \ldots, u^k(x), \ldots)$ engendre E. On dit que u est *cyclique* s'il existe un vecteur $x \in E$ cyclique pour u. Démontrer que u est cyclique si et seulement s'il existe une base de E dans laquelle la matrice de u est une matrice compagnon. Démontrer que dans ce cas $\chi_u = \varpi_u$.

8.9 Exercice. *Cet exercice m'a été proposé par Gentiana Danila.*

1. Démontrer que pour tout $n \in \mathbb{N}^*$ il existe un polynôme irréductible de degré n sur $\mathbb{Q}$.
2. Démontrer qu'il existe un corps K contenant $\mathbb{Q}$ et qui est un $\mathbb{Q}$-espace vectoriel de dimension n sur $\mathbb{Q}$. Construire une application $\mathbb{Q}$-linéaire de K dans $M_n(\mathbb{Q})$ qui soit aussi un homomorphisme d'anneaux.
3. Démontrer que tout sous-espace de dimension n^2-n+1 de $M_n(\mathbb{Q})$ contient une matrice inversible.

8.10 Exercice. Soient E un espace vectoriel de dimension finie et u un endomorphisme de E. Pour $x \in E$, notons $J_x = \{P \in K[X];\ P(u)(x) = 0\}$.

1. Démontrer que, pour tout $x \in E$, J_x est un idéal de $K[X]$.
2. Démontrer que le vecteur x est cyclique pour u si et seulement si J_x est l'idéal engendré par le polynôme caractéristique de u.

   Écrivons $\varpi_u = \prod_{j=1}^{k} P_j^{\alpha_j}$ la décomposition de ϖ_u en produit de polynômes irréductibles unitaires.

   Pour $j \in \{1, \ldots, k\}$, soit $Q_j \in K[X]$ le polynôme tel que $P_j Q_j = \varpi_u$.
3. Démontrer que pour tout j, il existe $x \in E$ tel que $(Q_j(u))(x) \neq 0$. En déduire qu'il existe $x_j \in E$ tel que $P_j^{\alpha_j}(u)(x_j) = 0$ mais $P_j^{\alpha_j - 1}(u)(x_j) \neq 0$. Démontrer que J_{x_j} est l'idéal engendré par $P_j^{\alpha_j}$.
4. On pose $y = \sum_{j=1}^{k} x_j$. Démontrer que J_y est l'idéal engendré par ϖ_u.
5. Démontrer que u est cyclique si et seulement si $\varpi_u = \chi_u$.

8.11 Exercice. Soient E un espace vectoriel de dimension finie et u un endomorphisme de E.

1. On suppose que u est cyclique. Soient x un vecteur cyclique pour u et F un sous-espace vectoriel de E stable par u.
   a) Démontrer que l'ensemble $\mathcal{J} = \{P \in K[X];\ P(u)(x) \in F\}$ est un idéal dans $K[X]$.
   Il existe donc un unique polynôme unitaire P_F qui engendre $\mathcal{J}$.
   b) Démontrer que P_F divise le polynôme minimal ϖ_u de u (qui est égal au polynôme caractéristique de u - au signe près).
   On écrit $\varpi_u = P_F Q_F$.
   c) Démontrer que $F = \operatorname{im} P_F(u) = \ker Q_F(u)$.
   d) Démontrer que la restriction de u à F est cyclique et que $\dim F = \partial Q_F$.
2. On suppose que le corps K est infini. Démontrer que u est cyclique si et seulement si l'ensemble des sous-espaces de E stables par u est fini*(on pourra utiliser l'exercice 4.4)*.
3. On suppose que de E n'est pas nul. Démontrer que E ne possède pas de sous-espaces invariants par u autres que $\{0\}$ et E si et seulement si son polynôme caractéristique est irréductible.

Décomposition de Dunford

8.12 Exercice. Quelle est la décomposition de Dunford de la matrice $\begin{pmatrix} 1 & 1 \\ 0 & t \end{pmatrix}$?

8.13 Exercice. Soit $A \in \mathcal{M}_n(\mathbb{R})$. Considérons-la comme matrice à coefficients complexes et soit $A = D + N$ sa décomposition de Dunford (vue comme matrice à coefficients complexes). Démontrer que D et N sont des matrices réelles.

8.14 Exercice. Soient E un espace vectoriel de dimension finie et u un endomorphisme de E ; notons ϖ_u son polynôme minimal. Soit $P \in K[X]$. Démontrer que $P(u)$ est inversible si et seulement si ϖ_u et P sont premiers entre eux et que, dans ce cas, il existe un polynôme $Q \in K[X]$ tel que $P(u)^{-1} = Q(u)$.

8.15 Exercice. Soit u un endomorphisme d'un K-espace vectoriel E de dimension finie.

1. On suppose que le polynôme minimal de u est de la forme P^k où P est un polynôme irréductible de $K[X]$. Soient $x \in E$ non nul et F le sous-espace vectoriel de E engendré par les $u^j(x)$ $(j \in \mathbb{N})$. Notons v l'endomorphisme de F déduit de u par restriction. Démontrer que $\chi_v = \varpi_v$ est une puissance de P. En déduire (à l'aide d'une récurrence) que le polynôme caractéristique de u est une puissance de P.
2. En utilisant le « lemme des noyaux », démontrer que le polynôme minimal et le polynôme caractéristique d'un endomorphisme ont mêmes diviseurs irréductibles.
3. Démontrer que pour $P \in K[X]$ les assertions suivantes sont équivalentes :
   (i) Les polynômes P et χ_u sont premiers entre eux.
   (ii) Les polynômes P et ϖ_u sont premiers entre eux.
   (iii) L'endomorphisme $P(u)$ est inversible.

8.16 Exercice. Nous proposons une autre méthode pour démontrer que χ_u et ϖ_u ont mêmes diviseurs irréductibles (exercice 8.15). Soit P un diviseur irréductible de χ_u. Soit L une extension de K dans laquelle P a une racine. En considérant la matrice de u dans une base comme matrice à coefficients dans L, démontrer que $\det(P(u)) = 0$. En déduire que P divise ϖ_u.

8.17 Exercice. Soient E un espace vectoriel de dimension finie non nulle sur un corps K et u un endomorphisme de E.

1. Soit ϖ le polynôme minimal de u et soit P un polynôme irréductible divisant ϖ. Notons k le degré de P. Démontrer qu'il existe un sous-espace de dimension k stable par u.
2. On suppose que $K = \mathbb{R}$. Démontrer que u possède un sous-espace stable de dimension 1 ou un sous-espace stable de dimension 2.

Puissances et exponentielle de matrices

8.18 Exercice.
1. Combien de chemins de longueur n joignent un sommet d'un triangle à un autre ?
2. Combien de chemins de longueur n joignent un sommet d'un hexagone au sommet diagonalement opposé ?
3. Combien de chemins de longueur n joignent un sommet d'un pentagone à un autre ?
4. Combien de chemins de longueur n joignent un sommet d'un tétraèdre à un autre ?
5. Combien de chemins de longueur n joignent le sommet d'un cube au sommet diagonalement opposé ?

8.19 Exercice. *Un exemple de matrice de transition.* Une étude de la météo dans une ville dont nous tairons le nom donne les observations suivantes :

- Il est presque impossible d'avoir deux beaux jours consécutifs.
- S'il fait beau un jour, on a la même probabilité d'avoir un gros orage ou une pluie fine le lendemain.
- S'il ne fait pas beau un jour, une fois sur deux le temps sera le même le jour suivant ; et, si le temps change, on aura une chance sur deux qu'il fasse beau.

On considère enfin que le temps qu'il fera demain ne dépend que du temps d'aujourd'hui et non pas du temps des jours passés...

On note B_k, G_k, P_k, respectivement l'événement : le jour k il fait beau, on a un gros orage, ou juste une pluie fine et b_k, g_k, p_k les probabilités respectives de ces événements. On pose $X_k = \begin{pmatrix} b_k \\ g_k \\ p_k \end{pmatrix}$.

1. Exprimer X_{k+1} en fonction de X_k.
2. En déduire pour tout k une écriture de X_k en fonction de X_0.
3. S'il fait beau aujourd'hui, quelle est la probabilité qu'il fasse beau dans une semaine ?
4. Quelle est la proportion moyenne des jours de beau temps ?

8.20 Exercice. Démontrer que pour tout endomorphisme u d'un espace vectoriel réel (ou complexe) de dimension finie, il existe un polynôme $P \in \mathbb{K}[X]$ tel que $\exp(u) = P(u)$.

8.21 Exercice. Un endomorphisme u est dit *unipotent* si $u - \mathrm{id}$ est nilpotent. Soit E un espace vectoriel réel ou complexe de dimension finie.

1. Démontrer que l'exponentielle d'un endomorphisme nilpotent de E, est un endomorphisme unipotent.
2. Pour $k \in \mathbb{N}$, notons E_k et L_k les polynômes donnés par $E_k = \displaystyle\sum_{j=1}^{k} \frac{X^j}{j!}$ et $L_k = \displaystyle\sum_{j=1}^{k} \frac{(-1)^{j+1} X^j}{j}$.
   Démontrer que $E_k \circ L_k$ et $L_k \circ E_k$ admettent en 0 les développements limités $E_k \circ L_k(x) = x + o(x^k)$ et $L_k \circ E_k(x) = x + o(x^k)$. En déduire que si u est un endomorphisme de E tel que $u^{k+1} = 0$, on a $\exp(L_k(u)) = \mathrm{id} + u$ et $L_k(\exp(u) - \mathrm{id}) = u$.
3. Démontrer que exp est un homéomorphisme de l'ensemble des matrices carrées d'ordre n nilpotentes sur l'ensemble des matrices carrées d'ordre n unipotentes.
4. Démontrer que l'application $\exp : M_n(\mathbb{C}) \to GL_n(\mathbb{C})$ est surjective.

9 Formes quadratiques

9.1 Formes bilinéaires, formes quadratiques

9.1.1 Définitions et généralités

9.1 Définition. Soient K un corps commutatif et E un K-espace vectoriel.
- Rappelons qu'une *forme bilinéaire* sur E est une application $b : E \times E \to K$ linéaire en chacune des variables, *i.e.* telle que, pour tout $x \in E$, les applications $y \mapsto b(x, y)$ et $y \mapsto b(y, x)$ sont des formes linéaires sur E.
- Une forme bilinéaire $b : E \times E \to K$ est dite *symétrique* si pour tout $(x, y) \in E \times E$ on a $b(y, x) = b(x, y)$.
- Une forme bilinéaire $b : E \times E \to K$ est dite *antisymétrique* si pour tout $(x, y) \in E \times E$ on a $b(y, x) = -b(x, y)$.
- Une forme bilinéaire $b : E \times E \to K$ est dite *alternée* si pour tout $x \in E$ on a $b(x, x) = 0$.

9.2 Proposition. *a) Toute forme bilinéaire alternée est antisymétrique.*

b) Si la caractéristique du corps K est différente de 2, on a la réciproque : toute forme bilinéaire antisymétrique est alternée.

c) Si la caractéristique du corps K est différente de 2, toute forme bilinéaire $b : E \times E \to K$ se décompose de manière unique sous la forme $b = b_s + b_a$ où b_s est une forme bilinéaire symétrique et b_a est une forme bilinéaire alternée.

Démonstration. Soient E un K-espace vectoriel et $b : E \times E \to K$ une forme bilinéaire sur E.

a) Pour tout $x, y \in E$, on a $b(x + y, x + y) = b(x, x) + b(y, y) + b(x, y) + b(y, x)$. Si b est alternée, il vient $0 = b(x, y) + b(y, x)$.

b) Si b est antisymétrique, prenant $x = y$, il vient $b(x, x) = -b(x, x)$. Si la caractéristique de K n'est pas 2, il vient $b(x, x) = 0$.

c) **Unicité.** Si $b = b_s + b_a$, il vient $b(x, y) + b(y, x) = 2b_s(x, y)$ et $b(x, y) - b(y, x) = 2b_a(x, y)$, donc
$$b_s(x, y) = \frac{1}{2}(b(x, y) + b(y, x)) \text{ et } b_a(x, y) = \frac{1}{2}(b(x, y) - b(y, x)).$$

Existence. Il suffit de poser $b_s(x, y) = \frac{1}{2}(b(x, y) + b(y, x))$ et $b_a(x, y) = \frac{1}{2}(b(x, y) - b(y, x))$. On vérifie immédiatement que b_s est une forme bilinéaire symétrique, que b_a est une forme bilinéaire alternée et que l'on a $b = b_s + b_a$. □

9.3 Définition. Soient K un corps commutatif et E un K-espace vectoriel. On appelle *forme quadratique* sur E une application $q : E \to K$ telle qu'il existe une forme bilinéaire $b : E \times E \to K$ satisfaisant $q(x) = b(x, x)$ pour tout $x \in E$.

9.4 Proposition. *Soient K un corps commutatif* de caractéristique différente de 2*, E un K-espace vectoriel et q une forme quadratique sur E. Il existe une unique forme bilinéaire* symétrique $\varphi : E \times E \to K$ *satisfaisant $q(x) = \varphi(x, x)$ pour tout $x \in E$.*

Démonstration. Par définition, il existe une forme bilinéaire $b : E \times E \to K$ telle que pour tout $x \in E$ on ait $b(x, x) = q(x)$. Soit $\varphi : E \times E \to K$ une forme bilinéaire symétrique. Alors $\varphi(x, x) = q(x)$ pour tout $x \in E$, si et seulement si la forme bilinéaire $b - \varphi$ est alternée, c'est à dire si et seulement si $\varphi = b_s$ où $b = b_s + b_a$ est la décomposition de b de la proposition ci-dessus (*cf.* c) de la proposition 9.2). □

9.5 Définition. Soient K un corps commutatif *de caractéristique différente de* 2, E un K-espace vectoriel, q une forme quadratique sur E et $\varphi : E \times E \to K$ une forme bilinéaire symétrique. Si pour tout $x \in E$ on a $\varphi(x, x) = q(x)$ on dit que q est la *forme quadratique associée* à φ et que φ est la *forme polaire* de q.

9.6 Identités de polarisation. Soient K un corps commutatif *de caractéristique différente de* 2, E un K-espace vectoriel, q une forme quadratique sur E et $\varphi : E \times E \to K$ sa forme polaire. En développant $\varphi(x \pm y, x \pm y)$ on trouve les *identités de polarisation* :

$$\varphi(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y)) = \frac{1}{4}(q(x+y) - q(x-y)) \text{ pour tous } x, y \in E.$$

9.7 Définition. Soient K un corps commutatif, E un K-espace vectoriel de dimension finie et $B = (e_1, \ldots, e_n)$ une base de E. Soit b sur E. La *matrice de la forme bilinéaire* b dans la base B est la matrice $A = (a_{i,j})$ où $a_{i,j} = b(e_i, e_j)$. Si la caractéristique de K est différente de 2, on appelle *matrice d'une forme quadratique* dans la base B la matrice (dans la base B) de sa forme polaire.

Soient $x, y \in E$. Notons $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ et $Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ les vecteurs-colonnes formés des coordonnées de x et y dans la base B. Soit b une forme bilinéaire sur E et notons $A = (a_{i,j})$ sa matrice dans la base B. Par bilinéarité de b, on a $b(x,y) = \sum_{i,j} a_{i,j} x_i y_j = {}^tXAY$. Notons que la matrice A est symétrique (égale à sa transposée) si et seulement si la forme bilinéaire b est symétrique ; de même la matrice A est antisymétrique si et seulement si la forme bilinéaire b est antisymétrique.

Supposons que la caractéristique de K soit différente de 2. Si $A = (a_{i,j})$ est la matrice dans la base B d'une forme quadratique q, on a $q(x) = \sum_{i,j} a_{i,j} x_i x_j = \sum_i a_{i,i} x_i^2 + \sum_{i<j} 2a_{i,j} x_i x_j$.

9.8 Changement de base. Soient B_0, B deux bases de E et notons P la matrice de passage de B_0 à B. Soit $x, y \in E$; notons X_0, Y_0 (*resp.* X, Y) les vecteurs-colonne formés des composantes de x, y dans la base B_0 (*resp.* B). On a $X_0 = PX$ et $Y_0 = PY$. Donc si A_0 (*resp.* A) est la matrice d'une forme bilinéaire φ dans la base B_0 (*resp.* B), on a $\varphi(x,y) = {}^tXAY = {}^tX_0A_0Y_0$, d'où l'on tire $A = {}^tPA_0P$.

9.9 Matrices congruentes. Deux matrices carrées A, B d'ordre n sont dites *congruentes* s'il existe une matrice inversible $P \in GL_n(K)$ telle que $A = {}^tPBP$. Deux matrices symétriques A, B sont donc congruentes si et seulement si elles sont matrices d'une même forme quadratique sur un K-espace vectoriel E dans deux bases de E (on suppose que la caractéristique de K est différente de 2).

9.10 Définition. Soient K un corps commutatif, E un K-espace vectoriel de dimension finie et q une forme quadratique sur E. Un vecteur x de E est dit *isotrope* pour q si $q(x) = 0$. L'ensemble des vecteurs isotropes pour q s'appelle le *cône isotrope* de q.

9.1.2 Orthogonalité

Soient K un corps commutatif *de caractéristique différente de* 2, E un K-espace vectoriel et q une forme quadratique sur E. Notons φ sa forme polaire.

- On dit que deux éléments $x, y \in E$ sont *orthogonaux* pour q si $\varphi(x,y) = 0$. On dit qu'une famille $(x_i)_{i \in I}$ est *orthogonale* pour q si pour tout $i, j \in I$ avec $i \neq j$, on a $\varphi(x_i, x_j) = 0$.
- L'orthogonal pour q d'une partie A de E est son orthogonal pour la forme bilinéaire φ (*cf.* 6.29) : c'est l'ensemble $A^\perp = \{y \in E;\ \forall x \in A;\ \varphi(x,y) = 0\}$. C'est un sous-espace vectoriel de E.
- En particulier, l'ensemble $\{x \in E;\ \forall y \in E;\ \varphi(x,y) = 0\}$ est un sous-espace vectoriel de E (c'est l'orthogonal $E^\perp$ de E tout entier). On l'appelle *noyau* de q ou noyau de φ et on le note $\ker q$ ou $\ker \varphi$.
- On dit que la forme quadratique q est *non dégénérée* si $\ker q = \{0\}$. On dit aussi que la forme bilinéaire φ est non dégénérée.

9.11 Définition. Supposons que la dimension de E soit finie et soit q une forme quadratique sur E. On appelle *rang* de q et l'on note $\operatorname{rg} q$ la codimension de $\ker q$.

On a donc $\operatorname{rg} q = \dim E - \dim \ker q$.

Si φ est la forme polaire de q, le rang de q s'appelle aussi le rang de φ et se note aussi $\operatorname{rg} \varphi$.

Supposons que la dimension de E soit finie et soit B une base de E. Notons A la matrice de q dans la base B. Soit $x \in E$ et X le vecteur-colonne formé des coordonnées de x dans la base B. On a $x \in \ker q \iff AX = 0$. Il vient $\operatorname{rg} q = \operatorname{rg} A$.

9.12 Proposition. *Si E est de dimension finie et q est non dégénérée, pour toute forme linéaire $\ell \in E^*$, il existe un unique $x \in E$ tel que l'on ait $\ell(y) = \varphi(x, y)$ pour tout $y \in E$.*

Démonstration. L'application $L : E \to E^*$ qui à $x \in E$ associe la forme linéaire $y \mapsto \varphi(x, y)$ est injective puisque q est non dégénérée, donc bijective puisque $\dim E^* = \dim E$ (*cf.* 6.23). □

Nous utiliserons plus loin le résultat suivant

9.13 Lemme. *Soit F un sous-espace vectoriel de E de dimension finie tel que la restriction de q à F soit non dégénérée. Alors $E = F \oplus F^\perp$.*

Démonstration. Soit $x \in E$. Par la proposition 9.12 (appliquée à la restriction de q à F), il existe un unique $y \in F$ tel que pour tout $z \in F$ on ait $\varphi(x, z) = \varphi(y, z)$, *i.e.* tel que $x - y \in F^\perp$. □

9.1.3 Décomposition de Gauss

Dans toute cette partie on fixe un corps commutatif K *de caractéristique différente de* 2.

9.14 Théorème. *Soit q une forme quadratique sur un K-espace vectoriel de dimension finie E. Alors il existe une base de E orthogonale pour q.*

Démonstration. On raisonne par récurrence sur la dimension n de E.
- Si $n \leqslant 1$ toute base de E est orthogonale.
- Supposons le théorème démontré pour toute forme quadratique sur un K-espace de dimension $n-1$. Si q est nulle, il n'y a rien à démontrer : toute base de E est orthogonale. Sinon, il existe un vecteur $e \in E$ tel que $q(e) \neq 0$. La restriction de q à Ke est alors non dégénérée. Par le lemme 9.13, on a alors $E = Ke \oplus (Ke)^\perp$. D'après l'hypothèse de récurrence, la restriction de q à $(Ke)^\perp$ admet une base orthogonale $(e_1, \dots, e_{n-1})$. Posons $e_n = e$. La base $(e_1, \dots, e_n)$ de E est orthogonale. □

Soient E un K-espace vectoriel de dimension finie, q une forme quadratique sur E et $B = (e_1, \dots, e_n)$ une base de E. La base B est orthogonale pour q si et seulement si la matrice de q dans la base B est diagonale.

Supposons que la base $(e_1, \dots, e_n)$ soit orthogonale. Quitte à intervertir les éléments de la base, on peut supposer qu'il existe $r \in \{0, \dots, n\}$ tel que $q(e_i) \neq 0$ pour $i \leqslant r$ et $q(e_i) = 0$ pour $i > r$. Pour $x = \sum_{i=1}^{n} x_i e_i$ et $y = \sum_{i=1}^{n} y_i e_i$, on a $\varphi(x, y) = \sum_{i=1}^{r} q(e_i) x_i y_i$ et $q(x) = \sum_{i=1}^{r} q(e_i) x_i^2 = \sum_{i=1}^{r} q(e_i) e_i^*(x)^2$ où (e_i^*) désigne la base duale de $(e_1, \dots, e_n)$. Alors $x \in \ker q$ si et seulement si $e_i^*(x) = 0$ pour $i \leqslant r$, donc $(e_{r+1}, \dots, e_n)$ est une base de $\ker q$. En particulier $r = \operatorname{codim} \ker q$.

On a démontré :

9.15 Corollaire : Décomposition de Gauss. *Soit q une forme quadratique sur un K-espace vectoriel de dimension finie E. Alors il existe des formes linéaires* indépendantes *$\ell_1, \dots, \ell_r$ et des scalaires non nuls $a_1, \dots, a_r$ tels que $q(x) = \sum_{i=1}^{r} a_i \ell_i(x)^2$. On a $r = \operatorname{rg} q$.*

□

Méthode de Gauss. Donnons-nous une forme quadratique q sur un K-espace vectoriel de dimension finie E. Notons φ sa forme polaire

Notons r le rang de q. Si on trouve une base orthogonale $(f_1, \dots, f_n)$ vérifiant $q(f_i) \neq 0$ pour $i \leqslant r$ et $q(f_i) = 0$ pour $i > r$, on aura $q = \sum_{i=1}^{r} a_i (f_i^*)^2$, où l'on a posé $a_i = q(f_i)$. Remarquons que, pour tout i, les formes linéaires $a_i f_i^*$ et $x \mapsto \varphi(x, f_i)$ coïncident en $x = f_i$ et sont nulles pour $x = f_j$ pour $j \neq i$. Puisqu'elles coïncident sur la base (f_j), elles sont égales.

Partons d'une base quelconque $(e_1, \dots, e_n)$ de E.

- Si $q(e_1) \neq 0$, on va prendre $f_1 = e_1$, donc poser $\ell_1(x) = \dfrac{1}{q(e_1)}\varphi(x, e_1)$. Notons que le noyau de la forme quadratique $q_1 = q - q(e_1)\ell_1^2$ est $\ker q \oplus Ke_1$, donc $\operatorname{rg} q_1 = r - 1$ et q_1 est une combinaison linéaire des formes $e_i^* e_j^*$ pour $2 \leqslant i \leqslant j \leqslant n$, en d'autres termes, on aura une expression de la forme $q_1(\sum_{i=1}^{n} x_i e_i) = \sum_{2 \leqslant i \leqslant j \leqslant n} b_{i,j} x_i x_j$.
  On aura donc à « réduire » une forme quadratique avec une variable de moins.
- Plus généralement, s'il existe k tel que $q(e_k) \neq 0$, nous pourrons appliquer cette recette.
- Si tous les $q(e_k)$ sont nuls, mais q n'est pas nulle, quitte à intervertir les vecteurs de la base, on peut supposer que $\varphi(e_1, e_2) \neq 0$. La restriction de q à $F = Ke_1 \oplus Ke_2$ est non dégénérée. En trouvant une base orthogonale de F (par exemple $(e_1 + e_2, e_1 - e_2)$), il nous restera à « réduire » la forme q restreinte à $F^\perp$, qui est de rang $r - 2$ et qui ne fait intervenir que les variables $(x_3, \dots, x_n)$.

En pratique, notons $A = (a_{i,j})$ la matrice de q dans cette base. Pour $x = \sum_{i=1}^{n} x_i e_i$, on a donc $q(x) = \sum_{1 \leqslant i,j \leqslant n} a_{ij} x_i x_j$.

La méthode expliquée ci-dessus revient à construire pas à pas, les formes ℓ_i de la façon suivante :

a) Si $a_{11} \neq 0$ (*i.e.* $q(e_1) \neq 0$), on écrit

$$\begin{aligned} q(x) &= a_{11}x_1^2 + 2\sum_{i=2}^{n} a_{1i}x_1x_i + \sum_{2 \leqslant i,j \leqslant n} a_{ij}x_ix_j \\ &= a_{11}\big(x_1 + \sum_{i=2}^{n} \frac{a_{1i}}{a_{11}}x_i\big)^2 - \frac{1}{a_{11}}\big(\sum_{i=2}^{n} a_{1i}x_i\big)^2 + \sum_{2 \leqslant i,j \leqslant n} a_{ij}x_ix_j \\ &= a_{1,1}\ell_1(x)^2 + q'(x) \end{aligned}$$

où $\ell_1(x) = x_1 + \sum_{i=2}^{n} \dfrac{a_{1i}}{a_{11}}x_i$ et q_1 est une forme quadratique qui ne fait plus intervenir x_1, *i.e.* telle que $e_1 \in \ker(q_1)$.

- Si l'un des coefficients diagonaux a_{ii} est non nul, on se ramène au premier cas en permutant les éléments de la base.

b) On a $a_{11} = a_{22} = 0$ mais $a_{12} \neq 0$

$$\begin{aligned} q(x) &= 2a_{12}x_1x_2 + 2x_1(\sum_{i=3}^{n} a_{1i}x_i) + 2x_2(\sum_{i=3}^{n} a_{2i}x_i) + \sum_{3 \leqslant i,j \leqslant n} a_{ij}x_ix_j \\ &= 2(a_{12}x_1 + \sum_{i=3}^{n} a_{2i}x_i)(x_2 + \frac{1}{a_{12}}\sum_{i=3}^{n} a_{1i}x_i) - \frac{2}{a_{12}}(\sum_{i=3}^{n} a_{2i}x_i)(\sum_{i=3}^{n} a_{1i}x_i) + \sum_{3 \leqslant i,j \leqslant n} a_{ij}x_ix_j. \\ &= \ell_1(x)\ell_2(x) + q_1(x) \\ &= \ell_1'(x)^2 - \ell_2'(x)^2 + q_1(x) \end{aligned}$$

où $\ell'_1(x) = \dfrac{\ell_1(x) + \ell_2(x)}{2}$ et $\ell'_2(x) = \dfrac{\ell_1(x) - \ell_2(x)}{2}$, et où q_1 est une forme quadratique qui ne fait plus intervenir x_1 et x_2, *i.e.* telle que $e_1, e_2 \in \ker(q_1)$.

9.1.4 Formes quadratiques positives - $K = \mathbb{R}$

On suppose ici que le corps de base K est le corps des réels.

9.16 Définition. Soit E un espace vectoriel réel. Une forme quadratique q sur E est dite *positive* si pour tout $x \in E$ on a $q(x) \geqslant 0$.

Une forme bilinéaire symétrique φ est dite positive si la forme quadratique associée $x \mapsto \varphi(x, x)$ est positive.

9.17 Inégalité de Cauchy-Schwarz. *Soit q une forme quadratique* positive *et φ sa forme polaire. Pour tout $x, y \in E$, on a $\varphi(x, y)^2 \leqslant q(x)q(y)$.*

Démonstration. Pour $t \in \mathbb{R}$ on a $q(tx + y) \geqslant 0$. Or $q(tx + y) = at^2 + 2bt + c$ avec $a = q(x)$, $b = \varphi(x, y)$ et $c = q(y)$. Le trinôme $at^2 + 2bt + c$ garde un signe constant, donc son discriminant $4(b^2 - ac)$ est négatif ou nul, *i.e.* $b^2 \leqslant ac$.

Notons que si $a = 0$, l'application affine $t \mapsto 2bt + c$ ne peut garder un signe constant que si elle est constante *i.e.* si $b = 0$. On trouve encore $b^2 \leqslant ac$. □

9.18 Corollaire. *Le cône isotrope d'une forme quadratique* positive *est égal à son noyau.*

Démonstration. Soient q une forme quadratique positive sur un espace vectoriel réel E et x un vecteur isotrope pour q. Notons φ la forme polaire de q. Pour tout $y \in E$, on a, d'après l'inégalité de Cauchy-Schwarz, $\varphi(x, y)^2 \leqslant q(x)q(y) = 0$. Donc $\varphi(x, y) = 0$. Cela prouve que $x \in \ker q$. □

En particulier, une forme quadratique positive non dégénérée n'admet pas de vecteur isotrope non nul : on dit qu'elle est *anisotrope* ou *définie*.

Rappelons une conséquence importante de l'inégalité de Cauchy-Schwarz.

9.19 Théorème. *Soit E un espace vectoriel réel de dimension finie muni d'une forme bilinéaire symétrique positive et non dégénérée $(x, y) \mapsto \langle x|y\rangle$. L'application $x \mapsto \|x\| = \sqrt{\langle x|x\rangle}$ est une norme sur E.*

Démonstration. Soient $x, y \in E$ et $\lambda \in \mathbb{R}$.
- D'après le corollaire précédent, on a $\|x\| = 0 \iff x = 0$;
- il est clair que $\|\lambda x\| = |\lambda|\|x\|$;
- On a, en utilisant l'inégalité de Cauchy-Schwarz

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2 + 2\langle x|y\rangle \leqslant \|x\|^2 + \|y\|^2 + 2\|x\|\|y\| = (\|x\| + \|y\|)^2,$$

d'où l'inégalité triangulaire. □

9.1.5 Signature ($K = \mathbb{R}$)

9.20 Théorème d'inertie de Sylvester. *Soient E un espace vectoriel* réel *de dimension finie et q une forme quadratique sur E. Donnons nous deux bases q-orthogonales $(e_1, \dots, e_n)$ et $(f_1, \dots, f_n)$. Le nombre des $i \in \{1, \dots, n\}$ tels que $q(e_i) > 0$ (resp. $q(e_i) < 0$, $q(e_i) = 0$) est égal au nombre des $i \in \{1, \dots, n\}$ tels que $q(f_i) > 0$ (resp. $q(f_i) < 0$, $q(f_i) = 0$).*

Démonstration. Notons E_+ (*resp.* E_-, E_0) le sous-espace vectoriel de E engendré par les e_j tels que $q(e_j) > 0$ (*resp.* $q(e_j) < 0$, $q(e_j) = 0$). De même, notons F_+ (*resp.* F_-, F_0) le sous-espace vectoriel de E engendré par les f_j tels que $q(f_j) > 0$ (*resp.* $q(f_j) < 0$, $q(f_j) = 0$). Remarquons que l'on a $E = E_+ \oplus E_- \oplus E_0 = F_+ \oplus F_- \oplus F_0$. Si $x \in E_+$ n'est pas nul, on a $q(x) > 0$; si $x \in F_- \oplus F_0$, on a $q(x) \leqslant 0$. Il vient $E_+ \cap (F_- \oplus F_0) = \{0\}$, donc $\dim E_+ \leqslant \operatorname{codim}(F_- \oplus F_0) = \dim F_+$.

De même, on a
- $F_+ \cap (E_- \oplus E_0) = \{0\}$, donc $\dim F_+ \leqslant \dim E_+$;
- $E_- \cap (F_+ \oplus F_0) = \{0\}$, donc $\dim E_- \leqslant \dim F_-$;
- $F_- \cap (E_+ \oplus E_0) = \{0\}$, donc $\dim F_- \leqslant \dim E_-$. □

Quelques remarques à propos de cette démonstration. Si $(e_1, \dots, e_n)$ est une base de E orthogonale pour q,

a) on a vu que les e_j tels que $q(e_j) = 0$ engendrent le noyau de q - autrement dit, avec les notations ci-dessus, on a $E_0 = F_0 = \ker q$;

b) cette démonstration démontre que si F est un sous-espace de E tel que la restriction de q à F soit non dégénérée et positive (*resp.* non dégénérée et négative), on a $\dim F \leqslant \dim E_+$ (*resp.* $\dim F \leqslant \dim E_-$).

9.21 Définition. Soient E un espace vectoriel réel de dimension finie et q une forme quadratique sur E. On appelle *signature* de q le couple (k, ℓ) où k et ℓ désignent respectivement le nombre des e_j tels que $q(e_j) > 0$ et $q(e_j) < 0$ pour une base de E orthogonale pour q.

Si q admet la décomposition de Gauss $q = \sum_{i=1}^{r} a_i f_i^2$ où $(f_1, \dots, f_r)$ est une famille indépendante de formes linéaires isur E, alors la signature de q est (k, ℓ) où k (*resp.* ℓ) est le nombre de $i \in \{1, \dots, r\}$ tels que $a_i > 0$ (*resp.* $a_i < 0$). En effet, la forme polaire de q est $\varphi : (x, y) \mapsto \sum_{i=1}^{r} a_i f_i(x) f_i(y)$, puisque φ est bilinéaire et symétrique et $q(x) = \varphi(x, x)$ pour tout $x \in E$. Complétons $(f_1, \dots, f_r)$ en une base $(f_1, \dots, f_n)$ de E^*. Cette base est la base duale d'une base $(e_1, \dots, e_n)$ de E ; on a

$$\varphi(e_j, e_{j'}) = \sum_{i=1}^{r} a_i \delta_{i,j} \delta_{i,j'} = \begin{cases} 0 & \text{si } j \neq j' \\ 0 & \text{si } j = j' > r \\ a_j & \text{si } j = j' \leqslant r. \end{cases}$$

Donc la base $(e_1, \dots, e_n)$ est orthogonale et k (*resp.* ℓ) est bien le nombre des j tels que $q(e_j) > 0$ (*resp.* $q(e_j) < 0$).

9.22 Conséquence : recherche d'extréma locaux. Soient U un ouvert d'un espace vectoriel réel E de dimension finie, a un point de U et $f : U \to \mathbb{R}$ une application. Rappelons que f est différentiable en a si et seulement si elle admet au voisinage de a un développement limité de la forme $f(x) = f(a) + \ell(x - a) + o(\|x - a\|)$ où ℓ est une forme linéaire sur E (la différentielle df_a de f en a). Si elle est deux fois différentiable en a, elle admet au voisinage de a un développement limité de la forme $f(x) = f(a) + \ell(x - a) + q(x - a) + o(\|x - a\|^2)$ où ℓ est une forme linéaire et q une forme quadratique sur E ($q/2$ est la différentielle seconde de f). On a :

a) Si f admet un extrémum local en a et est différentiable en a, alors $df_a = 0$.

b) Supposons que f admette au voisinage de a un développement limité d'ordre 2 de la forme $f(x) = f(a) + q(x-a) + o(\|x-a\|^2)$.
   - Si f présente en a un minimum (*resp.* maximum) local, alors la forme quadratique q est positive (*resp.* négative).
   - Si la forme quadratique q est définie positive (*resp.* définie négative), alors f présente en a un minimum (*resp.* maximum) local.

9.2 Formes quadratiques sur un espace vectoriel euclidien

9.2.1 Bases orthonormales

Soit E un espace vectoriel euclidien. Autrement dit E est un espace vectoriel réel de dimension finie muni d'une forme bilinéaire symétrique positive et non dégénérée $\langle\ |\ \rangle$. Rappelons que E possède une *base orthonormale* (on dit aussi *base orthonormée*), *i.e.* une base orthogonale (e_i) telle que, pour tout i on ait $\langle e_i|e_i\rangle = 1$. L'existence d'une base orthonormale résulte immédiatement de l'existence d'une base orthogonale (théorème 9.14). En effet, soit $(f_1, \dots, f_n)$ est une base orthogonale ; par positivité, on a $\langle f_i|f_i\rangle \in \mathbb{R}_+^*$; on pose alors $e_i = \langle f_i|f_i\rangle^{-1/2} f_i$ et la base $(e_1, \dots, e_n)$ est orthonormale.

Pour construire des bases orthonormales, on utilise le procédé d'orthonormalisation de Gram-Schmidt :

9.23 Orthonormalisation de Gram-Schmidt. *Soit $(x_1, ..., x_n)$ base de E. Il existe une unique base orthogonale $(f_1, ..., f_n)$ et une unique base orthonormale $(e_1, ..., e_n)$ de E telles que pour tout $k \in \{1, \dots, n\}$ on ait :*

a) $\mathrm{Vect}(x_1, \dots, x_k) = \mathrm{Vect}(f_1, \dots, f_k) = \mathrm{Vect}(e_1, \dots, e_k)$

b) $x_k - f_k \in \mathrm{Vect}(x_1, \dots, x_{k-1})$ *(en particulier $f_1 = x_1$) et* $\langle x_i|e_i\rangle \geqslant 0$ *(en fait $\langle x_i|e_i\rangle > 0$).*

On construit les f_i et les e_i de la manière suivante :

$$f_1 = x_1\,; \quad f_2 = x_2 - \frac{\langle f_1|x_2\rangle}{\langle f_1|f_1\rangle} f_1\,; \quad f_k = x_k - \sum_{j=1}^{k-1} \frac{\langle f_j|x_k\rangle}{\langle f_j|f_j\rangle} f_j\,; \quad e_k = \|f_k\|^{-1} f_k.$$

9.2.2 Endomorphismes et formes bilinéaires

9.24 Proposition. *Pour toute forme bilinéaire φ sur E, il existe un unique endomorphisme f de E tel que, pour tout $(x, y) \in E^2$ on ait $\varphi(x, y) = \langle f(x)|y\rangle$.*

Démonstration. Pour $x \in E$, notons ℓ_x l'application linéaire $y \mapsto \langle x|y\rangle$. Puisque $\langle\ |\ \rangle$ est non dégénérée, l'application linéaire $x \mapsto \ell_x$ est injective : c'est une bijection de E sur E^* puisque $\dim E = \dim E^*$.

Soient φ une forme bilinéaire sur E et $x \in E$. L'application $y \mapsto \varphi(x, y)$ est linéaire ; il existe donc un unique $z_x \in E$ tel que pour tout $y \in E$ on ait $\varphi(x, y) = \langle z_x|y\rangle$; on vérifie aisément que l'application $f : x \mapsto z_x$ est linéaire. □

9.25 Proposition. *Soient E un espace vectoriel euclidien et f un endomorphisme de E. Il existe un unique endomorphisme f^* de E tel que pour $x, y \in E$ on ait $\langle x|f(y)\rangle = \langle f^*(x)|y\rangle$.*

Démonstration. La forme $(x, y) \mapsto \langle x|f(y)\rangle$ est bilinéaire, donc s'écrit sous la forme $\langle f^*(x)|y\rangle$. □

9.26 Définition. Soient E un espace euclidien et f un endomorphisme de E. L'unique f^* de E tel que pour $x, y \in E$ on ait $\langle x|f(y)\rangle = \langle f^*(x)|y\rangle$ s'appelle l'*adjoint* de f. On dit que f est *symétrique* ou *autoadjoint* si $f^* = f$; on dit qu'il est *orthogonal* s'il est bijectif et $f^* = f^{-1}$; on dit qu'il est *normal* si $f^* \circ f = f \circ f^*$.

Remarquons que tout endomorphisme symétrique est normal et tout endomorphisme orthogonal est normal.

9.27 Proposition. *Soient E un espace euclidien et f un endomorphisme de E. La matrice de f^* dans une base orthonormale B de E est la transposée de la matrice de f dans la base B.*

Démonstration. Écrivons $B = (e_1, \dots, e_n)$. Notons $(a_{i,j})$ la matrice de f dans la base B. On a $f(e_j) = \sum_{i=1}^{n} a_{i,j} e_i$, donc $a_{i,j} = \langle f(e_j) | e_i \rangle$. La matrice de f^* dans la base B est donc $(c_{i,j})$ avec $c_{i,j} = \langle f^*(e_j) | e_i \rangle = \langle e_j | f(e_i) \rangle = a_{j,i}$. C'est la transposée de $(a_{i,j})$. □

9.28 Remarque. Soit q une forme quadratique d'un espace euclidien E et φ sa forme polaire. Il existe un unique endomorphisme f symétrique tel que, pour tout $x, y \in E$ on ait $\varphi(x, y) = \langle f(x) | y \rangle$. En particulier, $q(x) = \langle f(x) | x \rangle$.

L'application qui à un endomorphisme symétrique f associe la forme bilinéaire symétrique $(x, y) \mapsto \langle f(x) | y \rangle$ et l'application qui à une forme bilinéaire symétrique φ associe la forme quadratique $x \mapsto \varphi(x, x)$ sont bijectives, donc l'application qui à un endomorphisme symétrique f associe la forme quadratique $x \mapsto \langle f(x) | x \rangle$ est bijective.

Notons que si un endomorphisme symétrique f, une forme bilinéaire symétrique φ et une forme quadratique q se correspondent à travers ces bijections, on a $\ker f = \ker \varphi = \ker q$, donc $\operatorname{rg} f = \operatorname{rg} \varphi = \operatorname{rg} q$.

9.2.3 Diagonalisation simultanée

9.29 Théorème. *Soient E un espace vectoriel euclidien et q une forme quadratique sur E. Il existe une base orthonormale de E qui soit orthogonale pour q.*

Démonstration. On raisonne par récurrence sur la dimension n de E.

- Si $n = 1$, toute base est orthogonale pour toute forme quadratique !
- Supposons $n \geqslant 2$ et le résultat démontré pour toute forme bilinéaire symétrique d'un espace euclidien de dimension $n - 1$.
  Soit S la sphère unité de E. C'est une partie compacte de E. L'application continue q atteint son maximum en un vecteur $e_1 \in S$. Posons $\lambda = q(e_1)$ et $q_1(x) = \lambda \langle x | x \rangle - q(x)$. La forme polaire φ_1 de q_1 est donnée par $\varphi_1(x, y) = \lambda \langle x | y \rangle - \varphi(x, y)$ où φ est la forme polaire de q. Notons enfin H l'orthogonal de e_1 pour le produit scalaire de E.
  Par définition de e_1, la forme q_1 est positive et e_1 est isotrope pour q_1. Il appartient donc au noyau de q_1 : pour tout $y \in E$ on a $\varphi_1(e_1, y) = 0$, soit $\varphi(e_1, y) = \lambda \langle e_1 | y \rangle$. En particulier, pour $y \in H$ on trouve $\varphi(e_1, y) = 0$.
  Par l'hypothèse de récurrence, il existe une base orthonormale $(e_2, \dots, e_n)$ de H qui soit orthogonale pour la restriction de q à H. La base $(e_1, \dots, e_n)$ convient. □

On peut reformuler le théorème de façon plus abstraite :

9.30 Corollaire : Diagonalisation simultanée « abstraite ». *Soient E un espace vectoriel réel de dimension finie et q_1, q_2 deux formes quadratiques avec q_1 définie positive. Il existe une base orthonormale pour q_1 qui soit orthogonale pour q_2.*

Démonstration. Muni de la forme quadratique q_1, E est un espace euclidien. On peut donc appliquer directement le théorème. □

9.2.4 Diagonalisation des endomorphismes symétriques

Soit f un endomorphisme symétrique de E ; posons $\varphi(x,y) = \langle f(x)|y\rangle$. Par la diagonalisation simultanée, il existe une base orthonormale $(e_1,\dots,e_n)$ qui soit orthogonale pour φ. On a donc $\langle f(e_i)|e_j\rangle = 0$ pour $i \neq j$, donc la matrice de f est diagonale dans la base $(e_1,\dots,e_n)$. On a donc :

9.31 Théorème. *Tout endomorphisme autoadjoint d'un espace euclidien se diagonalise dans une base orthonormale.*

□

Nous trouverons en exercice (9.13) une généralisation de ce théorème pour les endomorphismes normaux.

Donnons une autre démonstration de ce théorème. Nous allons raisonner par récurrence. Notons P_n la propriété : Tout endomorphisme autoadjoint d'un espace euclidien de dimension n se diagonalise dans une base orthonormale.

Soit donc T un endomorphisme autoadjoint d'un espace euclidien de dimension n.

Pour $n = 1$, il n'y a rien à démontrer : tout endomorphisme est diagonal dans toute base !

Supposons donc que $n \geqslant 2$ et que P_{n-1} soit vraie.

Nous utilisons le résultat suivant :

9.32 Lemme. *Soit F un sous-espace de E invariant par T. Alors :*
a) L'orthogonal $F^\perp$ de F est invariant par T.
b) La restriction de T à F et $F^\perp$ est auto-adjointe.

Démonstration. a) Pour $x \in F^\perp$ et $y \in F$, on a - puisque T est autoadjoint $\langle T(x)|y\rangle = \langle x|T(y)\rangle = 0$ puisque $y \in F$ et F est invariant. Cela prouve que $T(x)$ est orthogonal à tout $y \in F$: donc $T(x) \in F^\perp$.

b) Pour $x, y \in E$ on a $\langle T(x)|y\rangle = \langle x|T(y)\rangle$. Cela est donc vrai si $x, y \in F$, ou $x, y \in F^\perp$. □

Pour finir la démonstration du théorème par récurrence, il suffit de démontrer que tout endomorphisme autoadjoint d'un espace vectoriel euclidien non nul possède un vecteur propre e_1 que l'on peut supposer de norme 1. Nous poserons alors $F = \mathbb{R}e_1$. Par l'hypothèse de récurrence, la restriction de f à $F^\perp$ admet une base orthonormale $(e_2,\dots,e_n)$ de vecteurs propres. Alors la base $(e_1, e_2,\dots,e_n)$ est orthonormale et formée de vecteurs propres de T.

Pour $n = 2$, choisissons une base orthonormale (e_1, e_2) et écrivons la matrice de T dans cette base : $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$. Le polynôme caractéristique de A est $X^2 - (a+c)X + (ac - b^2)$ dont le discriminant est $(a+c)^2 - 4ac + 4b^2 = (a-c)^2 + 4b^2$. Il est positif ou nul, donc T possède un vecteur propre.

Pour finir, on utilise le résultat suivant :

9.33 Lemme. *Soient E un espace vectoriel réel non nul de dimension finie. Tout endomorphisme de E possède un sous-espace stable de dimension 1 ou un sous-espace stable de dimension 2.*

Démonstration. Soit u un endomorphisme de E. Notons $M \in \mathcal{M}_n(\mathbb{R})$ la matrice de u dans une base quelconque. La matrice M possède des valeurs propres dans $\mathbb{C}$. Il existe donc $\lambda = s + it \in \mathbb{C}$ (avec $s, t \in \mathbb{R}$) et un vecteur-colonne $Z \in \mathbb{C}^n$ non nul tel que $MZ = \lambda Z$. Écrivons $Z = X + iY$ où X et Y sont des vecteurs-colonne réels. On a $M(X + iY) = (s + it)(X + iY)$, soit $MX = sX - tY$ et $MY = tX + sY$. Cela prouve que le sous-espace F engendré par les vecteurs x et y de composantes X et Y est stable par u. Comme $Z \neq 0$ ce sous-espace F n'est pas nul. Comme il est engendré par x, y, on a $\dim F \leqslant 2$. □

9.34 Interprétation matricielle. *Si A est une matrice symétrique (réelle), il existe une matrice orthogonale U et une matrice diagonale D telles que $A = U^{-1}DU$.*

9.2.5 Conséquences géométriques : quadriques

Généralités sur les quadriques : E est un K espace vectoriel

a) Définition des quadriques :
Une quadrique est un sous-ensemble D de l'espace E admettant une équation du type $\psi(x) = 0$ où $\psi(x) = q(x) + \ell(x) + c$, avec q forme quadratique, ℓ forme linéaire et $c \in \mathbb{R}$.

b) Quadriques non dégénérées.
Posons $K = \ker q \cap \ker \ell$ et soit $p : E \to E$ un projecteur de noyau K.
Pour $x \in E$ et $y \in K$, on a $\psi(x + y) = \psi(x)$ de sorte que $\psi = \psi \circ p$. Dans ce cas notre quadrique s'écrit $D_1 \times K$ où D_1 est une quadrique d'un supplémentaire de K (l'image de p).
On dira que la quadrique est *non dégénérée* si $K = \{0\}$. Comme $\dim \ker \ell \geqslant n - 1$, cela impose $\dim \ker q \leqslant 1$.

c) Centre d'une quadrique non dégénérée.
On cherche les symétries centrales laissant invariante (l'équation d') une quadrique.
Soit $a \in E$. On devra avoir $\psi(a - x) = \psi(x + a)$. Or $q(x + a) - q(a - x) = 4\varphi(x, a)$ où φ est la forme polaire de q. On a donc $\psi(a + x) - \psi(a - x) = 4\varphi(x, a) + 2\ell(x)$.
Si q est non dégénérée, il existe un unique a tel que pour tout x on ait $\varphi(x, a) = -\dfrac{1}{2}\ell(x)$.
Si q est dégénérée, prenant $x \in \ker q$ non nul (et donc $x \notin \ker \ell$ car notre quadrique est non dégénérée) on ne peut avoir $4\varphi(x, a) + 2\ell(x) = 0$.

Symétries d'une quadrique, axes principaux d'une quadrique à centre *(juste quelques mots...)*

En se plaçant au centre d'une quadrique à centre, l'équation devient $\psi(x) = q(x) + c = 0$. On dira alors qu'elle est *propre* si elle est non dégénérée et ne contient pas son centre, *i.e.* si q est non dégénérée et $c \neq 0$. L'équation devient donc $q(x) = 1$ avec q non dégénérée (on a divisé par c).

On suppose de plus que E est un espace affine euclidien (donc $K = \mathbb{R}$). L'équation d'une quadrique à centre propre (en prenant pour origine le centre) est $\langle x | f(x) \rangle = 1$ où f est un endomorphisme symétrique inversible de $\overrightarrow{E}$.

Les droites propres de f passant par le centre de la conique s'appellent les *axes principaux* de notre quadrique.

En diagonalisant, l'équation s'écrira $\displaystyle\sum_{i=1}^{k} \frac{x_i^2}{a_i^2} - \sum_{i=k+1}^{n} \frac{x_i^2}{a_i^2} = 1$ (avec $k \geqslant 1$ si notre quadrique n'est pas vide).

Pour $k = n$, notre quadrique est un ellipsoïde de *demi axes principaux* a_i.

On peut chercher les symétries de notre quadrique, *i.e.* les isométries g de l'espace la laissant invariante. Une telle isométrie fixera nécessairement le centre et on devra avoir $q \circ \vec{g} = q$, soit $\vec{g}^* \circ f \circ \vec{g} = f$, soit encore $\vec{g} \circ f = f \circ \vec{g}$. Si toutes les valeurs propres de f sont distinctes, $\vec{g}$ devra être diagonale, et comme c'est une isométrie, ses valeurs diagonales sont des ± 1.

Dans le cas général, g devra fixer les espaces propres de f. Sa matrice sera donc diagonale par blocs avec des blocs qui représentent des isométries des espaces propres de f. On peut déjà remarquer que s'il existe des isométries fixant q qui ne sont pas d'ordre 2, alors f a nécessairement des valeurs propres multiples (voir l'exercice 9.5).

9.3 Exercices

9.1 Exercice. Soit K un corps commutatif de caractéristique différente de 2. Soient E un K-espace vectoriel, q une forme quadratique sur E et $(e_1, \ldots, e_n)$ une base de E orthogonale pour q.

1. Soit $i \in \{1, \ldots, n\}$ tel que e_i soit isotrope. Démontrer que $e_i \in \ker q$.
2. Posons $J = \{j \in \{1, \ldots, n\};\ e_j \text{ isotrope}\}$. Démontrer que $(e_j)_{j \in J}$ est une base de $\ker q$.

9.2 Exercice. Quelle est la dimension de l'espace vectoriel des formes quadratiques sur K^n ?

9.3 Exercice. Notons Q l'espace vectoriel des formes quadratiques sur $\mathbb{R}^n$ et S la sphère unité de l'espace euclidien $\mathbb{R}^n$.

1. Démontrer que l'application $N : q \mapsto \sup\{|q(x)|;\ x \in S\}$ est une norme sur Q.
2. Démontrer que les formes quadratiques non dégénérées sur $\mathbb{R}^n$ forment un ouvert Q^* dense dans Q.
3. Démontrer que les formes quadratiques signature $(p, n-p)$ forment un ouvert dans Q.
4. Quelles sont les composantes connexes de Q^* ?

9.4 Exercice. Soit E un espace vectoriel réel de dimension finie n et q une forme quadratique non dégénérée sur E.

1. Notons (r, s) la signature de q. Quelles sont les signatures possibles des restrictions de q à des hyperplans de E ?
2. On se donne une suite $(E_k)_{0 \leqslant k \leqslant n}$ de sous-espaces de E tels que $\dim E_k = k$ et $E_k \subset E_{k+1}$. On suppose que pour tout k la restriction q_k de q à E_k est non dégénérée.
   a) Démontrer qu'il existe une base orthogonale $(e_1, \ldots, e_n)$ de E telle que pour $k \in \{1, \ldots, n\}$, les vecteurs $(e_1, \ldots, e_k)$ forment une base de E_k.
   b) Notons A_k la matrice de q_k dans une base de E_k. Démontrer que la signature de q est $(n-\ell, \ell)$ où ℓ est le nombre de changements de signes dans la suite $(\det A_k)_{0 \leqslant k \leqslant n}$ (le signe de $\det A_k$ ne dépend pas de la base choisie). - (Voir aussi exerc. **??**).

9.5 Exercice. Nature de la quadrique d'équation $xy + yz + zx + 1 = 0$.

9.6 Exercice. Démontrer que l'application $M \mapsto Tr(M^2)$ est une forme quadratique non dégénérée sur $M_n(\mathbb{R})$. Quelle est sa signature ?

9.7 Exercice. Soit q une forme quadratique sur un espace vectoriel réel. Quelle est en fonction de la signature de q la plus grande dimension de sous-espace totalement isotrope de E (*i.e.* sous-espace vectoriel de E formé de vecteurs isotropes) ?

9.8 Exercice. Soient K un corps de caractéristique différente de 2, E un K-espace vectoriel de dimension finie et q une forme quadratique sur E.

1. Soit F un sous-espace vectoriel de E démontrer que $\dim F^\perp = \dim E - \dim F + \dim(F \cap \ker q)$.
2. Plus généralement, soient F et G deux sous-espaces de E. Démontrer que

$$\dim G - \dim(F^\perp \cap G) = \dim F - \dim(F \cap G^\perp).$$

9.9 Exercice. Soient K un corps de caractéristique différente de 2, E un K-espace vectoriel de dimension finie et q une forme quadratique sur E.

Un sous-espace F de E est dit *totalement isotrope* si la restriction de q à F est nulle. Un sous-espace F de E est dit *totalement isotrope maximal* s'il est totalement isotrope et s'il n'y a pas de sous-espace de E totalement isotrope contenant F et distinct de F. Le but de cet exercice est de démontrer que tous les sous-espaces totalement isotropes maximaux de E ont même dimension.

Fixons un sous-espace totalement isotrope maximal F.

1. Soit $x \in F^\perp$ un vecteur isotrope. Démonter que $x \in F$.
2. Soit G un autre sous-espace totalement isotrope maximal. Démontrer que $F^\perp \cap G = F \cap G$.
3. Conclure à l'aide de l'exercice 9.8.

9.10 Exercice. Théorème de Witt. Soient E un espace vectoriel de dimension finie sur un corps K de caractéristique $\neq 2$ et q une forme quadratique non dégénérée sur E. Notons $O(q)$ le groupe orthogonal de q, c'est à dire l'ensemble des applications linéaires bijectives $\tau : E \to E$ telles que $q \circ \tau = q$.

Le but de cet exercice est d'établir le théorème de Witt qui affirme que pour tout sous-espace vectoriel F de E toute application linéaire injective $\sigma : F \to E$ satisfaisant $q \circ f(x) = q(x)$ pour tout $x \in F$, il existe $\tau \in O(q)$ qui prolonge σ.

On procède par récurrence sur $\dim E$.

1. Examiner le cas où $\dim E = 1$ ou $\dim F = 0$.

   On suppose à présent que $\dim E = n \geqslant 2$, que $\dim F \neq 0$ et le résultat établi pour un espace vectoriel de dimension $n-1$.
2. On suppose qu'il existe $x \in F$ tel que $q(x) \neq 0$ et $\sigma(x) = x$. Posons $E_1 = x^\perp$, $F_1 = F \cap E_1$.
   a) Démontrer que $\sigma(F_1) \subset E_1$.
   b) Démontrer qu'il existe $\tau \in O(q)$ qui prolonge σ.
3. On suppose que F n'est pas totalement isotrope. Soit $x \in F$ tel que $q(x) \neq 0$ et posons $y = \sigma(x)$.
   a) Calculer $q(x+y)+q(x-y)$ et en déduire que $x+y$ et $x-y$ ne sont pas tous deux isotropes.
   b) Démontrer qu'il existe un sous-espace $G \subset E$ tel que l'on ait $E = G \oplus G^\perp$, $x+y \in G$ et $x-y \in G^\perp$
   c) En déduire qu'il existe $\tau_1 \in O(q)$ telle que $\tau_1(x) = y$.
   d) Conclure dans ce cas.
4. On suppose que F est totalement isotrope. Notons φ la forme polaire de q. Soit ℓ une forme linéaire non nulle sur F.
   a) Démontrer qu'il existe $x \in E$ tel que, pour tout $y \in F$, on ait $\ell(y) = \varphi(x, y)$.
   b) Démontrer que l'élément x de la question précédente peut être choisi isotrope.
   c) Démontrer que l'on peut prolonger σ en une application linéaire injective $\overline{\sigma} : F \oplus Kx \to E$ telle que l'on ait encore $q(\overline{\sigma}(z)) = q(z)$ pour tout $z \in F \oplus Kx$.
   d) Conclure.

9.11 Exercice. On note $M_+(n, \mathbb{R})$ des matrices carrées d'ordre n symétriques positives. Démontrer que l'application $T \mapsto T^2$ est bijective de $M_+(n, \mathbb{R})$ dans lui même.

9.12 Exercice. (Décomposition d'Iwasawa). Démontrer que pour tout $A \in GL_n(\mathbb{K})$ il existe une unique matrice U orthogonale (unitaire) et une unique matrice triangulaire supérieure T dont les coefficients diagonaux sont (réels et) strictement positifs telles que $A = UT$.

9.13 Exercice. ***Réduction des endomorphismes normaux.*** Une matrice $M \in M_n(\mathbb{R})$ est dite *normale* si ${}^tMM = M{}^tM$. En particulier, les matrices symétriques, les matrices antisymétriques et les matrices orthogonales sont normales. Soit M une matrice normale.

1. On suppose que $n = 2$. Démontrer que M est soit symétrique soit de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ $(a, b \in \mathbb{R})$ - (*i.e.* une matrice de similitude directe).
2. On suppose que M se décompose par blocs sous la forme $M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ où A et C sont des matrices carrées. Démontrer que ${}^tAA = A{}^tA + B{}^tB$ et en déduire (à l'aide d'un calcul de trace) que $B = 0$, puis que A et C sont des matrices normales.
3. À l'aide du lemme 9.33 démontrer qu'il existe une matrice orthogonale U telle que ${}^tUMU$ s'écrive $M = \begin{pmatrix} D & 0 \\ 0 & D_1 \end{pmatrix}$ où $D = \mathrm{diag}(\lambda_i)$ est diagonale et $D_1 = \mathrm{diag}(S_i)$ est diagonale par blocs 2×2, les S_i étant des matrices de similitudes directes.
4. Rappelons qu'un endomorphisme u d'un espace euclidien E est dit *normal* si $uu^* = u^*u$. Énoncer un théorème de réduction des endomorphismes normaux. En déduire des théorèmes de réduction pour les endomorphismes orthogonaux et pour les endomorphismes antisymétriques.

10 Géométrie affine en dimension finie

10.1 Petit rappel sur les actions de groupes

10.1.1 Définitions

Rappelons pour commencer quelques définitions sur les actions de groupes.

10.1 Définition. Soient G un groupe et X un ensemble. Notons e l'élément neutre de G.

- Une *action* ou *opération* de G sur X est une application de $G \times X$ dans X notée $(g, x) \mapsto g.x$ (ou juste gx) telle que,

$$\forall x \in X,\ \forall g, h \in G \times G, \qquad (gh).x = g.(h.x) \quad \text{ et } e.x = x$$

  On appelle parfois *G-espace*, un ensemble muni d'une action d'un groupe G.
- On dit que l'action est *libre* ou que X est un *G-espace principal* si pour tout $x \in X$ et $g \in G$, on a $gx = x \iff g = e$;
- on dit que l'action est *transitive* si pour tout $(x, y) \in X^2$, il existe $g \in G$ tel que $gx = y$. Si $X \neq \emptyset$ on dit aussi que X est un *G-espace homogène.*

L'application $(g, x) \mapsto (gx, x)$ de $G \times X$ dans $X \times X$ est injective si et seulement si l'action est libre et surjective si et seulement si l'action est transitive.

Orbites. Une opération de G dans X donne lieu à une relation d'équivalence R sur X : pour $x, y \in X$, on a $x\,R\,y$ s'il existe $g \in G$ avec $a = g.b$. La classe d'équivalence d'un élément a est son *orbite* $G.a = \{g.a\,;\ g \in G\}$. L'ensemble quotient de cette relation d'équivalence - ensemble des orbites est noté $G\backslash X$. L'action est transitive, si et seulement s'il y a une seule orbite.

Orbites d'une permutation. Si σ est une permutation de X, autrement dit si $\sigma : X \to X$ est une bijection, on obtient une action du groupe $\mathbb{Z}$ dans X en posant $n.x = \sigma^n(x)$. On appelle *orbites de σ*, les orbites de X sous cette action de $\mathbb{Z}$.

Stabilisateurs. Soit $x \in X$. Le *stabilisateur* de x, est l'ensemble St_x des $g \in G$ tels que $g.x = x$. C'est un sous-groupe de G. Remarquons que les stabilisateurs de deux points de la même orbite sont conjugués : $h \in St_{g.x} \iff hgx = gx \iff (g^{-1}hg).x = x \iff g^{-1}hg \in St_x$.

Opération fidèle. Enfin, on dit que l'action est *fidèle* si pour tout $g \in G$ distinct de e, il existe $x \in X$ tel que $g.x \neq x$.

10.1.2 Digression : cas des groupes finis opérant sur un ensemble fini

Soit G un groupe fini opérant sur un ensemble fini X.

Opérations libres. Si l'action est libre, toutes les orbites ont même cardinal que G : on obtient $\operatorname{card} X = (\operatorname{card} G)\,(\operatorname{card} G\backslash X)$ ou $G\backslash X$ désigne le quotient d'équivalence de X par l'opération de G.

Un cas particulier important est le cas où l'on fait opérer sur un groupe G un sous-groupe H en posant $h.g = hg$. L'action est clairement libre et l'on en déduit la formule (théorème de Lagrange)

$$\boxed{\operatorname{card}(G) = \operatorname{card}(H).\operatorname{card}(G/H).}$$

Opérations transitives. On suppose que l'opération est transitive. Soit $a \in X$ et notons $H = St_a$ le stabilisateur de a, *i.e.* l'ensemble des $g \in G$ tels que $g.a = a$. C'est un sous-groupe de G. Pour $u, v \in G$, on a $u.a = v.a$ si et seulement si $(u^{-1}v).a = a$, *i.e.* si et seulement si $u^{-1}v \in H$. On en déduit une bijection $p : G/H \to X$ où G/H est le quotient de G par l'action (libre) $(h, g) \mapsto gh^{-1}$ de H sur G. Il vient $\operatorname{card} G = (\operatorname{card} H)(\operatorname{card} G/H) = (\operatorname{card} H)(\operatorname{card} X)$.

Formule des classes. Dans le cas général d'une action d'un groupe G sur X, en choisissant un point par orbite, on obtient une partie B de X qui rencontre chaque orbite en un point. On a

$$\boxed{\operatorname{card} X = \sum_{b\in B} \operatorname{card} G.b = \sum_{b\in B} \frac{\operatorname{card} G}{\operatorname{card} St_b}}$$

où $St_b = \{g \in G\,;\ g.b = b\}$ est le stabilisateur de b.

Formule de Burnside. Pour $g \in G$, notons $\mathrm{Fix}(g) = \{x \in X;\ g.x = x\}$. Calculons le nombre de points de $Y = \{(g,x) \in G \times X;\ gx = x\}$. En regroupant selon $g \in G$, on trouve $\operatorname{card} Y = \sum_{g\in G} \operatorname{card} \mathrm{Fix}(g)$. En regroupant selon $x \in X$, il vient $\operatorname{card} Y = \sum_{x\in X} \operatorname{card} St_x$. Regroupons encore les x en fonction des orbites de l'action. Choisissons pour cela une partie B de X qui rencontre chaque orbite en un point. Soit $b \in B$. Si $x \in G.b$ est dans l'orbite de b, les stabilisateurs de x et b sont conjugués, donc ont même nombre d'élements. Donc $\sum_{x\in G.b} \operatorname{card} St_x = (\operatorname{card} St_b)(\operatorname{card} G.b) = \operatorname{card} G$. Il vient $\operatorname{card} Y = \sum_{b\in B} \Big(\sum_{x\in G.b} \operatorname{card} St_x \Big) = (\operatorname{card} B)(\operatorname{card} G)$

On obtient ainsi la *formule de Burnside* :

$$\boxed{\operatorname{card} G\backslash X = \frac{1}{\operatorname{card} G} \sum_{g\in G} \operatorname{card} \mathrm{Fix}(g).}$$

10.2 Espaces affines, sous-espaces affines

Soit K un corps. Un espace affine est un espace vectoriel dont on aurait perdu le vecteur nul...

10.2 Définitions et conventions.

Espace affine. Un *espace affine* est un ensemble non vide E muni d'une action libre et transitive d'un espace vectoriel $\overrightarrow{E}$. L'espace vectoriel $\overrightarrow{E}$ s'appelle l'*espace vectoriel associé* à E, ou la *direction* de E. On dit que E est de dimension finie si $\overrightarrow{E}$ est de dimension finie et on pose $\dim E = \dim \overrightarrow{E}$. Une droite (*resp.* un plan) affine est un espace affine de dimension 1 (*resp.* 2).

Translations. L'action d'un vecteur $\vec{u} \in \overrightarrow{E}$ sur un point A de E se note $A+\vec{u}$ ou $T_{\vec{u}}(A)$. L'application $T_{\vec{u}}$ s'appelle la *translation* de vecteur $\vec{u}$. On a bien sûr $T_{\vec{u}} \circ T_{\vec{v}} = T_{\vec{u}+\vec{v}}$.

Notation $\overrightarrow{AB}$. Si $A, B \in E$, l'unique élément $\vec{u}$ de $\overrightarrow{E}$ tel que $A + \vec{u} = B$ se note $\overrightarrow{AB}$.

Relation de Chasles. Pour $A, B, C \in E$, on a $\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}$, $\overrightarrow{AA} = \overrightarrow{0}$.

Parallélogramme. Pour A, B, C, D, on a $\overrightarrow{AB} = \overrightarrow{DC}$ si et seulement si $\overrightarrow{AD} = \overrightarrow{BC}$. On dit alors que A, B, C, D est un *parallélogramme.*

Sous-espace affine. Soit E un espace affine ; notons $\overrightarrow{E}$ sa direction. Soit $\overrightarrow{F}$ un sous-espace vectoriel de $\overrightarrow{E}$. On appelle *sous-espace affine* de direction $\overrightarrow{F}$ une orbite de l'action de $\overrightarrow{F}$ dans E ; c'est alors un espace affine de direction $\overrightarrow{F}$. Un hyperplan affine est un sous-espace affine de co-dimension 1.

Il est d'usage de considérer que l'ensemble vide n'est pas un espace affine, mais que c'est un sous-espace affine dont tout sous-espace vectoriel est une direction. Avec cette convention, l'intersection d'une famille quelconque $(F_i)_{i\in I}$ de sous-espaces affines de E est un sous-espace affine de direction $\bigcap_{i\in I} \overrightarrow{F_i}$.

Sous-espace affine engendré. Soit E un espace affine et P une partie de E. Il existe un plus petit sous-espace affine de E contenant P (l'intersection de tous les sous-espaces affines de E contenant P).

Parallélisme. Deux sous-espaces affines ayant même direction sont dits *parallèles.* On dit encore qu'un sous-espace affine F est parallèle à un sous-espace affine G si la direction de F est contenue dans celle de G.

10.3 Applications affines

10.3 Définition. Soient E et F des espaces affines. Une application $f : E \to F$ est dite *affine* s'il existe une application linéaire $\vec{f} : \overrightarrow{E} \to \overrightarrow{F}$ telle que, pour tout $A, B \in E$ on ait $\overrightarrow{f(A)f(B)} = \vec{f}(\overrightarrow{AB})$. On dit que $\vec{f}$ est l'*application linéaire associée* à f.

10.4 Proposition. *Soient E et F des espaces affines et $f : E \to F$ une application. Pour $A \in E$, notons φ_A l'application $\varphi_A : \vec{u} \mapsto \overrightarrow{f(A)f(A+\vec{u})}$. On équivalence entre :*

(i) *Il existe $A \in E$ tel que l'application φ_A soit linéaire ;*

(ii) *pour tout $A \in E$ l'application φ_A soit linéaire ;*

(iii) *l'application f est affine - et dans ce cas, on a $\varphi_A = \vec{f}$ pour tout $A \in E$.*

L'image (*resp.* l'image réciproque) d'un sous-espace affine de E (*resp.* de F) par une application affine $f : E \to F$ est un sous-espace affine de F (*resp.* de E).

Soit $f : E \to E$ une application affine. Les *points fixes* de f sont les $A \in E$ tels que $f(A) = A$. L'ensemble des points fixes de f est un sous-espace affine de E. S'il n'est pas vide, sa direction est $\ker(\vec{f} - \mathrm{id}_{\overrightarrow{E}})$.

Une composée d'applications affines est affine ; la réciproque d'une application affine bijective est affine.

10.5 Exemples. Soit E un espace affine. Soient F un sous-espace affine non vide de E et $\overrightarrow{G}$ un sous-espace supplémentaire de $\overrightarrow{F}$.

Projecteurs. Pour $M \in E$ il existe un unique point $P \in F$ tel que $\overrightarrow{PM} \in \overrightarrow{G}$. L'application $f : M \mapsto P$ ainsi construite est affine. On l'appelle le *projecteur* ou *projection* sur F parallèlement à $\overrightarrow{G}$. On a $f \circ f = f$. Inversement, toute application affine idempotente est de cette forme.

Symétries. Soit $M \in E$; notons P le projeté de M sur F parallèlement à $\overrightarrow{G}$. Posons $M' = P + \overrightarrow{MP}$. L'application $g : M \mapsto M'$ ainsi construite est affine. On l'appelle la *symétrie* par rapport à F parallèlement à $\overrightarrow{G}$. On a $g \circ g = \mathrm{id}_E$. Inversement, (si la caractéristique de K n'est pas 2) toute application affine involutive est de cette forme.
Question. Que se passe-t-il en caractéristique 2 ?

10.4 Barycentres

Soit E un espace affine. Un *point pondéré* est un couple $(A, \lambda) \in E \times K$.

10.6 Proposition. *Soient $(A_i, \lambda_i)_{i \in I}$ une famille finie de points pondérés.*

a) Si $\sum_{i \in I} \lambda_i = 0$, le vecteur $\sum_{i \in I} \lambda_i \overrightarrow{MA_i}$ ne dépend pas de M. On le note $\sum_{i \in I} \lambda_i A_i$

b) On suppose que $\sum_{i \in I} \lambda_i \neq 0$. Pour $G \in E$, les conditions suivantes sont équivalentes :

(i) *On a $\sum_{i \in I} \lambda_i \overrightarrow{GA_i} = \overrightarrow{0}$.*

(ii) *Il existe $M \in E$ tel que $\sum_{i \in I} \lambda_i \overrightarrow{MA_i} = \Big(\sum_{i \in I} \lambda_i\Big) \overrightarrow{MG}$.*

(iii) *Pour tout* $M \in E$ *on a* $\sum_{i\in I} \lambda_i \overrightarrow{MA_i} = \Big(\sum_{i\in I} \lambda_i\Big)\overrightarrow{MG}$.

Il existe un unique point G *de* E *vérifiant ces conditions.*

10.7 Définition. Le point G défini dans la proposition précédente s'appelle le *barycentre* des « points pondérés » $((A_1, \lambda_1), \ldots, (A_n, \lambda_n))$.

Lorsque $\lambda_1 = \ldots = \lambda_n$, on dit que M est l'*isobarycentre* de $(A_1, \ldots, A_n)$.

10.8 Propriétés des barycentres. Soient $((A_1, \lambda_1), \ldots, (A_n, \lambda_n))$ des points pondérés. On suppose que $\sum_{i=1}^{n} \lambda_i \neq 0$. Notons G le barycentre de $((A_1, \lambda_1), \ldots, (A_n, \lambda_n))$.

Homogénéité. Pour $\lambda \in K^*$, le barycentre de $((A_1, \lambda\lambda_1), \ldots, (A_n, \lambda\lambda_n))$ est encore G. On peut ainsi se ramener au cas où $\sum_{i=1}^{n} \lambda_i = 1$. Dans ce cas, le barycentre de $((A_1, \lambda_1), \ldots, (A_n, \lambda_n))$ se note $\sum_{i=1}^{n} \lambda_i A_i$.

Commutativité des barycentres. Pour toute permutation σ de $\{1, \ldots, n\}$, G est le barycentre de $((A_{\sigma(1)}, \lambda_{\sigma(1)}), \ldots, (A_{\sigma(n)}, \lambda_{\sigma(n)}))$.

Associativité des barycentres. Soit k un entier compris entre 1 et $n-1$. Posons $\mu = \sum_{i=k+1}^{n} \lambda_i$, et supposons que $\mu \neq 0$. Notons G_k le barycentre de $((A_{k+1}, \lambda_{k+1}), \ldots, (A_n, \lambda_n))$. Alors le barycentre de $((A_1, \lambda_1), \ldots, (A_k, \lambda_k), (G_k, \mu))$ est G.

10.9 Proposition. *a) Une partie d'un espace affine est un sous-espace affine si et seulement si elle est* stable par barycentres.

b) Une application entre espaces affines est affine si et seulement si elle respecte les barycentres.

Soit E un espace affine. Une partie F de E est dite *stable par barycentres* si pour tous $A_1, \ldots, A_n \in F$ et $\lambda_1, \ldots, \lambda_n \in K$ tels que $\sum_{i=1}^{n} \lambda_i \neq 0$, le barycentre de $((A_1, \lambda_1), \ldots, (A_n, \lambda_n))$ appartient à F.

Soient E, F des espaces affines et $f : E \to F$ une application. On dit que f *respecte les barycentres* si pour tous $A_1, \ldots, A_n \in E$ et $\lambda_1, \ldots, \lambda_n \in K$ tels que $\sum_{i=1}^{n} \lambda_i \neq 0$, l'image par f du barycentre de $((A_1, \lambda_1), \ldots, (A_n, \lambda_n))$ est le barycentre de $((f(A_1), \lambda_1), \ldots, (f(A_n), \lambda_n))$.

10.10 Corollaire. *Le sous-espace affine engendré par une partie d'un espace affine est l'ensemble des barycentres de points de cette partie.*

Tout ce qui concerne les barycentres devient « évident » si on suppose que E est un espace vectoriel, *i.e.* si on choisit une origine. Reste que ce choix n'est pas « canonique ». On peut par contre toujours considérer E comme sous-espace affine d'un espace vectoriel $\overrightarrow{H}$. Dans ce cas, G est le barycentre de $((A_1, \lambda_1), \ldots, (A_n, \lambda_n))$ si $\left(\sum_{i\in I} \lambda_i\right) G = \sum_{i\in I} \lambda_i A_i$ (dans $\overrightarrow{H}$) - et lorsque $\sum_{i\in I} \lambda_i = 1$, on a bien $\sum_{i\in I} \lambda_i A_i = G$.

10.11 Proposition. *Soit* E *un espace affine.*

a) Il existe un espace vectoriel $\overrightarrow{H}$, et une application affine injective $\varphi : E \to \overrightarrow{H}$ telle que $\overrightarrow{0} \notin \varphi(E)$. Quitte à remplacer $\overrightarrow{H}$ par le sous-espace engendré par $\varphi(E)$, on peut supposer que $\varphi(E)$ engendre $\overrightarrow{H}$, ce que l'on suppose dans la suite.

b) Il existe une unique forme linéaire $f : \overrightarrow{H} \to K$ telle que $\varphi(E) = \{x \in \overrightarrow{H};\ f(x) = 1\}$. On a alors une identification canonique de $\overrightarrow{E}$ avec $\ker f$, qui envoie $\overrightarrow{AB}$ sur $\varphi(B) - \varphi(A)$.

c) Si on se donne $(\overrightarrow{H}_1, f_1, \varphi_1)$ et $(\overrightarrow{H}_2, f_2, \varphi_2)$ il existe un unique isomorphisme $u : \overrightarrow{H}_1 \to \overrightarrow{H}_2$ tel que $f_1 = f_2 \circ u$ et $\varphi_2 = u \circ \varphi_1$.

10.5 Repères

10.5.1 Repère cartésien

10.12 Définition. On appelle *repère cartésien* de E un $(n+1)$-uplet $(O, \vec{e}_1, \ldots, \vec{e}_n)$ où O est un point de E et $(\vec{e}_1, \ldots, \vec{e}_n)$ une base de $\overrightarrow{E}$.

Coordonnées cartésiennes. Lorsqu'on a fixé un repère cartésien $(O, \vec{e}_1, \ldots, \vec{e}_n)$ d'un espace affine E, on peut *repérer* un point M par ses *coordonnées cartésiennes*, *i.e.* les composantes du vecteur $\overrightarrow{OM}$ dans la base $(\vec{e}_1, \ldots, \vec{e}_n)$. En d'autres termes un repère cartésien nous donne un isomorphisme d'espaces affines de K^n sur E.

Changement de repère. Un changement de repère est donné par un changement d'origine (*i.e.* les coordonnées de la nouvelle origine dans l'ancien repère) et un changement de base (*i.e.* une matrice de passage).

Un repère cartésien sur E fixe, une base de l'espace vectoriel $\overrightarrow{E}$, donc, d'après 7.2.4 si $K = \mathbb{R}$:

- Une *orientation* :
- Une notion de *volume*, *i.e.* une mesure de Lebesgue.

Une transformation affine f de E
- préserve l'orientation si l'application linéaire tangente $\vec{f}$ a un déterminant positif, sinon elle la renverse ;
- multiplie les volumes par $|\det \vec{f}|$.

10.5.2 Repère affine

Equivalents affines de parties libres et génératrices : On a déjà vu l'équivalent des parties génératrices : une partie est (affinement) génératrice si le plus petit sous-espace affine qui la contient est E. Des points $(A_1, \ldots, A_n)$ sont dits *affinement indépendants* si pour tout $(\lambda_1, \ldots, \lambda_n) \in K^n$ les égalités $\sum \lambda_i = 0$ et $\sum \lambda_i A_i = \overrightarrow{0}$ impliquent $\lambda_1 = \ldots = \lambda_n = 0$.

10.13 Définition. Un *repère affine* ou *repère barycentrique* est une famille affinement indépendante et génératrice de points de E.

Soit $(A_0, A_1, \ldots, A_n)$ une famille de points de E. Cette famille est un repère affine si et seulement si la famille $(A_0, \overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_n})$ est un repère cartésien, *i.e.* si la famille $(\overrightarrow{A_0A_1}, \ldots, \overrightarrow{A_0A_n})$ est une base de $\overrightarrow{E}$.

Soit $(A_0, A_1, \ldots, A_n)$ un repère barycentrique de E. Pour tout point M de E il existe $(\lambda_0, \lambda_1, \ldots, \lambda_n) \in K^{n+1}$ tels que $\sum_{i=0}^{n} \lambda_i \neq 0$ et M soit le barycentre de $((A_0, \lambda_0), (A_1, \lambda_1), \ldots, (A_n, \lambda_n))$. Le $(n+1)$-uplet $(\lambda_0, \lambda_1, \ldots, \lambda_n)$ est unique à multiplication par un scalaire non nul près ; il s'appelle un système de *coordonnées barycentriques de* M dans le repère $(A_0, A_1, \ldots, A_n)$.

Commentaire. Qu'est-ce qu'un « repère » ? On veut que :

a) une application affine soit déterminée par ses valeurs dans le repère ;

b) « toutes les valeurs » soient possibles.

En particulier :

a) Une application affine qui fixe un repère est l'identité ;

b) étant donnés deux repères, il y a une (unique) application affine qui passe de l'un à l'autre.

10.6 Convexité

10.6.1 Généralités

Soit E un espace affine *réel* (ou complexe). Rappelons la Définition suivante.

10.14 Définition. Soit E un espace affine. Une partie C de E est dite *convexe* si pour tous $A_1, \ldots, A_n \in F$ et $t_1, \ldots, t_n \in \mathbb{R}_+$ non tous nuls, le barycentre de $((A_1, t_1), \ldots, (A_n, t_n))$ appartient à C.

10.15 Proposition. *Soit C une partie de E. La partie C est convexe dans E si et seulement si, pour tout $A, B \in C$ et tout $t \in [0,1]$, on a $(1-t)A + tB \in C$.*

Démonstration. Supposons que pour tout $A, B \in C$ et tout $t \in [0,1]$, on ait $(1-t)A + tB \in C$.
Nous devons démontrer que pour tout $n \in \mathbb{N}$, pour toute suite $A_1, \ldots, A_n$ d'éléments de C et toute suite $t_1, \ldots, t_n$ d'éléments de $\mathbb{R}_+$ tels que $\sum_{i=1}^{n} t_i = 1$, on a $\sum_{i=1}^{n} t_i A_i \in C$.
Démontrons cela par récurrence sur n. Cette propriété est vraie pour $n = 1$ (et $n = 2$). Si elle est vraie pour $n \geqslant 1$, soient $A_1, \ldots, A_n, A_{n+1}$ des points de C et $t_1, \ldots, t_n, t_{n+1} \in \mathbb{R}_+$ tels que $\sum_{i=1}^{n+1} t_i = 1$. Démontrons que $\sum_{i=1}^{n+1} t_i A_i \in C$; posons $t = \sum_{i=1}^{n} t_i = 1 - t_{n+1}$ et soient $s_1, \ldots, s_n \in \mathbb{R}_+$ tels que $\sum_{i=1}^{n} s_i = 1$ et $s_i t = t_i$. Par l'hypothèse de récurrence, on a $B = \sum_{i=1}^{n} s_i A_i \in C$; par le cas $n = 2$, on a aussi $\sum_{i=1}^{n+1} t_i A_i = tB + (1-t)A_{n+1} \in C$.
La réciproque est immédiate. □

Regroupons ci-dessous un certain nombre d'énoncés concernant la convexité.

Quelques propriétés de la convexité

a) Les parties convexes de l'espace $\mathbb{R}$ sont les intervalles.

Soit E un espace affine.

b) Tout sous-espace affine de E est convexe (dans E).

c) Une intersection de parties convexes de E est convexe. En particulier, si A est une partie quelconque de E, l'intersection de toutes les parties convexes de E contenant A est *le plus petit convexe de E contenant A*; cette partie s'appelle l'*enveloppe convexe* de A. C'est aussi l'ensemble $\mathrm{conv}(A)$ des combinaisons convexes d'éléments de A, c'est-à-dire des $x \in E$ tels qu'il existe $p \in \mathbb{N}$ des points $x_0, \dots, x_p \in A$ et $(t_0, \dots, t_p) \in \mathbb{R}_+$ tels que $\sum_{i=1}^{p} t_i = 1$ et $x = \sum_{i=1}^{p} t_i x_i$. En effet cet ensemble est convexe (par associativité des barycentres) et tout ensemble convexe contenant A contiendra toutes les combinaisons convexes d'éléments de A.

d) Soit F un espace affine. L'image d'une partie convexe de E par une application affine $E \to F$ est convexe dans F.

De même, l'image réciproque d'une partie convexe de F par une application affine $E \to F$ est convexe dans E.

10.6.2 Théorème de Caratheodory

10.16 Théorème de Caratheodory. *Soient E un espace affine de dimension n et A une partie de E. Pour tout $x \in \mathrm{conv}(A)$, il existe $x_0, \dots, x_n \in A$ tels que x soit barycentre à coefficients positifs ou nuls de $x_0, \dots, x_n$.*

Démonstration. Soit $x \in \mathrm{conv}(A)$. Il suffit de démontrer qu'il existe $p \leqslant n$ tel que l'on puisse trouver $x_0, \dots, x_p \in A$ et $t_0, \dots, t_p \in \mathbb{R}_+$ de somme 1 tels que $x = \sum_{j=0}^{p} t_j x_j$ (quitte à poser $x_k = x_0$ et $t_k = 0$ pour $p < k \leqslant n$).

Notons $\mathcal{F}$ l'ensemble des parties finies F de A telles que x soit dans l'enveloppe convexe de F. Par Définition de $\mathrm{conv}(A)$, x est barycentre d'un nombre fini de points de A, autrement dit $\mathcal{F} \neq \emptyset$. Parmi les éléments $F \in \mathcal{F}$, soit J une partie possédant le plus petit nombre d'éléments. Démontrons que J a au plus $n+1$ éléments.

Soit $F = \{x_0, \dots, x_p\} \in \mathcal{F}$. Écrivons $x = \sum_{j=0}^{p} t_j x_j$ où $(t_j) \in \mathbb{R}_+^{p+1}$.

Supposons que les points $(x_0, \dots, x_p)$ sont affinement liés et démontrons que $F \neq J$.

Il existe $(\lambda_0, \dots, \lambda_p) \in \mathbb{R}^{p+1}$, non tous nuls tels que $\sum_{j=0}^{p} \lambda_j = 0$ et $\sum_{j=0}^{p} \lambda_j x_j = \vec{0}$.

Alors, pour tout $s \in \mathbb{R}$, on a $x = \sum_{j=0}^{p} (t_j + s\lambda_j) x_j$.

Pour $s \in \mathbb{R}$, posons $\varphi(s) = \inf\{t_j + s\lambda_j,\ 0 \leqslant j \leqslant p\}$. L'application φ est continue, positive en 0, et puisque les λ_j ne sont pas tous nuls et leur somme est nulle, il existe j tel que $\lambda_j < 0$, donc $\lim_{s \to +\infty} \varphi(s) = -\infty$. Par le théorème des valeurs intermédiaires, il existe $u \in \mathbb{R}$ tel que $\varphi(u) = 0$. Posons $\mu_j = t_j + u\lambda_j$. Les μ_j sont positifs ou nuls et il existe j tel que $\mu_j = 0$. Alors $x = \sum_{j=0}^{p} \mu_j x_j$, donc $F' = \{x_j \in F;\ \mu_j \neq 0\} \in \mathcal{F}$. En particulier, F n'a pas un nombre minimum d'éléments, donc $F \neq J$.

On en déduit que J est affinement libre. En particulier $\mathrm{card}\, J \leqslant n+1$. □

10.17 Corollaire. *L'enveloppe convexe d'une partie compacte d'un espace affine de dimension finie est compacte.*

Démonstration. Soit A une partie compacte d'un espace affine E de dimension n.

Posons $\Sigma = \{(t_0, \dots, t_n) \in [0,1]^{n+1};\ \sum_{j=0}^{n} t_j = 1\}$. C'est un fermé de $[0,1]^{n+1}$, donc Σ est compact.

Posons $K = A^{n+1} \times \Sigma$; c'est un compact de (l'espace affine de dimension finie) $E^{n+1} \times \mathbb{R}^{n+1}$. Notons que nous pouvons choisir une origine dans E de sorte que E est un espace vectoriel de dimension finie. L'application $\varphi : A^{n+1} \times \Sigma \to E$ qui à $((x_0, \dots, x_n), (t_0, \dots, t_n))$ associe $\sum_{j=0}^{n} t_j x_j$ est continue. Son image est $\mathrm{conv}(A)$ d'après le théorème de Caratheodory. Elle est compacte. □

10.6.3 Fonctions convexes

10.18 Définition. Soient E un espace affine réel et C une partie convexe de E. Une application $f : C \to \mathbb{R}$ est dite *convexe* si son *surgraphe* $\{(x,u) \in E \times \mathbb{R}; f(x) \leqslant u\}$ est une partie convexe de $E \times \mathbb{R}$.

10.19 Proposition. *Soient E un espace affine réel, C une partie convexe de E et $f : C \to \mathbb{R}$ une application. Les conditions suivantes sont équivalentes :*

(i) *l'application f est convexe ;*

(ii) *pour tout $x, y \in C$ et tout $t \in [0,1]$, on a $f\big(tx + (1-t)y\big) \leqslant tf(x) + (1-t)f(y)$;*

(iii) *pour tout $n \in \mathbb{N}$, pour toute suite $x_1, \dots, x_n$ d'éléments de C et toute suite $t_1, \dots, t_n$ d'éléments de $\mathbb{R}_+$ tels que $\sum_{i=1}^{n} t_i = 1$, on a $f\Big(\sum_{i=1}^{n} t_i x_i\Big) \leqslant \sum_{i=1}^{n} t_i f(x_i)$.*

Démonstration. Le cas $n = 2$ dans (iii) est (ii) ; donc (iii)⇒(ii).

Notons S_f le surgraphe de f.

Démontrons que (ii)⇒(i). Soient (x,u) et (y,v) des éléments de S_f et $t \in [0,1]$; si (ii) est satisfaite, on a $f\big(tx + (1-t)y\big) \leqslant tf(x) + (1-t)f(y) \leqslant tu + (1-t)v$ puisque (x,u) et (y,v) sont dans S_f ; cela montre que $t(x,u) + (1-t)(y,v) \in S_f$; donc S_f est convexe d'après la prop. 10.15.

Enfin, soient $n \in \mathbb{N}$, $x_1, \dots, x_n$ une suite d'éléments de C et $t_1, \dots, t_n$ une suite d'éléments de $\mathbb{R}_+$ tels que $\sum_{i=1}^{n} t_i = 1$. Pour tout $i \in \{1, \dots, n\}$, on a $\big(x_i, f(x_i)\big) \in S_f$; si S_f est convexe, on a $\sum_{i=1}^{n} t_i \big(x_i, f(x_i)\big) \in S_f$, d'où l'on déduit l'assertion (i)⇒(iii). □

Soit E un espace affine réel.

- Une application affine $f : E \to \mathbb{R}$ est convexe (on a alors égalité dans la condition (ii) de la prop. 10.19).
- La somme de deux fonctions convexes est convexe.

10.7 Espaces affines euclidiens

10.20 Définition. Soit E un espace affine dont la direction est un espace vectoriel réel $\overrightarrow{E}$. Lorsque $\overrightarrow{E}$ est un espace vectoriel euclidien, on dit que E est un *espace affine euclidien.*

Soit E un espace affine euclidien de direction $\overrightarrow{E}$.

- La distance entre deux points A et B de E est $AB = \|\overrightarrow{AB}\|$.

- On dit qu'un repère cartésien $(O, \vec{e}_1, \ldots, \vec{e}_n)$ est orthonormé si la base $(\vec{e}_1, \ldots, \vec{e}_n)$ de $\overrightarrow{E}$ est orthonormée.

Projection orthogonale. Soit F un sous-espace affine (non vide) de E. Puisque $\overrightarrow{E} = \overrightarrow{F} \oplus \overrightarrow{F}^{\perp}$, on peut définir la projection sur F parallèlement à $\overrightarrow{F}^{\perp}$ (*cf.* exemple 10.5) : on l'appelle *projection orthogonale* sur F. Pour $A \in E$, le projeté orthogonal P de A sur F est l'unique point de F minimisant la distance : pour $M \in F$, puisque $\overrightarrow{PM} \in \overrightarrow{F}$ et $\overrightarrow{AP} \in \overrightarrow{F}^{\perp}$, on a $AM^2 = AP^2 + PM^2 \geqslant AP^2$.

Symétrie orthogonale. On définit de même la *symétrie orthogonale* par rapport à un sous-espace à F : c'est la symétrie par rapport à F parallèlement à $\overrightarrow{F}^{\perp}$. La symétrie orthogonale s_F par rapport à F est une isométrie : elle est bijective et pour $A, B \in E$, on a $s(A)s(B) = AB$.

Réflexion. Une *réflexion* est une symétrie orthogonale par rapport à un hyperplan.

Hyperplan médiateur. Soient A, B deux points distincts de E. L'ensemble $\{M \in E;\ AM = BM\}$ est un hyperplan affine : l'hyperplan médiateur de A et B : il passe par le milieu du segment $[A, B]$ et sa direction est $\overrightarrow{AB}^{\perp}$. La réflexion par rapport à cet hyperplan est l'unique réflexion s échangeant A et B.

Rappelons qu'une isométrie de E est une bijection de E sur E qui préserve les distances $f(A)f(B) = AB$ pour tout $A, B \in E$.

Il est bien sûr clair que l'identité est une isométrie, que la réciproque d'une isométrie est une isométrie et que la composée de deux isométries est une isométrie. Les isométries forment donc un sous-groupe du groupe des permutations de E, *i.e.* des bijections de E sur E.

10.21 Théorème. *Toute isométrie d'un espace affine euclidien de dimension n est composée d'au plus $n+1$ réflexions. En particulier, elle est affine.*

Nous allons en fait établir un résultat légèrement plus fort :
Soient $\mathcal{S}$ une partie de E contenant un répère affine $(A_1, A_2, \ldots, A_n, A_{n+1})$ et $f : \mathcal{S} \to E$ une application préservant les distances, i.e. telle que pour tout $M, N \in \mathcal{S}$ on a $f(M)f(N) = MN$. Alors, il existe une ismétrié affine $\sigma : E \to E$ composée d'au plus $n+1$ réflexions, telle que pour tout $M \in \mathcal{S}$ on ait $f(M) = \sigma(M)$.

Démonstration. Nous allons démontrer :

a) pour tout $k \in \{0, \ldots, n+1\}$, il existe une isométrie affine σ_k, produit d'au plus k réflexions telle que $\sigma_k \circ f(A_j) = A_j$ pour $1 \leqslant j \leqslant k$ (par convention l'identité est un produit de 0 réflexions) ;

b) Pour tout $M \in \mathcal{S}$ on a $\sigma_{n+1} \circ f(M) = M$.

Alors $\sigma = \sigma_{n+1}^{-1}$ convient.

a) On pose $\sigma_0 = \mathrm{id}_E$. Soit $k \in \{1, \ldots, n+1\}$ et supposons σ_{k-1} construite ; si $\sigma_{k-1} \circ f(A_k) = A_k$, on pose $\sigma_k = \sigma_{k-1}$. Sinon, notons τ_k la réflexion par rapport à l'hyperplan médiateur de A_k et $B_k = \sigma_{k-1} \circ f(A_k)$ et posons $\sigma_k = \tau_k \circ \sigma_{k-1}$. On a évidemment $\sigma_k \circ f(A_k) = A_k$. Pour $j < k$, comme $\sigma_{k-1} \circ f$ préserve les distances et fixe A_j, la distance entre A_j et A_k est égale à la distance entre leurs images A_j et B_k : en d'autres termes, A_j est dans l'hyperplan médiateur de A_k et B_k et est donc fixe par τ_k ; il en résulte que $\sigma_k \circ f(A_j) = A_j$.

b) Soit $M \in \mathcal{S}$ et posons $N = \sigma_{n+1} \circ f(M)$. Comme $\sigma_{n+1} \circ f$ préserve les distances et fixe tous les A_j, on a $MA_j = NA_j$. L'ensemble des points P tels que $MP = NP$ contient un repère, donc n'est pas contenu dans un hyperplan. Cela impose que $M = N$. □

10.22 Décomposition canonique. Soient E un espace affine euclidien et $f : E \to E$ une isométrie. Il existe une unique décomposition $f = T \circ g = g \circ T$ où T est une translation et g est une isométrie possédant des points fixes. Cette décomposition de f s'appelle sa *décomposition canonique.*

Pour voir cela, remarquons que si $T_{\vec{v}}$ et la translation de vecteur $\vec{v} \in \overrightarrow{E}$ et g est une application affine, alors $g \circ T_{\vec{v}} = T_{\vec{g}(\vec{v})} \circ g$; donc $T_{\vec{v}}$ et g commutent si et seulement si $\vec{g}(\vec{v}) = \vec{v}$. Remarquons aussi que si $f = T_{\vec{v}} \circ g$ alors $\vec{f} = \vec{g}$. Soit alors $A \in E$ et posons $\vec{w} = \overrightarrow{Af(A)}$.

Si g est telle que $f = T_{\vec{v}} \circ g$ et B est un point fixe de g, on a $g(A) = g(B) + \vec{f}(\overrightarrow{BA})$, donc $f(A) = B + \vec{f}(\overrightarrow{BA}) + \vec{v}$ et enfin $\vec{w} = \overrightarrow{AB} + \vec{f}(\overrightarrow{BA}) + \vec{v} = (\mathrm{id}_{\vec{E}} - \vec{f})(\overrightarrow{AB}) + \vec{v}$. Or $\ker(\mathrm{id}_{\vec{E}} - \vec{f}) = \mathrm{im}(\mathrm{id}_{\vec{E}} - \vec{f})^{\perp}$, donc le seul $\vec{v}$ possible est le projeté orthogonal de $\vec{w}$ sur $\ker(\mathrm{id}_{\vec{E}} - \vec{f})$, d'où l'unicité.
Inversement, il existe un unique $\vec{u} \in \mathrm{im}(\mathrm{id}_{\vec{E}} - \vec{f})$ et $\vec{v} \in \ker(\mathrm{id}_{\vec{E}} - \vec{f})$ tels que $\vec{w} = \vec{u} + \vec{v}$. Il existe alors B tel que $\vec{u} = (\mathrm{id}_{\vec{E}} - \vec{f})(\overrightarrow{AB})$ et l'on vérifie que B est bien point fixe de g.

Classifications des isométries du plan euclidien

$\dim(\ker(\vec{f} - \mathrm{id}))$	avec points fixes	sans points fixes
2	id_E	translation
1	symétrie par rapport à une droite	symétrie glissée
0	rotation	*impossible*

Classifications des isométries de l'espace euclidien (dimension 3)

$\dim(\ker(\vec{f} - \mathrm{id}))$	avec points fixes	sans points fixes
3	id_E	translation
2	symétrie par rapport à un plan (réflexion)	symétrie glissée
1	rotation	vissage
0	antirotation	*impossible*

10.23 Exemple : le groupe du cube. Notons G le groupe des isométries directes du cube, *i.e.* les éléments de $SO(3)$ qui laissent invariant le cube $[-1, 1]^3 \subset \mathbb{R}^3$. Le groupe G opère sur les 8 sommets les 12 arêtes et les 6 faces du cube. Quiconque a déjà vu un dé, sait que l'action sur les faces est transitive (toutes les faces du dé peuvent apparaître lorsqu'on lance le dé !). Le stabilisateur d'une face consiste en le groupe des quatre rotations d'axe perpendiculaire à cette face et d'angle $k\pi/2$. On en déduit que G a 24 éléments.

Le groupe du cube opère aussi sur les 4 grandes diagonales (qui passent par deux sommets opposés). On en déduit un homomorphisme de groupes f de G dans $\mathfrak{S}_4$. Nous allons démontrer que f est bijectif. Démontrons donc que f est injectif et surjectif - en sachant que, puisque G et $\mathfrak{S}_4$ ont même nombre d'éléments (24), il suffit de démontrer l'une de ces deux propriétés.

Injectivité. Soit $g \in G$. Si $g \in \ker f$, alors g fixe les 4 grandes diagonales ; en d'autres termes, leurs vecteurs directeurs $e_1 \pm e_2 \pm e_3$ sont propres pour g de valeur propre ± 1 - où (e_1, e_2, e_3) désigne la base canonique de $\mathbb{R}^3$. Les espaces propres étant en somme directe, on ne peut avoir deux espaces propres de dimension 2 ; trois quelconques de ces quatre vecteurs forment une base : on en déduit que $g = \pm\mathrm{id}_{\mathbb{R}^3}$; comme $-\mathrm{id}_{\mathbb{R}^3}$ n'est pas directe, il vient $g = \mathrm{id}_{\mathbb{R}^3}$.

Surjectivité. Notons g le demi tour d'axe $e_1 + e_2$. Les vecteurs $e_1 - e_2 \pm e_3$ sont orthogonaux à $e_1 + e_2$ donc sont des vecteurs propres de g pour la valeur propre -1 et g échange les deux vecteurs $e_1 + e_2 \pm e_3$. En d'autres termes, l'image de g est une transposition. Les 6 transpositions de $\mathfrak{S}_4$ sont ainsi obtenues comme images des demi-tours d'axes $e_i \pm e_j$ avec $1 \leqslant i < j \leqslant 3$, *i.e.* les stabilisateurs des arêtes. Comme ces transpositions engendrent $\mathfrak{S}_4$, on en déduit que f est surjective.

On trouvera en exercice (exerc. 10.14) quelques autres éléments sur le groupe du cube.

10.8 Exercices

10.1 Exercice. Soient E un espace affine de dimension finie et f une application affine de E dans E. Démontrer que si 1 n'est pas valeur propre de $\vec{f}$, alors f admet un unique point fixe.

10.2 Exercice. Soit E un espace affine de dimension $\geqslant 2$. Démontrer que toute bijection de E dans lui-même qui envoie toute droite sur une droite qui lui est parallèle est une homothétie-translation.

10.3 Exercice. Soient F, G des sous-espaces affines de E, A un point de F et B un point de G. Démontrer que l'on a $F \cap G \neq \emptyset$ si et seulement si $\overrightarrow{AB} \in \overrightarrow{F} + \overrightarrow{G}$.

10.4 Exercice. Dans un espace affine de dimension supérieure ou égale à 3, on considère un ensemble $\mathcal{D}$ de droites (affines). On suppose que deux droites de $\mathcal{D}$ ont un point commun. Démontrer que, soit toutes ces droites ont un point commun, soit elles sont coplanaires.

10.5 Exercice. Soit E un espace affine euclidien. Soient $A_1, \ldots, A_n$ des points de E et $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$. Pour $M \in E$ on pose $\varphi(M) = \sum_{i=1}^{n} \lambda_i \|A_i M\|^2$. Quels sont les extrema locaux de φ ?

10.6 Exercice. Soit C une partie convexe de E et $f : C \to \mathbb{R}$ une application convexe. Soit $a \in \mathbb{R}$. Démontrer que les ensembles $\{M \in E;\ f(M) < a\}$ et $\{M \in E;\ f(M) \leqslant a\}$ sont des parties convexes de E.

10.7 Exercice. *Coordonnées barycentriques des points remarquables du triangle.* Soit E un plan affine euclidien. Le but de cet exercice est de retrouver les coordonnées barycentriques des points remarquables d'un triangle non aplati ABC dans le repère affine (A, B, C). On note $\hat{A}, \hat{B}, \hat{C}$ les (mesures dans $]0, \pi[$ des) angles $\widehat{CAB}, \widehat{ABC}, \widehat{BCA}$ (on peut soit prendre des angles non orientés, ou mieux, on choisit l'orientation du plan de telle sorte que $\hat{A}, \hat{B}, \hat{C} \in]0, \pi[$).

1. Quelles sont les coordonnées barycentriques du centre de gravité G ?
2. a) Comment choisir un repère orthonormé de E pour lequel les affixes de A, B, C aient même module ?
   On fixe un tel repère.
   b) Démontrer qu'il existe $z \in \mathbb{C}^*$ et $s, t \in \mathbb{R}$ tels que s, t et $s + t$ ne sont pas multiples entiers de 2π tels que les affixes de A, B, C soient $z_A = z,\ z_B = ze^{is}$ et $z_C = ze^{-it}$. Exprimer s et t en fonction de $\hat{B}$ et $\hat{C}$.
   c) En remarquant que $(\sin t)e^{is} + (\sin s)e^{-it} = \sin(s+t)$, trouver des coordonnées barycentriques du centre du cercle circonscrit du triangle ABC.
3. a) Notons A' la projection orthogonale de A sur (BC). Calculer BA' et CA' en fonction de AA', $\hat{B}$ et $\hat{C}$. En déduire les coordonnées barycentriques de A' dans le repère affine (B, C) (discuter suivant le cas où les angles $\hat{B}$ et $\hat{C}$ sont aigus ou non).
   b) Démontrer qu'un système de coordonnées barycentriques de l'orthocentre H dans le repère (A, B, C) est $(\tan \hat{A}, \tan \hat{B}, \tan \hat{C})$.
4. On note I le centre du cercle inscrit à ABC.
   a) Démontrer que les vecteurs $\overrightarrow{AI}$ et $\dfrac{\overrightarrow{AB}}{AB} + \dfrac{\overrightarrow{AC}}{AC}$ sont colinéaires.
   b) Démontrer que (BC, AC, AB) est un système de coordonnées barycentriques de I dans le repère (A, B, C).

c) Démontrer que $(\sin\hat{A}, \sin\hat{B}, \sin\hat{C})$ est un système de coordonnées barycentriques de I dans le repère (A, B, C).

10.8 Exercice. *Variation autour du théorème de Pick (cet exercice m'a été suggéré par Gentiana Danila).* On se place dans l'espace euclidien orienté $\mathbb{R}^2$. Soient $A \in \mathbb{R}^2$ et $\vec{u}$ et $\vec{v}$ deux vecteurs indépendants. Notons $\mathcal{P}(A, \vec{u}, \vec{v})$ le parallélogramme de sommets $A, A+\vec{u}, A+\vec{v}, A+\vec{u}+\vec{v}$. On rappelle que l'aire algébrique du parallélogramme $\mathcal{P}(A, \vec{u}, \vec{v})$ est $\det(\vec{u}, \vec{v})$ (en particulier, cette aire est entière si $\vec{u}, \vec{v} \in \mathbb{Z}^2$).

Deux points distincts A et B de $\mathbb{Z}^2$ sont dits *visibles l'un de l'autre* si le segment $[A, B]$ ne contient aucun autre point de $\mathbb{Z}^2$ que A et B (on écrira $]A, B[\cap \mathbb{Z}^2 = \emptyset$).

1. Soit $\vec{u} = (a, a') \in \mathbb{Z}^2$ un vecteur non nul. Démontrer que $M \in \mathbb{Z}^2$ et $M + \vec{u}$ sont visibles l'un de l'autre si et seulement si a et a' sont premiers entre eux.
2. Soient $\vec{u} = (a, a')$ et $\vec{v} = (b, b')$ de $\mathbb{Z}^2$ indépendants et tels que $O+\vec{u}$ et $O+\vec{v}$ soient visibles depuis l'origine O.
   a) Construire $P \in \mathcal{M}_2(\mathbb{Z})$ telle que $\det P = 1$ et $\begin{pmatrix} a \\ a' \end{pmatrix} = P \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

   Soit $\begin{pmatrix} c \\ c' \end{pmatrix} = P^{-1} \begin{pmatrix} b \\ b' \end{pmatrix}$ et $\vec{w} = (c, c') \in \mathbb{Z}^2$. On pose aussi $\vec{i} = (1, 0) \in \mathbb{Z}^2$.

   b) Montrer que les parallélogrammes $\mathcal{P}(O, \vec{u}, \vec{v})$ et $\mathcal{P}(O, \vec{i}, \vec{w})$ ont même nombre de points de $\mathbb{Z}^2$ situés dans leur l'intérieur.

   c) En déduire que le nombre de points de $\mathbb{Z}^2$ situés à l'intérieur de $\mathcal{P}(O, \vec{u}, \vec{v})$ est $|\det(\vec{u}, \vec{v})| - 1$.
3. Si le point $A = (a, a') \in \mathbb{Z}^2$ est visible depuis O, décrire géométriquement les points $M = (m, m') \in \mathbb{Z}^2$ vérifiant la relation de Bézout $am' - ma' = \pm 1$.

10.9 Exercice. Soient E un espace affine euclidien et $f : E \to E$ une isométrie.

1. On suppose que l'ensemble $F = \{x \in E;\ f(x) = x\}$ des point fixes de f n'est pas vide. Démontrer que f est produit de $\dim E - \dim F$ réflexions et qu'on ne peut pas faire mieux.
2. On suppose que f n'a pas de points fixes et on pose $\overrightarrow{F} = \{\vec{v} \in \overrightarrow{E};\ \vec{f}(\vec{v}) = \vec{v}\}$ des points fixes de l'application linéaire $\vec{f}$ associée à f. Démontrer que f est produit de $\dim \overrightarrow{E} - \dim \overrightarrow{F} + 2$ réflexions et qu'on ne peut pas faire mieux.

10.10 Exercice. Soient E un espace affine et $f : E \to E$ une application affine. Soit $A \in E$. Démontrer qu'il existe $\vec{v}$ tel que l'on ait $T_{\vec{v}} \circ f = f \circ T_{\vec{v}}$ et $f \circ T_{\vec{v}}$ possède des points fixes si et seulement si $\overrightarrow{Af(A)} \in \ker(\mathrm{id}_{\vec{E}} - \vec{f}) + \mathrm{im}(\mathrm{id}_{\vec{E}} - \vec{f})$ et qu'on a unicité de ce vecteur si et seulement si $\ker(\mathrm{id}_{\vec{E}} - \vec{f}) \cap \mathrm{im}(\mathrm{id}_{\vec{E}} - \vec{f}) = \{0\}$.

10.11 Exercice. Soient E un espace affine euclidien et $f : E \to E$ une isométrie. Quels sont les points M de E qui minimisent la distance $Mf(M)$?

10.12 Exercice. *Oral CAPES, dossier du 12 juillet 2007 (suggéré par Gentiana Danila).* Paul trouve un parchemin dans une bouteille jetée à la mer. Voici ce qui est écrit :

« *Rends-toi sur l'île du pendu, tu y trouveras une potence.*

À partir de la potence, dirige-toi vers l'unique chêne de l'île en comptant tes pas. Au chêne, pivote d'un quart de tour vers ta droite et marche le même nombre de pas. Plante un piquet en terre.

À partir de la potence, dirige-toi ensuite vers la vieille barque éventrée en comptant tes pas. Arrivé à la barque, pivote d'un quart de tour vers ta gauche et marche le même nombre de pas. Plante à nouveau un piquet en terre.

Creuse à mi-chemin entre les deux piquets : le trésor est là. »

Paul se rend sur l'île du pendu, y trouve le chêne et la vieille barque éventrée, mais, à son grand désespoir, il n'y a plus aucune trace de la potence. Il part de l'endroit où il se trouve et suit à la lettre les consignes précédentes et trouve le trésor. A-t-il réellement eu de la chance ?

10.13 Exercice. (*Exercice 5.3 du cours de groupes et géométrie - de Catherine Gille.*) Soit $\mathcal{E}$ un plan affine euclidien orienté muni d'un repère orthonormé direct $(O, \vec{u}, \vec{v})$. Soit ρ la rotation de centre O d'angle $2\pi/n$, et soit σ la symétrie orthogonale par rapport à l'axe $(O, \vec{u})$. On pose $P_0 = O + \vec{u}$ et pour tout $k \in \{1, ..., n-1\}$, $P_k = \rho^k(P_0)$. On appelle *groupe diédral* et on note D_n le groupe des isométries qui envoient le polygone régulier $\{P_0, P_1, \ldots, P_{n-1}\}$ sur lui-même.

1. Montrer que les isométries directes de D_n forment un sous-groupe cyclique engendré par ρ. Quel est l'ordre de ce sous-groupe ?
2. Montrer que tout élément de D_n est de la forme ρ^k ou $\rho^k \circ \sigma$ pour un $k \in \{0, ..., n-1\}$. Quel est l'ordre de D_n ?
3. Caractériser géométriquement les éléments de D_n (distinguer suivant la parité de n). Expliciter géométriquement le produit de deux éléments quelconques de D_n.

10.14 Exercice. Groupe de cube.

1. Décrire les 24 isométries directes du cube, leur action sur les diagonales, (*i.e.* leur image dans le groupe $\mathfrak{S}_4$) et leur action sur les faces du cube.
2. Construire un homomorphisme du groupe du cube à valeurs dans $\mathfrak{S}_3$. Quel est son noyau ?

10.15 Exercice. (Coloriages) Fixons un ensemble C fini à d éléments qui représentera l'ensemble des couleurs. On appelle coloriage d'un ensemble Y par C une application de Y dans C. Ainsi un coloriage (des faces) d'un cube est un choix d'une couleur par face, donc une application de l'ensemble de ses faces dans C.

Un groupe G qui opère sur Y opère sur ses coloriages : pour un coloriage $c : Y \to C$, et $g \in G$, on note $g.c$ le coloriage défini par $(g.c)(y) = c(g^{-1}.y)$. On vérifie immédiatement qu'il s'agit d'une opération.

Deux coloriages seront alors considérés comme équivalents s'ils sont dans la même orbite pour l'action ainsi définie de G.

Soit G un groupe fini opérant sur un ensemble fini Y. On fait opérer G sur l'ensemble C^Y des coloriages de Y.

1. Démontrer que le nombre de coloriages fixés par un élément $g \in G$ est $d^{k(g)}$, où $k(g)$ est le nombre d'orbites de g dans son action sur Y.
2. *Coloriages du cube.* On suppose que G est le groupe des rotations du cube et Y l'ensemble de ses faces. Combien y a-t-il de coloriages ?
3. *Collier de perles.* On suppose que $G = D_n$ est le groupe diédral agissant sur le polygone Y à n sommets (les perles). Combien y a-t-il de coloriages ?

11 Solutions des exercices

I. Algèbre générale

11.1 Arithmétique dans $\mathbb{Z}$

Exercice 1.1.

1. Notons d le plus grand commun diviseur de a et b. Puisque δ est un diviseur commun à a et b, δ divise d. Comme d divise a et b, il existe deux entiers relatifs a' et b' tels que $a = da'$ et $b = db'$. Donc $\delta = au + bv = d(a'u + b'v)$ et d divise δ. Par suite $|\delta| = d$.
2. On a $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, donc $ca\mathbb{Z} + cb\mathbb{Z} = cd\mathbb{Z}$. On en déduit que cd est le plus grand commun diviseur de ca et cb.

   Par définition du plus petit commun multiple de a et b, on a $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, donc $c(a\mathbb{Z}) \cap c(b\mathbb{Z}) = cm\mathbb{Z}$. Donc cm est bien le plus petit commun multiple de ac et bc.
3. Écrivons $a = a'd$ et $b = b'd$ avec a' et b' premiers entre eux. Alors le plus petit commun multiple de a' et b' est $a'b'$, donc le plus petit commun multiple de a et b est $a'b'd$. On a bien $md = a'db'd = ab$.

Exercice 1.2.

1. Comme a divise c, il existe un entier relatif a' tel que $c = aa'$ et ainsi b divise aa' avec a et b premiers entre eux. On en déduit, d'après le théorème de Gauss, que b divise a'. Alors ab divise $aa' = c$.
2. On suppose que a est premier à b et à c, donc d'après le théorème de Bézout, il existe des entiers relatifs u, v, u' et v' tels que : $au + bv = 1$ et $au' + cv' = 1$. Donc : $1 = (au + bv)(au' + cv') = a(auu' + ucv' + u'bv) + (bc)(vv')$, avec $(auu' + ucv' + u'bv) \in \mathbb{Z}$ et $vv' \in \mathbb{Z}$; donc a est premier à bc.
3. a) • Démontrons que a et b^n sont premiers entre eux par récurrence sur n :
     ∗ Il n'y a rien à démontrer pour $n = 1$.
     ∗ Supposons que a et b^n ($n \in \mathbb{N}^*$) soient premiers entre eux. Alors, comme a et b sont premiers entre eux, d'après la question précédente, a et $b^n b = b^{n+1}$ sont premiers entre eux.
   • On en déduit immédiatement que a^n et b^n sont premiers entre eux en appliquant ce qui précède à b^n et à a.

   b) Comme d est le plus grand commun diviseur de a et b, il existe deux entiers relatifs a' et b' tels que $a = da'$ et $b = db'$, avec a' et b' premiers entre eux. D'après la question précédente, on a alors $a^n = d^n a'^n$ et $b^n = d^n b'^n$, avec a'^n et b'^n premiers entre eux. Ainsi le plus grand commun diviseur de a^n et b^n est d^n.
4. Notons d le plus grand commun diviseur de a et b et écrivons $a = ed$ et $b = b'd$ avec e et b' premiers entre eux. Comme $ed = a|bc = db'c$, il vient $e|b'c$ et comme e et b' sont premiers entre eux, il vient $e|c$.

Exercice 1.3. Si n est premier, le théorème de Wilson nous dit que $(n-1)! \equiv -1 \ \ [n]$ - (voir exerc. 3.15 pour une démonstration).

Si n n'est pas premier, il peut s'écrire $n = pm$ où p est un diviseur premier. Si $m \neq p$, alors m et p figurent dans $(n-1)!$ donc $(n-1)! \equiv 0 \ \ [n]$. Si $n = p^2$ avec $p \geqslant 3$, alors p et $2p$ figurent dans $(n-1)!$. Il vient $(n-1)! \equiv 0 \ \ [n]$.

Reste 4 et $(4-1)! = 6 \equiv 2 \ \ [4]$.

Exercice 1.4. On peut sauver tous les prisonniers sauf celui qui parle en premier.

Afin d'expliquer une tactique gagnante, notons $c_1, \ldots, c_p$ la couleur des chapeaux des prisoniers. Le k-ième prisonier voit $c_{k+1}, \ldots, c_p$.

- Les prisoniers conviennent d'une bijection f de l'ensemble C des couleurs sur $\mathbb{Z}/d\mathbb{Z}$.
- Afin de pouvoir sauver tous les autres prisonniers le premier prisonier calcule la somme $S = \sum_{i=2}^{p} f(c_i)$ des chapeaux qu'il voit. Il énonce $f^{-1}(S)$.
- Le deuxième, connait $S_2 = \sum_{i=3}^{p} f(c_i)$, donc il déduit $f(c_2) = S - S_2$. Il annonce donc correctement sa couleur.
- Le troisième, connait $S_3 = \sum_{i=4}^{p} f(c_i)$, il a entendu c_2, donc il déduit $f(c_3) = S - S_3 - f(c_2)$.
- Et ainsi de suite, le k-ième connait $S_k = \sum_{i=k+1}^{p} f(c_i)$, il a entendu $c_2, \ldots, c_{k-1}$, et a calculé $A_k = \sum_{j=2}^{k-1} f(c_j)$; il en déduit $f(c_k) = S - S_k - A_k$, donc c_k.

On peut mettre en pratique cet exercice avec des élèves que l'on dispose en file indienne et à qui on attache dans le dos des pastilles de couleur : bleues=0, rouge=1 et verte=2 (modulo 3). On leur demande de pratiquer la stratégie : le premier annonce S et « sauve » tous les suivants (si aucune erreur n'est commise !). Ils seront absolument ravis ! C'est très intéressant de voir chaque nouvel élève faire la somme modulo 3 des annonces faites avant lui, puis la somme modulo 3 des couleurs devant lui, puis calculer $S - A_k - S_k$ et annoncer la couleur correspondante... On retire alors la pastille de son dos et il constate que c'est la couleur qu'il avait annoncée. Succès garanti !

Exercice 1.5.

1. Puisque e et N sont premiers entre eux, la classe de e est inversible dans $\mathbb{Z}/N\mathbb{Z}$; il existe un unique $d \in \mathbb{Z}$, avec $0 \leqslant d \leqslant N-1$ dont la classe est l'inverse de celle de e modulo N.
2. On peut écrire $ed = k(p-1)+1$. Si n n'est pas divisible par p, alors $n^{p-1} \equiv 1 \ [p]$ (théorème de Fermat), donc $n^{k(p-1)} \equiv 1 \ [p]$ et enfin $n^{ed} \equiv n \ [p]$. Cela reste vrai si p divise n : dans ce cas p divise aussi n^{ed}. De même $n^{ed} \equiv n[q]$.
3. La réciproque de cette application est l'application qui à a associe le reste dans la division de a^d par pq.

Exercice 1.6.

1. Notons d le pgcd de a et b et $S_c = \{(x,y) \in \mathbb{Z} \times \mathbb{Z};\ ax + by = c\}$. On remarque d'abord que $S_c \neq \emptyset \iff c \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$. Autrement dit, l'équation admet des solutions si et seulement si c est multiple de d.

   Supposons que c est un multiple de d et soit (x_0, y_0) une solution particulière. Alors l'équation devient $a(x-x_0) + b(y-y_0) = 0$, soit $(x-x_0, y-y_0) \in S_0$. Il reste à décrire S_0 et une méthode pour trouver une solution particulière.

   Écrivons $a = a'd$ et $b = b'd$. L'équation $ax + by = 0$ est équivalente à $a'x + b'y = 0$ et maintenant a' et b' sont premiers entre eux. Si (x,y) est solution, b' divise $a'x = -b'y$ et est premier avec a', donc b' divise x. On écrit $x = kb'$. Notre équation devient $a'kb' + b'y = 0$, soit $y = -ka'$. Inversement, pour tout $k \in \mathbb{Z}$, on a $(kb', -ka') \in S_0$, donc $S_0 = \{(kb', -ka');\ k \in \mathbb{Z}\}$. Enfin $S_c = \{(x_0 - kb', y_0 + ka');\ k \in \mathbb{Z}\}$.

   L'algorithme d'Euclide qui permet de trouver d, a', b', permet aussi de trouver une solution particulière (x_0, y_0). En effet, en remontant l'algorithme d'Euclide, on trouve (u,v) tels que $au+bv = d$. Si on écrit $c = c'd$ (puisque c est multiple de d), on pourra poser $x_0 = c'u$ et $y_0 = c'v$.

Remarque : On peut partir de *n'importe quelle* solution particulière. Une telle solution particulière peut être évidente (par exemple, si $c = a + b$...).

Discussion. Pour la suite de l'exercice a et b sont supposés premiers entre eux. Supposons $c \geqslant 0$ et décrivons les solutions positives ou nulles. Pour cela, remarquons qu'il existe un unique $u \in [0, b-1] \cap \mathbb{N}$ tel que $c - au \in b\mathbb{Z}$. En effet, u est le représentant dans $[0, b-1]$ du quotient de la classe de c par celle de a (qui est inversible) dans $\mathbb{Z}/b\mathbb{Z}$. Alors $c = au + bv$. Les solutions sont $(u+kb, v-ka),\ k \in \mathbb{Z}$. Comme $0 \leqslant u < b$, les solutions positives sont $(u+kb, v-ka),\ k \in \mathbb{N},\ ka \leqslant v$. Si $v < 0$, il n'y a pas de solutions positives ; si $v \geqslant 0$, les solutions positives sont données par les entiers $k \in [0, E(v/a)]$, soit $k \in [0, E((c-au)/ab)]$. Il y a alors exactement $E\Big(\dfrac{c-au}{ab}\Big) + 1$ solutions.

2. L'équation $ax + by = ab$ admet les solutions positives $(b, 0)$ et $(0, a)$. Par ce qui précède, si l'équation $ax + by = c$ admet deux solutions positives, alors $c - ax_0 \geqslant ab$ donc $c \geqslant ab$. Le plus petit entier qui s'écrit de deux façons sous la forme $ax + by$ est donc ab.

3. De la discussion ci-dessus, il résulte que $c \in A$ si et seulement s'il existe $u \in [0, b-1]$ et $v \in \mathbb{N}^*$ tels que $c = au - bv$.

   a) On a $ab - a - b = a(b-1) - b$ donc $ab - b - a \in A$. Si $c \in A$, il existe $u \leqslant b-1$ et $v \geqslant 1$ tels que $c = au - bv$, donc $c \leqslant a(b-1) - b$. Donc le plus grand élément de A est $ab - a - b$.

   b) On a vu que $c \in A$ si et seulement s'il s'écrit sous la forme $c = ua - vb$ avec $0 \leqslant u \leqslant b-1$ et $v \geqslant 1$. Remarquons que, puisque $c \geqslant 0$, on a $ua \geqslant vb$. Or $ua < ab$ donc $v < a$ soit $v \leqslant a-1$ et $vb > 0$ donc $u > 0$ soit $u \geqslant 1$. Cela prouve que tout élément de A s'écrit $ua - vb;\ (u, v) \in \mathbb{N}^2,\ 1 \leqslant u \leqslant b-1;\ 1 \leqslant v \leqslant a-1$.
   Inversement, tout élément positif qui s'écrit comme ça est dans A. Si $c = -(ua - bv)$ avec $1 \leqslant u \leqslant b-1;\ 1 \leqslant v \leqslant a-1$, alors on a $c = (b-u)a - (a-v)b$; puisque $1 \leqslant b-u \leqslant b-1$ et $1 \leqslant a-v \leqslant a-1$, il vient encore $c \in A$.

   c) Par ce qui précède, lorsque (u, v) décrit $[\![1, b-1]\!] \times [\![1, a-1]\!]$, $ua - bv$ décrit $A \cup -A$. Si $ua - bv = u'a - bv'$, alors $(u-u')a = b(v-v')$, et par le théorème de Gauss, b divise $u - u'$; or puisque $1 \leqslant u, u' \leqslant b-1$, il vient $|u - u'| \leqslant b-2$, donc la seule possibilité est $u = u'$ et $v = v'$. On a donc une bijection de $[\![1, b-1]\!] \times [\![1, a-1]\!]$ sur $A \cup -A$. Il s'ensuit que A a exactement $\dfrac{(a-1)(b-1)}{2}$ éléments.
   Notons que ce nombre est entier, puisque a et b étant premiers entre eux, il ne peuvent être tous deux pairs.

4. a) Lorsque $a = 7$ et $b = 5$, on trouve $ab - a - b = 35 - 7 - 5 = 23$.

   b) Il y a $\dfrac{(3-1)(5-1)}{2} = 4$ scores impossibles avec 3 et 5 qui sont $1, 2, 4, 7$ (nos calculs donnent les nombres positifs de la forme $5u-3v$ avec $v > 0$ et $u = 1$ ou $u = 2$ soit $5-3$ et $10-3$, $10-6$ et $10-9$). Le nombre 7 étant la valeur d'un essai transformé, les seuls scores impossibles sont $1, 2, 4$.

Exercice 1.7. [un peu rapide]

1. On commence par une remarque : si $p_1, \ldots, p_k$ sont des nombres premiers distincts et ξ_i, η_i des nombres entiers (pouvant être nuls), alors $x = \prod_{i=1}^{k} p_i^{\xi_i}$ divise $y = \prod_{i=1}^{k} p_i^{\eta_i}$ si et seulement pour out i on a $\xi_i \leqslant \eta_i$.
   En effet,

   • si les $\eta_i - \xi_i$ sont positifs ou nuls on a $y = x \prod_{i=1}^{k} p_i^{\eta_i - \xi_i}$ donc x divise y.

- si x divise y, alors on écrit $y = xz$ où $z = \prod_{i=1}^{k} p_i^{\zeta_i}$. D'après l'unicité de la décomposition en nombres premiers, il vient $\eta_i = \xi_i + \zeta_i$.

Écrivons $a = \prod p_i^{\alpha_i}$ et $b = \prod_{i=1}^{k} p_i^{\beta_i}$. Les diviseurs communs sont de la forme $c = \prod p_i^{\gamma_i}$ avec $\gamma_i \leqslant \alpha_i$ et $\gamma_i \leqslant \beta_i$. Il vient $d = \prod p_i^{\delta_i}$ avec $\delta_i = \inf(\alpha_i, \beta_i)$. De même, ou en utilisant la formule $dm = ab$, on a $m = \prod p_i^{\mu_i}$ avec $\mu_i = \sup(\alpha_i, \beta_i)$.

Pour des petits nombres, cette façon de calculer le pgcd peut être plus rapide que l'algorithme d'Euclide. Par contre, pour des nombres relativement grands la décomposition en nombres premiers est « impraticable », contrairement à l'algorithme d'Euclide.

2. Posons $A = \{i;\ \alpha_i < \beta_i\}$, puis $a_1 = \prod_{i\in A} p_i^{\alpha_i}$, $a_2 = \prod_{i\notin A} p_i^{\alpha_i}$, $b_1 = \prod_{i\in A} p_i^{\beta_i}$ et $b_2 = \prod_{i\notin A} p_i^{\beta_i}$. On a bien
   - $a = a_1a_2$, $b = b_1b_2$;
   - $a_1|b_1$ puisque pour $i \in A$ on a $\alpha_i < \beta_i$ et $b_2|a_2$ puisque pour $i \notin A$ on a $\alpha_i \geqslant \beta_i$;
   - a_2 et b_1 n'ont pas de diviseurs premiers communs, ils sont donc premiers entre eux.
3. Le nombre $d' = a_1b_2$ divise clairement a et b ; comme a/d' divise a_2 et b/d' divise b_1, donc a/d' et b/d' sont premiers entre eux. Donc $d' = d$. De l'égalité $ab = md$ il vient $a_2b_1 = m$.
4. D'après le théorème chinois, on a des isomorphismes

$$\begin{aligned}\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} &\simeq (\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z}) \times (\mathbb{Z}/b_1\mathbb{Z} \times \mathbb{Z}/b_2\mathbb{Z})\\ &\simeq (\mathbb{Z}/a_1\mathbb{Z} \times \mathbb{Z}/b_2\mathbb{Z}) \times (\mathbb{Z}/b_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z})\\ &\simeq \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.\end{aligned}$$

Exercice 1.8.

1.

Exercice 1.9.

1. Les premiers nombres de Fibonacci sont :

n	0	1	2	3	4	5	6	7	8	9	10
F_n	0	1	1	2	3	5	8	13	21	34	55
n	11	12	13	14	15	16	17	18	19	20	21
F_n	89	144	233	377	610	987	1597	2584	4181	6765	10946

D'après ce tableau, les F_{3k} sont pairs, les F_{4k} sont multiples de 3 et les F_{5k} sont multiples de 5...

2. a) Démontrons que $F_m|F_{km}$ par récurrence sur k.
   C'est vrai pour $k = 0$ (car $F_0 = 0$) et $k = 1$.
   On sait que $\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}^p = \begin{pmatrix}F_{p-1} & F_p\\ F_p & F_{p+1}\end{pmatrix}$. Il vient, pour tout $p, q \in \mathbb{N}$,

$$\begin{pmatrix}F_{p-1} & F_p\\ F_p & F_{p+1}\end{pmatrix}\begin{pmatrix}F_{q-1} & F_q\\ F_q & F_{q+1}\end{pmatrix} = \begin{pmatrix}F_{p+q-1} & F_{p+q}\\ F_{p+q} & F_{p+q+1}\end{pmatrix}.$$

   En particulier, on a $F_{p+q} = F_pF_{q-1} + F_{p+1}F_q$. Prenant $p = m$ et $q = km$, si F_p et F_q sont des multiples de F_m, il en va de même pour F_{p+q}.

   b) Pour $n \in \mathbb{N}$, notons $M_2(\mathbb{Z}/n\mathbb{Z})$ l'anneau des matrices 2×2 à coefficients dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ et $G_n = GL(2, \mathbb{Z}/n\mathbb{Z})$ le groupe formé par les éléments inversibles de cet anneau, *i.e.* les matrices 2×2 à coefficients dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ inversibles. Notons aussi Δ_n le sous-groupe de G_n formé des matrices diagonales.

L'application $\psi : \mathbb{Z} \to G_n$ qui à k associe la classe dans $GL(2, \mathbb{Z}/n\mathbb{Z})$ de la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^k$ est un homomorphisme de groupes. Pour $k \in \mathbb{N}$ on a $n|F_k \iff \psi(k) \in \Delta_n$. En d'autres termes, on a

$$\{k \in \mathbb{N};\ n|F_k\} = \mathbb{N} \cap \psi^{-1}(\Delta_n).$$

Or, puisque Δ_n est un sous-groupe de G_n et ψ est un homomorphisme de groupes, $\psi^{-1}(\Delta_n)$ est un sous-groupe de $\mathbb{Z}$; il existe un unique élément $a \in \mathbb{N}$ tel que $\psi^{-1}(\Delta_n) = a\mathbb{Z}$, donc $\mathbb{N} \cap \psi^{-1}(\Delta_n) = a\mathbb{N}$. Enfin, puisque G_n est fini, ψ n'est pas injective ; son noyau n'est pas réduit à $\{0\}$ et est contenu dans $\psi^{-1}(\Delta_n)$, donc $a \neq 0$.

3. Soit $p \geqslant 7$ un nombre premier. Remarquons que $X^2 - X - 1$ admet une racine dans $\mathbb{F}_p$ si et seulement si 5 (le discriminant de ce trinôme) est un carré dans $\mathbb{F}_p$. En effet,
   - Supposons qu'il existe $a \in \mathbb{F}_p$ tel que $a^2 = 5$. Comme $5 \neq 0$, il vient $a \neq 0$. De plus $p \neq 2$, donc 2 est inversible dans $\mathbb{F}_p$. Alors $\alpha = \dfrac{1+a}{2}$ et $\beta = \dfrac{1-a}{2}$ sont deux racines distinctes du polynôme $X^2 - X - 1$ dans $\mathbb{F}_p$.
   - Supposons que $\alpha \in \mathbb{F}_p$ est racine du polynôme $X^2 - X - 1$; alors $\alpha^2 = \alpha + 1$, donc $(2\alpha - 1)^2 = 4\alpha^2 - 4\alpha + 1 = 4(\alpha + 1) - 4\alpha + 1 = 5$.

   Notons J la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ à coefficients dans $\mathbb{F}_p$.

   a) On suppose que 5 est un carré modulo p. Alors le polynôme caractéristique $X^2 - X - 1$ de J a deux racines distinctes α, β, donc J est diagonalisable. Il existe donc $P \in GL(2, \mathbb{F}_p)$ tel que $PJP^{-1} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$. Par le petit théorème de Fermat on a $\alpha^{p-1} = \beta^{p-1} = 1$ (notons que α et β sont non nuls car J est inversible - son déterminant est -1). On a donc $J^{p-1} = P^{-1} \begin{pmatrix} \alpha^{p-1} & 0 \\ 0 & \beta^{p-1} \end{pmatrix} P = I_2$. La classe modulo p de $\begin{pmatrix} F_{p-2} & F_{p-1} \\ F_{p-1} & F_p \end{pmatrix}$ est donc I_2, et p divise F_{p-1}.

   b) (i) L'ensemble K est un sous-espace vectoriel - donc un sous-groupe additif de $M_2(\mathbb{F}_p)$. Comme $J^2 = J + I_2$, pour $a, b, c, d \in \mathbb{F}_p$, on a

$$\begin{aligned} (aI_2 + bJ)(cI_2 + dJ) &= acI_2 + (ad + bc)J + bd(J + I_2) \\ &= (ac + bd)I_2 + (ad + bc + bd)J \end{aligned}$$

   donc K est stable par le produit : c'est un sous-anneau de $M_2(\mathbb{F}_p)$. Comme I_2 et J commutent, l'anneau K est commutatif.

   (ii) Pour $a \neq 0$, aI_2 est inversible dans K. On suppose que 5 n'est pas un carré modulo p. Alors le polynôme caractéristique $X^2 - X - 1$ de J n'a pas de racines dans $\mathbb{F}_p$. Donc bJ n'a pas de valeurs propres pour $b \neq 0$, donc $aI_2 + bJ$ est inversible dans $M_2(\mathbb{F}_p)$ pour $b \neq 0$. Or d'après la formule([3])

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = \frac{1}{ad - bc} \left((a + d)I_2 - \begin{pmatrix} a & c \\ b & d \end{pmatrix} \right)$$

   l'inverse d'une matrice inversible $A \in M_2(\mathbb{F}_p)$ est dans l'espace vectoriel engendré par I_2 et A ; donc $(aI_2 + bJ)^{-1} \in K$.

   Cela prouve que K est un corps.

   (iii) Posons $\varphi(x) = x^p$. On a $\varphi(I_2) = I_2$. Soient $x, y \in K$. Comme K est commutatif, on a $\varphi(xy) = \varphi(x)\varphi(y)$. La formule du binôme, puisque p divise $\binom{p}{k}$ pour $1 \leqslant k \leqslant p - 1$, donne $\varphi(x + y) = \varphi(x) + \varphi(y)$.

3. Cette formule évidente est la formule de la comatrice en dimension 2. C'est aussi le théorème de Cayley-Hamilton en dimension 2.

(iv) Le polynôme $X^p - X$ admet dans K les p racines aI_2 avec $a \in \mathbb{F}_p$; comme un polynôme de degré k sur un corps commutatif K a au plus k racines, il n'en admet pas d'autre.

(v) D'après la question précédente, on a $J^p \neq J$. On a $J^2 = J + I_2$. Comme φ est un automorphisme de corps, il vient $\varphi(J^2) = \varphi(J) + I_2$.

(vi) Le polynôme $X^2 - X - 1$ admet dans K les racines J et $-J^{-1}$. Il ne peut en admettre d'autres donc J^p, qui est racine de ce polynôme et distinct de J est égal à $-J^{-1}$.

(vii) On a donc $J^{p+1} = -I_2$, en d'autres termes, la classe de $\begin{pmatrix} F_p & F_{p+1} \\ F_{p+1} & F_{p+2} \end{pmatrix}$ modulo p est $-I_2$.

Exercice 1.10.

1. Puisque $r_{n+1} = 0$, il vient $r_{n-1} = q_n r_n$; or $r_n < r_{n-1}$ (c'est un reste de division euclidienne), donc $q_n > 1$; enfin $q_n \geqslant 2$ (car c'est un entier).

2. a) L'égalité $r_{k-1} = q_k r_k + r_{k+1}$ se lit

$$(E_k) \qquad \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} \begin{pmatrix} r_{k+1} \\ r_k \end{pmatrix} = \begin{pmatrix} r_k \\ r_{k-1} \end{pmatrix}.$$

On procède par récurrence sur k. Pour $k = 1, \ldots, n$, notons (P_k) l'égalité

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} \begin{pmatrix} r_{k+1} \\ r_k \end{pmatrix} = \begin{pmatrix} r_1 \\ r_0 \end{pmatrix}.$$

L'identité (E_1) donne P_1.
Si (P_{k-1}) est vrai, l'identité (E_k) donne (P_k).

b) Ecrivons

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} = \begin{pmatrix} a_k & c_k \\ b_k & d_k \end{pmatrix} = A_k.$$

On a $\begin{pmatrix} a_k & c_k \\ b_k & d_k \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_{k+1} \end{pmatrix} = \begin{pmatrix} a_{k+1} & c_{k+1} \\ b_{k+1} & d_{k+1} \end{pmatrix}$. Ce qui donne $a_{k+1} = c_k$, $b_{k+1} = d_k$,

c) et pour $1 \leqslant k \leqslant n-1$, $a_{k+2} = c_{k+1} = a_{k+1}q_{k+1} + a_k \geqslant a_{k+1}$ et, de même $b_{k+2} = b_{k+1}q_{k+1} + b_k \geqslant b_{k+1}$.
Pour $k = 1$, on trouve $a_1 = 0,\ a_2 = 1,\ b_1 = 1,\ b_2 = q_1$.
Si $n = 1$ on a $a_{n+1} = 1 > 2a_0 = 0$ et $b_{n+1} = q_n \geqslant 2 = 2b_n$.
Sinon, $b_{n+1} = q_n b_n + b_{n-1} \geqslant 2b_n + b_0 > 2b_n$ et $a_{n+1} = q_n a_n + a_{n-1} \geqslant 2a_n$ avec égalité possible si $a_{n-1} = 0$ ce qui impose $n = 1$ (car sinon $a_{n-1} \geqslant a_1 = 1$) et $a_2 = 2$.

d) La matrice A_k est produit de k matrices de déterminant -1. Son déterminant est $(-1)^k$.

e) L'égalité $A_n \begin{pmatrix} r_{n+1} \\ r_n \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$ donne $\begin{pmatrix} r_{n+1} \\ r_n \end{pmatrix} = A_n^{-1} \begin{pmatrix} a \\ b \end{pmatrix}$. La formule de la comatrice donne $A_n^{-1} = (-1)^n \begin{pmatrix} b_{n+1} & -a_{n+1} \\ -b_n & a_n \end{pmatrix}$, ([4]) d'où le résultat.

3. a) L'égalité se démontre par récurrence sur k ; elle est vraie pour $k = 1$ car $F_0 = 0$, $F_1 = F_2 = 1$; si elle est vraie pour k, on a

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{k+1} = \begin{pmatrix} F_{k-1} & F_k \\ F_k & F_{k+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} F_k & F_{k-1} + F_k \\ F_{k+1} & F_k + F_{k+1} \end{pmatrix} = \begin{pmatrix} F_k & F_{k+1} \\ F_{k+1} & F_{k+2} \end{pmatrix}.$$

4. Plus généralement, pour une matrice 2×2 inversible on a $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} = \dfrac{1}{ad - bc} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$.

b) Les inégalités $b_k \geqslant F_k$ et $a_k \geqslant F_{k-1}$ se démontrent par récurrence forte sur k. Elles sont vraies pour $k = 1$ et $k = 2$. Si elles ont vraies pour k et $k+1$, on a $a_{k+2} = q_{k+1}a_{k+1} + a_k \geqslant a_{k+1} + a_k \geqslant F_k + F_{k-1} = F_{k+1}$ et $b_{k+2} = q_{k+1}b_{k+1} + b_k \geqslant b_{k+1} + b_k \geqslant F_{k+1} + F_k = F_{k+2}$.

4. On construit des suites a_k, b_k, r_k ; il suffit de garder en mémoire uniquement deux termes consécutifs de ces trois suites pour construire le suivant. On s'arrête quand $r_{n+1} = 0$; on a alors le pgcd de a, b (c'est r_n) et une relation de Bézout grâce à la question 2.e). La question 3 nous indique que la convergence est assez rapide : il faut moins de $k+1$ étapes si $b \leqslant F_k$. Or F_k croît géométriquement en k.

5. Puisque a et b sont premiers entre eux, il existe n tel que $r_n = 1$ et $r_{n+1} = 0$. On a donc

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Cela donne

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} u & a \\ v & b \end{pmatrix}.$$

6. Si on a une telle égalité, le calcul du déterminant nous donne une relation de Bézout $ub - va = (-1)^n$, donc a et b sont premiers entre eux. Démontrons par récurrence sur n que $a < b$ et que les quotients successifs de la division de a par b sont les q_j.

Si $n = 1$, on a $a = 1$ et $b = q_1 \geqslant 2$.

Supposons $n \geqslant 2$ et le cas de longueur $n - 1$ traité. Ecrivons

$$\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_3 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} u' & a' \\ v' & b' \end{pmatrix}.$$

D'après l'hypothèse de récurrence, $a' < b'$ et les quotients successifs de la division euclidienne de b' par a' sont $q_2, q_3, \ldots, q_n$. Or $\begin{pmatrix} u & a \\ v & b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} u' & a' \\ v' & b' \end{pmatrix}$, soit $b' = a$ et $b = q_1 a + a'$. Donc le quotient de b par a est q_1 et le reste a', et la suite des quotients successifs de la division euclidienne de b par a est bien $q_1, q_2, \ldots, q_n$.

Exercice 1.11.

1. a) Soit d le plus grand commun diviseur de a et b. Alors d^2 divise p, donc d divise p et $d \neq p$ soit $d = 1$.

   b) L'existence et unicité de $q_1, \ldots, q_n$ résultent de l'exercice 1.10.

   c) (*cf.* exerc. 1.10) Écrivons $\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_{n-1} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, avec $\alpha, \beta\gamma \in \mathbb{N}$. Il vient $u = \beta$, $v = \gamma$, puis $a = q_n u + \alpha \geqslant 2u$ et $b = q_n v + \gamma \geqslant 2v$ (puisque $q_n \geqslant 2$).

   d) Écrivons $\begin{pmatrix} u & v \\ a & b \end{pmatrix} \begin{pmatrix} u & a \\ v & b \end{pmatrix} = \begin{pmatrix} x & \ell \\ k & p \end{pmatrix}$. Cette matrice est symétrique et donc $k = \ell$ et il est clair que $q = p$. On a $2\ell = 2(ua + bv) \leqslant p$ d'après la question précédente. Enfin le déterminant de cette matrice est 1 (c'est un produit pair de matrices de déterminant -1), donc $\ell^2 \equiv -1$ [p]. Alors -1 a deux racines dans le corps $\mathbb{Z}/p\mathbb{Z}$: ℓ et $p - \ell$. Une seule des deux est $\leqslant p/2$.

2. D'après l'exercice 1.10, l'algorithme d'Euclide fournit un entier $m \in \mathbb{N}^*$, un m-uplet $(q_1, \ldots, q_m)$ d'entiers $\geqslant 1$ avec $q_m \geqslant 2$ et $\alpha, \beta \in \mathbb{N}$ tels que $\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_m \end{pmatrix} = \begin{pmatrix} \alpha & \ell \\ \beta & p \end{pmatrix}$ et on a $\beta \leqslant p/2$. Prenant les déterminants, il vient $-\beta\ell \equiv (-1)^m$ [p], donc β est, au signe près l'inverse de ℓ modulo p, c'est à dire $\pm\ell$, et puisque $\beta < p/2$, il vient $\beta = \ell$ et m est pair. Prenant

les transposées, on trouve $\begin{pmatrix}0&1\\1&q_m\end{pmatrix}\begin{pmatrix}0&1\\1&q_{m-1}\end{pmatrix}\dots\begin{pmatrix}0&1\\1&q_1\end{pmatrix}=\begin{pmatrix}\alpha&\ell\\\ell&p\end{pmatrix}$, et par unicité, on trouve $q_j=q_{m+1-j}$.

Posons alors $m=2k$ et $\begin{pmatrix}0&1\\1&q_{k+1}\end{pmatrix}\begin{pmatrix}0&1\\1&q_{k+2}\end{pmatrix}\dots\begin{pmatrix}0&1\\1&q_m\end{pmatrix}=\begin{pmatrix}u&a\\v&b\end{pmatrix}=A$. On a $\begin{pmatrix}\alpha&\ell\\\ell&p\end{pmatrix}={}^tAA$, donc $p=a^2+b^2$.

Remarquons de plus que l'on a $\begin{pmatrix}0&1\\1&q_1\end{pmatrix}\begin{pmatrix}0&1\\1&q_2\end{pmatrix}\dots\begin{pmatrix}0&1\\1&q_k\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}\ell\\p\end{pmatrix}$. Comme la matrice $\begin{pmatrix}0&1\\1&q_1\end{pmatrix}\begin{pmatrix}0&1\\1&q_2\end{pmatrix}\dots\begin{pmatrix}0&1\\1&q_k\end{pmatrix}$ est inversible, $\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}r_k\\r_{k+1}\end{pmatrix}$ d'après l'exercice 1.10. Notons aussi que $r_{k+2}\geqslant r_k+r_{k+1}$, donc $r_{k+2}^2>p$. En d'autres termes, a et b sont les deux derniers restes inférieurs à $\sqrt{p}$ dans les divisions euclidiennes successives entre p et ℓ.

Exercice 1.12.

1. Pour $a\in\mathbb{Z}$ et $m\in\mathbb{N}$, on a $a\equiv 1\ [a-1]$, donc $a^m\equiv 1\ [a-1]$. De même $a\equiv -1\ [a+1]$, donc si m est impair, alors $a^m\equiv -1\ [a+1]$.
   Si k est un diviseur de n, prenant $a=2^k$, on en déduit que 2^k-1 divise 2^n-1 ; donc si 2^n-1 est premier, on a $2^k-1=1$ (*i.e.* $k=1$) ou $2^k-1=2^n-1$, donc $k=n$. Autrement dit n est premier.
   Écrivons $n=2^km$ avec $k\in\mathbb{N}$ et m impair. Alors $2^{2^k}+1$ divise 2^n+1, donc, si 2^n+1 est premier, alors $m=1$.
2. On a $2^{2^k}\equiv -1\ [F_k]$, donc $2^{2^\ell}=(2^{2^k})^{2^{\ell-k}}\equiv 1\ [F_k]$. Enfin $F_\ell\equiv 2\ [F_k]$. Le pgcd de F_k et F_ℓ divise 2 et, puisque F_ℓ est impair, F_k et F_ℓ sont premiers entre eux.
3. Puisque $q|M_p$, on a $2^p\equiv 1\ [q]$. Donc l'ordre de 2 dans $\mathbb{F}_q^*$ divise p ; ce ne peut être que p. Or l'ordre de p divise l'ordre du groupe $\mathbb{F}_q^*$, donc p divise $q-1$. Comme q est impair $2p|q-1$.
4. Si M_{13} n'était pas premier, son plus petit diviseur non nul q serait $<\sqrt{M_{13}}<64\sqrt{2}<100$ et un nombre premier de la forme $26k+1$. Comme 27 n'est pas premier, il reste à teste 53 et 79. Or $2^6\equiv 11\ [53]$, donc $2^{12}\equiv 121\equiv 15\ [53]$ et enfin $M_{13}\equiv 2\times 15-1=29\neq 0\ [53]$ et $2^6\equiv -15\ [53]$, donc $2^{12}\equiv 225\equiv -12\ [79]$ et enfin $M_{13}\equiv -2\times 12-1=-25\neq 0\ [79]$.
5. a) On a $2^{2^\ell}\equiv -1\ [q]$, donc $2^{2^{\ell+1}}\equiv 1\ [q]$. L'ordre de 2 dans le groupe $\mathbb{F}_q^*$ divise $2^{\ell+1}$ et ne divise pas 2^ℓ : c'est $2^{\ell+1}$.
   b) L'ordre de 2 dans le groupe $\mathbb{F}_q^*$ divise l'ordre de $\mathbb{F}_q^*$, donc $2^{\ell+1}$ divise $q-1$.
   c) Comme ω^4 est la classe de 2^{2^ℓ}, on a $\omega^4=-1$, donc $\omega^2+\omega^{-2}=0$, donc $(\omega+\omega^{-1})^2=2$. On a $(\omega+\omega^{-1})^{2^{\ell+1}}=-1$, donc l'ordre de $\omega+\omega^{-1}$ divise $2^{\ell+2}$ et ne divise pas $2^{\ell+1}$: c'est $2^{\ell+2}$. On en déduit que $2^{\ell+2}$ divise $q-1$.
   d) Si q est le plus petit nombre premier divisant F_5, alors $q\simeq 1\ [2^7]$. Or 3 divise 129 et $4\times 128+1=513$ et 5 divise $3\times 128+1=385$. Enfin, $2\times 128+1=257=F_3$ est un nombre de Fermat donc premier à F_5. Le premier nombre à tester est donc $5\times 128+1$.
   e) On a $2^4\equiv -5^4\ [641]$, donc $F_5=2^{28}2^4+1\equiv 1-5^42^{28}\ [641]$.
   f) On a $52^7=640\equiv -1\ [641]$, donc $5^42^{28}=(52^7)^4\equiv 1\ [641]$ et 641 divise F_5.

Exercice 1.13.

Le cas $b=4$: 1. Écrivons $a^2+1=kp$. C'est une identité de Bézout prouvant que a et p sont premiers entre eux.
2. Puisque $p|a^2+1$, on en déduit que $x^2+1=0$, donc $x^4-1=(x^2+1)(x^2-1)=0$.
3. Comme $p\neq 2$, on a $-1\neq 1$. Or $x^2=-1$ donc $x^2\neq 1$.

4. L'ordre de x dans le groupe multiplicatif $\mathbb{F}_p^*$ divise 4 mais ne divise pas 2 : c'est 4. On en déduit que 4 divise l'ordre de $\mathbb{F}_p^*$, donc que $p \equiv 1 \ [4]$.
5. Soit $n \in \mathbb{N}$, tel que $n \geqslant 2$. Posons $a = n!$ et soit p un diviseur premier de a^2+1. Alors p est premier avec a, donc $p > n$ et $p \equiv 1 \ [4]$. On en déduit que l'ensemble des nombres premiers congrus à 1 modulo 4 n'est pas majoré : il est infini.
6. Si $n \geqslant 4$, alors $4|n!$, donc $n! - 1 \equiv -1 \ [4]$. Écrivons $n! - 1 = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ la décomposition de $n!-1$ en nombres premiers. Comme ce produit est congru à 3 modulo 4, un au moins de ses facteurs n'est pas congru à 1. Il existe donc j tel que $p_j \equiv 3 \ [4]$. Comme p_j divise $n!-1$, il ne divise pas $n!$, donc $p_j > n$. On en déduit que l'ensemble des nombres premiers congrus à 3 modulo 4 n'est pas majoré : il est infini.

Le cas $b = 6$: 1. Écrivons $a^2+a+1 = kp$, soit $kp - (a+1)a = 1$. C'est une identité de Bézout prouvant que a et p sont premiers entre eux.
2. Puisque $p|a^2+a+1$, on en déduit que $x^2+x+1 = 0$, donc $x^3 - 1 = (x^2+x+1)(x-1) = 0$.
3. Comme $p \neq 3$, on a et $1^2+1+1 \neq 0$, donc $x \neq 1$.
4. L'ordre de x dans le groupe multiplicatif $\mathbb{F}_p^*$ divise 3 mais n'est pas 1 : c'est 3. On en déduit que 3 divise l'ordre de $\mathbb{F}_p^*$, donc que $p \equiv 1 \ [3]$. En particulier, $p \neq 2$, donc p est impair : donc $p \equiv 1 \ [6]$.
5. Soit $n \in \mathbb{N}$, tel que $n \geqslant 3$. Posons $a = n!$ et soit p un diviseur premier de a^2+a+1. Alors p est premier avec a, donc $p > n$ et $p \equiv 1 \ [6]$. On en déduit que l'ensemble des nombres premiers congrus à 1 modulo 6 n'est pas majoré : il est infini.
6. Si $n \geqslant 3$, alors $3|n!$, donc $n! - 1 \equiv -1 \ [6]$. Écrivons $n! - 1 = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ la décomposition de $n!-1$ en nombres premiers. Comme ce produit est congru à 5 modulo 6, un au moins de ses facteurs n'est pas congru à 1. Il existe donc j tel que $p_j \equiv 5 \ [6]$. Comme p_j divise $n!-1$, il ne divise pas $n!$, donc $p_j > n$. On en déduit que l'ensemble des nombres premiers congrus à 5 modulo 6 n'est pas majoré : il est infini.

Le cas $b = 12$: 1. On a $a^4 - a^2 = 6a\binom{a+1}{3}$, donc $a^4 - a^2 + 1 \equiv 1 \ [6]$.
2. On a $a^{12} - 1 = (a^4-1)(a^4+a^2+1)(a^4-a^2+1)$. Donc $x^{12} = 1$.
3. On a $x^6 + 1 = (x^2+1)(x^4-x^2+1) = 0$, donc $x^6 - 1 = -2 \neq 0$ (puisque $p \neq 2$). On a $(x^2-2)(x^2+1) = x^4 - x^2 - 2 = -3 \neq 0$ (puisque $p \neq 3$), donc $x^4 - 1 = x^4 - x^2 + 1 + x^2 - 2 = x^2 - 2 \neq 0$. item L'ordre de x dans le groupe multiplicatif $\mathbb{F}_p^*$ divise 12 mais ne divise ni 4 ni 6 : c'est 12. On en déduit que 12 divise l'ordre de $\mathbb{F}_p^*$, donc que $p \equiv 1 \ [12]$.
4. Soit $n \in \mathbb{N}$, tel que $n \geqslant 2$. Posons $a = n!$ et soit p un diviseur premier de $a^4 - a^2 + 1$. Alors p est premier avec a, donc $p > n$ et $p \equiv 1 \ [12]$. On en déduit que l'ensemble des nombres premiers congrus à 1 modulo 12 n'est pas majoré : il est infini.

Le cas général 1. On démontre la première assertion par récurrence « forte » sur n.

- Si n est premier, $\Phi_n = \sum_{k=0}^{n-1} X^k$, donc $\Phi_n(0) = 1$.
- Dans le cas général, en utilisant l'égalité $\Phi_n \Phi_1 \prod_{d|n;\ 1<d<n} \Phi_d = X^n - 1$, on trouve $\Phi_n(0)\Phi_1(0) \prod_{d|n;\ 1<d<n} \Phi_d(0) = -1$. Or $\Phi_1 = X - 1$ donc $\Phi_1(0) = -1$ et l'on conclut par récurrence.

Pour la deuxième assertion, écrivons $\Phi_n = 1 + \sum_{k=1}^{N} \alpha_k X^k$. Il vient $\Phi_n(a) = 1 + a \sum_{k=1}^{N} \alpha_k a^{k-1}$, donc a et $\Phi_n(a)$ sont premiers entre eux d'après le théorème de Bézout.

2. On a $a^n - 1 = \Phi_n(a) \prod_{d|n;\ d<n} \Phi_d(a)$, donc $p|a^n - 1$, *i.e.* $x^n = 1$.

3. Remarquons que, puisque a et p sont premiers entre eux et $n|a$, n est inversible dans $\mathbb{F}_p$, donc nX^{n-1} et X^n-1 sont premiers entre eux dans $\mathbb{F}_p[X]$. Si Q^2 divisait X^n-1, on écrirait $X^n-1=Q^2P$ donc, en dérivant, $nX^{n-1}=Q(2Q'P+QP')$, et Q serait un diviseur commun de nX^{n-1} et X^n-1.
4. Soit $d\in\mathbb{N}$ un diviseur de n distinct de n. Écrivons $X^n-1=\prod_{k|n}\Phi_k$ et $X^d-1=\prod_{k|d}\Phi_k$, il vient $X^n-1=(X^d-1)\Phi_n\prod_{k|n;\ k\not|d,\ k<n}\Phi_k$. Cela prouve que le produit $(X^d-1)\Phi_n$ divise X^n-1, donc n'a pas de facteur carré dans $\mathbb{F}_p[X]$. En particulier, les polynômes X^d-1 et Φ_n sont premiers entre eux dans $\mathbb{F}_p[X]$. Ils n'ont donc pas de racine commune. Or, puisque $p|\Phi_n(a)$, x est racine de Φ_n, donc $x^d\neq 1$.
5. D'après ce qui précède, x est d'ordre n dans le groupe $\mathbb{F}_p^*$. L'ordre $p-1$ de ce groupe est donc un multiple de n ; autrement dit, p est congru à 1 modulo n.
6. Soit $N\geqslant n$. Prenant $a=N!$, on a démontré (puisque $n|a$) que tout diviseur premier de $\Phi_n(a)$ est premier avec a - donc $p>N$, et congru à 1 modulo n. L'ensemble des nombres premiers congrus à 1 modulo n n'est donc pas majoré : il est infini.

Exercice 1.14.

1. a) Si $x=y^2$, l'équation $z^2=x$ admet deux solutions $z=\pm y$ dans le corps $\mathbb{F}_p$; l'une des deux est congrue à un unique nombre $c\in\left\{1,\dots,\frac{p-1}{2}\right\}$. L'application qui à $c\in\left\{1,\dots,\frac{p-1}{2}\right\}$ associe la classe dans $\mathbb{F}_p$ de c^2 est donc une bijection de $\left\{1,\dots,\frac{p-1}{2}\right\}$ sur C ; C a donc $\frac{p-1}{2}$ éléments.
   b) Si $x=y^2$, on a $x^{\frac{p-1}{2}}=y^{p-1}=1$ d'après le petit théorème de Fermat.
   c) Le polynôme $X^{\frac{p-1}{2}}-1$ admet donc $\frac{p-1}{2}$ racines : tous les éléments de C. Son degré étant $\frac{p-1}{2}$, il ne peut avoir d'autres racines.
   d) Par (c), -1 est un carré dans $\mathbb{F}_p$ si et seulement si $(-1)^{\frac{p-1}{2}}=1$ (dans $\mathbb{F}_p$). Or $(-1)^{\frac{p-1}{2}}=1$ si $p\equiv 1\ [4]$ et $(-1)^{\frac{p-1}{2}}=-1$ si $p\equiv 3\ [4]$. Notons que $-1\neq 1$ dans $\mathbb{F}_p$ puisque on a supposé $p\neq 2$.
2. a) Puisque $p\neq 2$, on peut inverser 2 dans $\mathbb{F}_p$. On a $P=\left(X-\frac{a}{2}\right)^2-\frac{a^2-4b}{4}\cdot$ Il s'ensuit que P a une racine dans $\mathbb{F}_p$ si et seulement si a^2-4b est un carré dans $\mathbb{F}_p$.
   b) • L'équivalence entre (i) et (ii) résulte immédiatement de (a).
   • Si x est d'ordre 3 dans $\mathbb{F}_p^*$, alors x est racine de $X^3-1=(X-1)(X^2+X+1)$ et $x\neq 1$, donc $x^2+x+1=0$. Inversement, si $x^2+x+1=0$, alors $x^3=1$ et, puisque $3\neq 0$ dans $\mathbb{F}_p$, $x\neq 1$; donc x est d'ordre 3. Cela prouve (ii) $\Longleftrightarrow$ (iii).
   • Si $\mathbb{F}_p^*$ admet un élément d'ordre 3, alors 3 divise l'ordre $p-1$ du groupe $\mathbb{F}_p^*$, donc $p\equiv 1\ [3]$. Inversement, si p s'écrit $3k+1$, l'ensemble des $x\in\mathbb{F}_p$ tels que $x^k=1$ sont les racines du polynôme X^k-1. Il y en a au plus k dans le corps commutatif $\mathbb{F}_p$. Si $y\in\mathbb{F}_p^*$ est tel que $y^k\neq 1$, on a $(y^k)^3=y^{3k}=y^{p-1}=1$, d'après le petit théorème de Fermat. L'élément y^k est alors d'ordre 3 dans $\mathbb{F}_p^*$.
3. a) Pour $x\in\mathbb{F}_p^*$, on a $\left(x^{\frac{p-1}{2}}\right)^2=x^{p-1}=1$, donc $x^{\frac{p-1}{2}}=\pm 1$; si $x\notin C$, il vient $x^{\frac{p-1}{2}}=-1$. Si $a,b\in\mathbb{F}_p^*\setminus C$, il vient $(ab)^{\frac{p-1}{2}}=a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}=(-1)^2=1$, donc $ab\in C$.
   b) Si $-1\notin C$ et $2\notin C$, alors leur produit -2 est un carré par (a).

c) Si $-1 = a^2$, il vient $X^4 + 1 = (X^2 - a)(X^2 + a)$; si $2 = a^2$, il vient $X^4 + 1 = (X^2 + aX + 1)(X^2 - aX + 1)$ et si $-2 = a^2$, il vient $X^4 + 1 = (X^2 + aX - 1)(X^2 - aX - 1)$. Dans tous les cas $X^4 + 1$ n'est pas irréductible. Notons que pour $p = 2$, on a $X^4 + 1 = (X + 1)^4$.

d) On a $X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$. Comme $X^4 + 1$ n'a pas de racines dans $\mathbb{R}$, les polynômes $X^2 + \sqrt{2}X + 1$ et $X^2 - \sqrt{2}X + 1$ sont irréductibles.

e) D'après (d) les polynômes $P \in \mathbb{R}[X]$ divisant $X^4 + 1$ sont des multiples scalaires de $1, X^4 + 1, X^2 + \sqrt{2}X + 1$ et $X^2 - \sqrt{2}X + 1$. Donc $X^4 + 1$ n'a pas de diviseurs dans $\mathbb{Q}[X]$ autres que les scalaires et les multiples scalaires de $X^4 + 1$. Il est irréductible sur $\mathbb{Q}$ (et sur $\mathbb{Z}$).

Exercice 1.15.

1. a) On a $1^p = 1$, $(ab)^p = a^p b^p$ et, puisque $p | \binom{p}{k}$ pour $0 < k < p$, $(a + b)^p = a^p + b^p$.

   b) D'après (a), l'ensemble des racines de ce polynôme forment un sous-corps de L, qui a au plus p éléments : c'est donc le sous-corps $\mathbb{F}_p$ de L (appelé sous-corps premier de L).

2. a) Puisque $\omega^4 = -1$, on a $\omega^2 = -\omega^{-2}$, donc $(\omega + \omega^{-1})^= \omega^2 + 2\omega\omega^{-1} + \omega^{-2} = 2$.

   b) Dans L, le polynôme $X^2 = 2$ possède les racines x et $-x$. Il a des racines dans $\mathbb{F}_p$ si et seulement si $x \in \mathbb{F}_p$, donc (i) $\iff$ (ii).

   D'après 1.b) pour $y \in L$, on a équivalence entre $y^p = y$ et $y \in \mathbb{F}_p$, soit (ii) $\iff$ (iii).

   Remarquons que $\omega^5 = 1$ et comme $p \neq 5$ est impair, il vient $\omega^p \in \{\omega, \omega^2, \omega^3, \omega^4\}$. Remarquons aussi que, puisque $2x + 1 \neq 0$, $x \neq -1 - x$, donc $\omega^2 + \omega^{-2} \neq x$. Remarquons aussi que $x^p = \omega^p + \omega^{-p}$, donc si $\omega^p = \omega$ ou $\omega^p = \omega^{-1}$, il vient $x^p = x$; si $\omega^p = \omega^2$ ou $\omega^p = \omega^3$, il vient $x^p = -1 - x \neq x$. Cela prouve que (iii) $\iff$ (iv) $\iff$ (v).

3. a) On a $\omega^5 = 1$, donc $\omega^{-1} = \omega^4$ et enfin $\omega + \omega^2 + \omega^{-2} + \omega^{-1} = -1$, soit $\omega^2 + \omega^{-2} = -1 - x$. Enfin, $x^2 = \omega^2 + 2 + \omega^{-2} = -x + 1$.

   b) On a $(2x + 1)^2 = 4x^2 + 4x + 1 = 5$. Dans L, le polynôme $X^2 = 5$ possède les racines $2x + 1$ et $-2x - 1$. Il a des racines dans $\mathbb{F}_p$ si et seulement si $2x + 1 \in \mathbb{F}_p$, ce qui a lieu (puisque $p \neq 2$) si et seulement si $x \in \mathbb{F}_p$, donc (i) $\iff$ (ii).

   D'après 1.b) pour $y \in L$, on a équivalence entre $y^p = y$ et $y \in \mathbb{F}_p$, soit (ii) $\iff$ (iii).

   Remarquons que $\omega^8 = 1$ et comme p est impair, il vient $\omega^p \in \{\omega, \omega^3, \omega^5, \omega^7\}$. Remarquons aussi que $\omega^5 = -\omega$ et $\omega^7 = \omega^{-1}$, donc $\omega^3 = -\omega^{-1}$. Remarquons aussi que $x^p = \omega^p + \omega^{-p}$, donc si $\omega^p = \omega$ ou $\omega^p = \omega^{-1}$, il vient $x^p = x$; si $\omega^p = \omega^3$ ou $\omega^p = \omega^5$, il vient $x^p = -x \neq x$. Cela prouve que (iii) $\iff$ (iv) $\iff$ (v).

Exercice 1.16.

1. Voir exercice 1.14.
2. Remarquons que $\dfrac{p+1}{4} \in \mathbb{N}$. Puisque $x^{\frac{p-1}{2}} = 1$, on a $\left(x^{\frac{p+1}{4}}\right)^2 = x^{\frac{p-1}{2}+1} = x$.
3. a) On a $b^{2^\ell} = a^{u2^\ell} = 1$ d'après le théorème de Fermat, donc l'ordre de b dans $\mathbb{F}_p^*$ divise 2^ℓ ; il est de la forme 2^k avec $0 \leqslant k \leqslant \ell$.

   b) On a $a \mapsto a^u = \pm 1$ si et seulement si a est racine du polynôme $X^{2u} - 1$. Comme $X^{2u} - 1$ divise $X^{p-1} - 1$ qui est scindé a racines simples (il possède $p - 1$ racines d'après le théorème de Fermat), donc $X^{2u} - 1$ possède $2u$ racines distinctes. En prenant au hasard un élément de $\mathbb{F}_p^*$, on a donc $\dfrac{2u}{p-1} = 2^{1-\ell}$ chances d'avoir $b = \pm 1$.

   c) Si $b \neq \pm 1$, alors b est d'ordre 2^k avec $k \geqslant 2$, donc $c = b^{2^{k-2}}$ est d'ordre 4 : il vérifie $(c^2)^2 = 1$ et $c^2 \neq 1$, donc $c^2 = -1$. En pratique, si $b \neq \pm 1$, on pose $b_1 = b^2$ (modulo p) ; si $b_1 = -1$, alors b est une racine de -1 ; sinon, on continue : on pose $b_2 = b_1^2$. Au bout d'au plus $k - 1$ étapes, on aura trouvé notre racine de -1.

NB C'est en pratique la méthode qu'on utilise pour trouver la racine de -1 dans $\mathbb{F}_p$: on essaie des nombres a au hasard, avec à chaque fois au moins une chance sur deux de succès. Le nombre d'opérations utilisées est un « petit » poynôme en $\log p$: c'est beaucoup plus rapide si p est grand que d'essayer tous les nombres de $\mathbb{F}_p^*$...

Exercice 1.17.

1. Soit a un nombre strictement tel que $a-2$ soit multiple de tous les nombres premiers $\leqslant n+1$ (par exemple $a=(n+1)!+2$. Alors, pour $0\leqslant j\leqslant n-1$, $2+j$ a un diviseur premier $p\leqslant n+1$ et p divise aussi $a-2$, donc $a+j$ n'est pas premier.

2. a) On décompose a comme produit de nombres premiers. Cela donne : $a=\prod_{j=1}^{k} p_j^{\alpha_j}$ $(\alpha_j\in\mathbb{N})$. On effectue alors la division euclidienne de α_j par 2 sous la forme $\alpha_j=2\beta_j+\varepsilon_j$ avec $\beta_j\in\mathbb{N}$ et $\varepsilon_j\in\{0,1\}$. On pose $b=\prod_{j=1}^{k} p_j^{\beta_j}$.
Si $a\leqslant x$, il vient $1\leqslant b\leqslant\sqrt{x}$; on a donc $E(\sqrt{x})$ choix pour b et 2 choix pour chaque ε_j. Notons que l'inégalité est en général stricte puisque pour $b\leqslant\sqrt{x}$ et ε_j donnés on n'a pas toujours $b^2p_1^{\varepsilon_1}\dots p_k^{\varepsilon_k}\leqslant x$.
   b) Pour chaque $p\in\mathbb{N}$ le nombre des multiples de p dans $[1,x]$ est $E(x/p)$ donc leur proportion est $\dfrac{E(x/p)}{x}\leqslant\dfrac{1}{p}\cdot$ Or tout élément de $[1,x]\setminus A_k$ possède un diviseur premier dans $]p_k,x]$, d'où l'estimation.
   c) Pour $x=4^{k+1}$, le nombre d'éléments de $A_k\cap[1,x]$ est $\leqslant 2^{2k+1}$ d'après (a), donc leur proportion est $\leqslant 1/2$. On en déduit que la la proportion d'éléments $\mathbb{N}\setminus A_k$ dans $[1,x]$ est $\geqslant 1/2$, donc $\sum_{p\in\mathcal{P},\ p_k<p\leqslant x} 1/p\geqslant 1/2$ par (b). La série $\sum_j 1/p_k$ ne peut converger car son reste $\sum_{j>k} 1/p_j$ ne tend pas vers 0.

3. a) Pour $(k,n)\in\mathbb{N}^2$, notons B_k^n l'ensemble des nombres entiers qui s'écrivent $\prod_{i=1}^{k} p_i^{\alpha_i}$ avec $\alpha_i\in\mathbb{N}$, $\alpha_i\leqslant n$. D'après l'unicité de la décomposition en nombres premiers, l'application $(q,\gamma)\mapsto qp_k^{\gamma}$ est une bijection de $B_{k-1}^n\times[[0,n]]$ sur B_k^n. On en déduit que
$$\sum_{m\in B_k^n}\frac{1}{m}=\Big(\sum_{q\in B_{k-1}^n}\frac{1}{q}\Big)\Big(\sum_{\gamma=0}^{n}p_k^{-\gamma}\Big)=\Big(\sum_{q\in B_{k-1}^n}\frac{1}{q}\Big)\Big(\frac{1-p_k^{-1-n}}{1-p_k^{-1}}\Big),$$
puis, à l'aide d'une récurrence sur k,
$$\sum_{m\in B_k^n}\frac{1}{m}=\prod_{i=1}^{k}\Big(\frac{1-p_i^{-1-n}}{1-p_i^{-1}}\Big)\leqslant\prod_{i=1}^{k}\frac{p_i}{p_i-1}\cdot$$
Or, prenant $n\geqslant\log_2 k$, on a $\{1,\dots,k\}\subset B_k^n$, d'où le résultat.
   b) On a donc $-\sum_{i=1}^{k}\ln\Big(\dfrac{1}{p_i}\Big)\geqslant\ln\Big(\sum_{i=1}^{k}\dfrac{1}{i}\Big)$, donc la série de terme général $\Big(-\ln\Big(\dfrac{1}{p_i}\Big)\Big)$ diverge. Comme $-\ln\Big(\dfrac{1}{p_i}\Big)\sim\dfrac{1}{p_i}$ on en en déduit que la série de terme général $\Big(\dfrac{1}{p_i}\Big)$ diverge aussi.

4. Soit $B\subset\mathbb{N}^*$ l'ensemble des nombres entiers ne comportant pas le chiffre 9 dans leur développement décimal. Il y a 8.9^k éléments de B à $k+1$ chiffres tous plus grands que 10^k. On a donc $\sum_{n\in B}\dfrac{1}{n}\leqslant 8\sum_{k=1}^{+\infty}\dfrac{9^k}{10^k}<+\infty$. En particulier $\sum_{n\in\mathcal{P}\setminus B}\dfrac{1}{n}=+\infty$, donc $\mathcal{P}\setminus B$ est infini.

Exercice 1.18.

1. a) Remarquons que $v_p(n)$ est le nombre de $k \geqslant 1$ tels que np^{-k} soit entier, soit $\sum_{k=1}^{+\infty} E\big(np^{-k}\big) - E\big((n-1)p^{-k}\big)$. La formule s'en déduit par récurrence sur n puisque $v_p(1!) = 0$ et $v_p(n!) = \sum_{k=1}^{n} v_p(k) = v_p((n-1)!) + v_p(n)$.

   b) Pour $x \in \mathbb{R}$, on a $E(2x) - 2E(x) = 0$ si $E(2x)$ est pair et $E(2x) - 2E(x) = 1$ si $E(2x)$ est impair, d'où le résultat d'après (a).

   c) • De (b), on déduit que $v_p\binom{2n}{n}$ est inférieur ou égal au nombre des k tels que $E\big(2np^{-k}\big)$ soit non nul, c'est-à-dire $v_p\binom{2n}{n} \leqslant E\Big(\dfrac{\ln 2n}{\ln p}\Big)$.

   • Si $n < p \leqslant 2n$, alors $v_p(n!) = 0$ et $v_p((2n)!) = 1$.

   • Si $p \leqslant n < \dfrac{3p}{2}$, alors on ne peut avoir $p = 2$ (car $n \geqslant 3$) ; il vient $2n < p^2$; on a alors $E(2np^{-1}) = 2$ et, pour $k \geqslant 2$, on a $E(2np^{-k}) = 0$. Donc d'après (b), on a $v_p\binom{2n}{n} = 0$.

   d) On a $\ln\binom{2n}{n} = \sum_{p \text{ premier}} v_p\binom{2n}{n} \ln p$.

   (i) Il vient $\ln\binom{2n}{n} \geqslant \sum_{\substack{n<p<2n \\ p \text{ premier}}} v_p\binom{2n}{n} \ln p \geqslant (\pi(2n) - \pi(n)) \ln n$.

   (ii) On a d'après (c),

$$\begin{aligned} \ln\binom{2n}{n} &= \sum_{\substack{p \leqslant 2n/3 \\ p \text{ premier}}} v_p\binom{2n}{n} \ln p + \sum_{\substack{n<p<2n \\ p \text{ premier}}} \ln p \\ &\leqslant \pi(2n/3) \ln 2n + (\pi(2n) - \pi(n)) \ln 2n \end{aligned}$$

2. On a $\sum_{k=0}^{2n-1} \binom{2n-1}{k} = 2^{2n-1}$. Or pour tout k, on a $\binom{2n-1}{k} = \binom{2n-1}{2n-k-1}$ d'où l'égalité $\sum_{k=0}^{n-1} \binom{2n-1}{k} = 2^{2n-2}$.

   Remarquons que pour $0 \leqslant k < n-1$, on a $\binom{2n-1}{k+1} = \dfrac{2n-1-k}{k+1}\binom{2n-1}{k} \geqslant \binom{2n-1}{k}$; en d'autres termes, la suite $\binom{2n-1}{k}_{0 \leqslant k \leqslant n-1}$ est croissante ; il vient $\binom{2n-1}{n-1} \leqslant 2^{2n-2} = \sum_{k=0}^{n-1} \binom{2n-1}{k} \leqslant n\binom{2n-1}{n-1}$. Or $\binom{2n}{n} = 2\binom{2n-1}{n-1}$, d'où $\binom{2n}{n} \leqslant 2^{2n-1} \leqslant n\binom{2n}{n}$.

3. a) Remarquons que $\prod_{\substack{m<p\leqslant 2m \\ p \text{ premier}}} p$ divise $\binom{2n}{n} = 2\binom{2n-1}{n-1}$ donc il divise $\binom{2n-1}{n-1}$. On en déduit que $\sum_{\substack{m<p\leqslant 2m \\ p \text{ premier}}} \ln p \leqslant \ln\binom{2n-1}{n-1} \leqslant (n-1)\ln 4$ (d'après la question 2).

   Démontrons la deuxième par « récurrence forte sur n ». On la vérifie sans peine pour $n = 3$ et $n = 4$. Soit $n \geqslant 5$ et notons m la partie entière de $\dfrac{k+1}{2}$. D'après la question 2, on

a $\sum_{\substack{m<p\leqslant n\\ p \text{ premier}}} \ln p \leqslant \sum_{\substack{m<p\leqslant 2m\\ p \text{ premier}}} \ln p \leqslant (m-1)\ln 4$. D'après l'hypothèse de récurrence, on trouve $\sum_{\substack{p\leqslant n\\ p \text{ premier}}} = \sum_{\substack{p\leqslant m\\ p \text{ premier}}} + \sum_{\substack{m<p\leqslant n\\ p \text{ premier}}} \ln p \leqslant (m-1)\ln 4 + (m-1)\ln 4 \leqslant (n-1)\ln 4$.

b) On vérifie cette inégalité pour $n = 2, 3, 4...$

Supposons n pair $n = 2m$. D'après les questions 1.d.(ii) et 2, on a $\ln(2m)\pi(2m) \geqslant \ln \binom{2m}{m} \geqslant (2m-1)\ln 2 - \ln m$, d'où l'inégalité voulue. Si n est impair, on a $\pi(n) = \pi(n+1) \geqslant \frac{(n+1)(\ln 2)}{\ln(n+1)} - 1 \geqslant \frac{n(\ln 2)}{\ln n} - 1$ (la fonction $x \mapsto \frac{x}{\ln x}$ est croissante sur $[e, +\infty[$).

11.2 Anneaux

Exercice 2.1. On a $2 = 1^2 + 1^2 = (1+i)(1-i)$ et $-1 \equiv 1 \equiv 1^2$ est un carré modulo 2. Donc 2 vérifie tous ces énoncés.

On peut supposer désormais que p est impair.

Un carré est congru à 0 ou 1 modulo 4, donc (i)⇒(iv).

Il résulte de l'exercice 1.14 que (iv) ⟺ (iii).

Si p vérifie (iii), soit $x \in \mathbb{N}$ avec $x \leqslant p-1$ tel que $x^2 \equiv -1\ [p]$. Alors $p|(x+i)(x-i)$. Comme $\frac{x \pm i}{p} \notin Z[i]$, p ne peut diviser un de ces facteurs : il n'est pas irréductible, donc (iii)⇒(ii).

Enfin si $p = xy$ avec $x, y \in \mathbb{Z}[i]$ non inversibles, il vient $p^2 = v(p) = v(x)v(y)$. Et comme x et y ne sont pas inversibles, $v(x) \neq 1$ et $v(y) \neq 1$, donc $v(x) = v(y) = p$; écrivant $x = a + ib$ il vient $p = a^2 + b^2$, donc (ii)⇒(i).

Exercice 2.2.

1. a) Comme G est commutatif, on a $(ab)^m = a^m b^m$ pour tout $m \in \mathbb{Z}$.
Soit ℓ l'ordre de ab dans G. On a $(ab)^{k_a k_b} = a^{k_a k_b} b^{k_a k_b} = 1$, donc ℓ divise $k_a k_b$. Par ailleurs, on a $(ab)^\ell = 1$, donc $1 = (ab)^{\ell k_a} = (a^{k_a})^\ell b^{\ell k_a}$. On en déduit que $b^{\ell k_a} = 1$, donc $k_b | \ell k_a$, et $k_b | \ell$ d'après le théorème de Gauss. Puis, $b^\ell = 1$ et comme $(ab)^\ell = 1$, il vient aussi $a^\ell = 1$, ce qui implique que $k_a | \ell$. Enfin $k_a k_b | \ell$, donc $k_a k_b = \ell$.

b) On a $x^k = 1$ pour tout $x \in G$ si et seulement si k est multiple de l'ordre de x pour tout x, *i.e.* si et seulement si k est multiple du PPCM noté n des ordres des éléments de G. Comme l'ordre tout élément divise le cardinal de G, le PPCM des ordres divise le cardinal de G.

c) Il existe $y_j \in G$ tel que $\frac{n}{p_j}$ ne soit pas un multiple de l'ordre de y_j. L'ordre q de y_j est de la forme $q = p_j^k m$ avec m premier avec p_j. Comme q divise n mais pas $\frac{n}{p_j}$, il vient $k = m_j$. Posons alors $x_j = y_j^m$ qui est d'ordre $p_j^{m_j}$.

d) D'après la question a) et par récurrence, l'ordre de $\prod x_j$ est $\prod p_j^{m_j} = n$.

2. Soit K un corps commutatif et G un sous-groupe fini à N éléments de K^*. Soit n son exposant.

a) Les éléments de K qui vérifient $x^n = 1$ sont les racines du polynôme $X^n - 1$. Ce polynôme de degré n a au plus n racines. Tous les éléments de G vérifient $x^n = 1$, donc $N \leqslant n$.

b) On a vu que n divise l'ordre N de G. Comme $N \leqslant n$, il vient $n = N$. Il existe donc un élément d'ordre N : le groupe G est cyclique.

Exercice 2.3.

1. a) Pour tout $a \in \{0, \dots, d-1\}$ on a $\dfrac{a}{d} \in A_n$. L'écriture $\dfrac{a}{d}$ est irréductible si et seulement a et d sont premiers entre eux. Dans A_n, il y a donc $\varphi(d)$ éléments dont l'écriture irréductible est de la forme $\dfrac{a}{d}$.

   b) En regroupant les éléments de A_n selon le dénominateur de leur écriture irréductible, on obtient l'égalité $\displaystyle\sum_{d|n} \varphi(d) = n$.

2. a) En regroupant les éléments de G suivant leur ordre, il vient $\displaystyle\sum_{d|n} s_d = n$.

   b) • Par définition de l'ordre d'un élément d'un groupe, H a d éléments. Le groupe H est cyclique d'ordre d ; il est isomorphe à $(\mathbb{Z}/d\mathbb{Z}, +)$; il a $\varphi(d)$ générateurs (éléments d'ordre d).
   • Comme H est un groupe d'ordre d, tout élément de H vérifie $x^d = 1$.
   • Les éléments de K qui vérifient $y^d = 1$ sont les racines du polynôme $X^d - 1$. Ce polynôme de degré d a au plus d racines.
   • Posons $Z = \{y \in K^*;\ y^d = 1\}$. D'après ce qui précède, $H \subset Z$ et Z a au plus d éléments, donc $Z = H$.

   c) D'après ce qui précède, si G a un élément x d'ordre d, alors les élément d'ordre d sont les générateurs du sous-groupe H engendré par x, et il y en a $\varphi(d)$.

   d) On a $\displaystyle\sum_{d|n} s_d = n = \sum_{d|n} \varphi(d)$. Or pour tout d on a $s_d \leqslant \varphi(n)$. Les nombres positifs $\varphi(d) - s_d$ ont une somme nulle : ils sont tous nuls. En particulier $s_n = \varphi(n)$ n'est pas nul, donc G possède un élément d'ordre n : il est cyclique.

Exercice 2.4.

1. a) Un sous-groupe d'un groupe cyclique est cyclique, donc si $G \times H$ est cyclique, G et H sont cycliques (car isomorphes à des sous-groupes de $G \times H$). Il reste à déterminer quand le produit de deux groupes cycliques est cyclique, autrement dit, pour quels $a, b \in \mathbb{N}^*$ le groupe $\mathbb{Z}/a\mathbb{Z} \times b\mathbb{Z}$ est cyclique. Si a, b sont premiers entre eux, le groupe $\mathbb{Z}/a\mathbb{Z} \times b\mathbb{Z}$ est cyclique d'après le théorème chinois (1.35). Inversement, soit m le PPCM de a et b. Pour tout $(x, y) \in \mathbb{Z}/a\mathbb{Z} \times b\mathbb{Z}$, on a $m(x, y) = (mx, my) = 0$. Donc si $\mathbb{Z}/a\mathbb{Z} \times b\mathbb{Z}$ est cyclique, il existe $(x, y) \in \mathbb{Z}/a\mathbb{Z} \times b\mathbb{Z}$ d'ordre ab, donc $ab = m$, ce qui implique que a et b sont premiers entre eux.

   b) On a $\varphi(1) = \varphi(2) = 1$. Si $n \geqslant 3$ alors ou bien $n = 2^k$ avec $k \geqslant 2$ et $\varphi(n) = 2^{k-1}$ est pair ; ou bien n admet un diviseur premier p distinct de 2 donc s'écrit $n = p^k m$ où $k \geqslant 1$ et m est premier avec p. Alors $\varphi(n) = (p-1)p^{k-1}\varphi(m)$ est divisible par $p - 1$, donc est pair.

   c) D'après le théorème Chinois, $(\mathbb{Z}/nm\mathbb{Z})^*$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$. Les ordres $\varphi(n)$ et $\varphi(m)$ de $(\mathbb{Z}/n\mathbb{Z})^*$ et $(\mathbb{Z}/m\mathbb{Z})^*$ sont pairs et ne sont donc pas premiers entre eux. Leur produit n'est donc pas cyclique.

   d) Les éléments du groupe $(\mathbb{Z}/8\mathbb{Z})^*$ vérifient tous $x^2 = 1$, puisque $3^2 - 1$, $5^2 - 1$ et $7^2 - 1$ sont multiples de 8. Donc $(\mathbb{Z}/8\mathbb{Z})^*$ n'a pas d'éléments d'ordre 4 : il n'est pas cyclique.

2. a) Cela est vrai pour $k = 0$. Supposons $k \geqslant 0$ et $(1+p)^{p^k} = 1 + p^{k+1}(1+pb)$. On a alors $(1+p)^{p^{k+1}} = (1+p^{k+1}(1+pb))^p = \displaystyle\sum_{j=0}^{p} \binom{p}{j} p^{j(k+1)}(1+pb)^j$. Or $p^{k+3} | \binom{p}{2}.p^{2k+2}$ et pour $j \geqslant 3$, $p^{k+3} | p^{j(k+1)}$, donc, modulo p^{k+3},

$$\begin{aligned}(1+p)^{p^{k+1}} &\equiv 1 + p.p^{k+1}(1+pb)\\ &\equiv 1 + p^{k+2}\end{aligned}$$

b) On a $(1+p)^{p^{n-1}} \equiv 1 \quad [p^n]$ et $(1+p)^{p^{n-2}} \not\equiv 1 \quad [p^n]$. Donc l'ordre de $1+p$ divise p^{n-1} et ne divise pas p^{n-2} ; c'est donc p^{n-1}.

c) Soit m l'ordre de x dans $(\mathbb{Z}/p^n\mathbb{Z})^*$. On a $a^m \equiv 1 \quad [p^n]$. En particulier $a^m \equiv 1 \quad [p]$, donc m est un multiple de $p-1$. Écrivons $m = (p-1)d$ ([5]). Alors x^d est d'ordre $p-1$.

d) On a vu que dans $(\mathbb{Z}/p^n\mathbb{Z})^*$ il y a un élément u d'ordre p^{n-1} et un élément v d'ordre $p-1$. Soit ℓ l'ordre de uv dans $(\mathbb{Z}/p^n\mathbb{Z})^*$; on a $(uv)^\ell = 1$, donc $1 = (uv)^{\ell(p-1)} = (u^{p-1})^\ell v^{\ell(p-1)}$. On en déduit que $v^{\ell(p-1)} = 1$, donc $p^{n-1}|\ell(p-1)$, donc $p^{n-1}|\ell$ (d'après le théorème de Gauss, puisque p^{n-1} et $p-1$ sont premiers entre eux). Enfin, $v^\ell = 1$ et comme $(uv)^\ell = 1$, il vient aussi $u^\ell = 1$, ce qui implique que $p-1|\ell$. Enfin $p^{n-1}(p-1) = \varphi(p^n)|\ell$, d'où l'on déduit que uv engendre $(\mathbb{Z}/p^n\mathbb{Z})^*$.

Enfin, d'après le théorème Chinois, $(\mathbb{Z}/2p^n\mathbb{Z})^*$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p^n\mathbb{Z})^*$, lui même isomorphe à $(\mathbb{Z}/p^n\mathbb{Z})^*$ (car $(\mathbb{Z}/2\mathbb{Z})^*$ est le groupe à un seul élément) donc est cyclique

3. Ce sont $1, 2, 4$ et les nombres de la forme p^k ou $2p^k$ avec p premier distinct de 2 et $k \in \mathbb{N}^*$.

Exercice 2.5.

1. a) On a $v(x) = \overline{x}\,x \in x\mathbb{Z}[\tau]$. Soient $m, n \in \mathbb{Z}$, notons $r, s \in \{0, \dots, v(x)-1\}$ leurs restes ans la division euclidienne par $v(x)$. Alors $(m+n\tau) - (r+s\tau) \in x\mathbb{Z}[\tau]$. Cela prouve que tout élément de $\mathbb{Z}[\tau]/x\mathbb{Z}[\tau]$ est la classe d'un $r+s\tau$ avec $r, s \in \{0, \dots, v(x)-1\}$, donc $\mathbb{Z}[\tau]/x\mathbb{Z}[\tau]$ est fini.

b) Pour tout $z \in \mathbb{Z}[\tau]$, on a $z-(r_i+xs_j) \in xy\mathbb{Z}[\tau] \iff z-r_i \in x\mathbb{Z}[\tau]$ et $\dfrac{z-r_i}{x} - s_j \in y\mathbb{Z}[\tau]$. On en déduit qu'il existe un et un seul couple (i,j) tel que $z-(r_i+xs_j) \in xy\mathbb{Z}[\tau]$. L'application de $\{1, \dots, n\} \times \{1, \dots, m\}$ dans $\mathbb{Z}[\tau]/xy\mathbb{Z}[\tau]$ qui à (i,j) associe la classe de $r_i + xs_j$ est une bijection. On en déduit que $\mathbb{Z}[\tau]/xy\mathbb{Z}[\tau]$ a nm éléments, soit $v(xy) = v(x)v(y)$.

c) Pour $k \in \mathbb{Z}$, on a $a+b\tau \in k\mathbb{Z}[\tau] \iff a \in k\mathbb{Z}$ et $b \in k\mathbb{Z}$. Il y a donc k^2 classes : celles de $a+b\tau$ où $a, b \in \{0, \dots, k-1\}$. Notons que l'application $x \mapsto \overline{x}$ est un automorphisme de l'anneau $\mathbb{Z}[\tau]$. On en déduit que $v(x) = v(\overline{x})$. On a alors $v(x)^2 = v(x)v(\overline{x}) = v(x\overline{x}) = (x\,\overline{x})^2$, donc $v(x) = x\,\overline{x} = |x|^2$.

2. a) Soit $z \in \mathbb{Z}[\tau]$. Il existe q et r tels que $z = qx + r$ avec $V(r) < V(x)$. Par minimalité de $V(x)$, il vient $r \in \{0, -1, 1\}$. On en déduit que $\mathbb{Z}[\tau]/x\mathbb{Z}[\tau]$ a au plus 3 éléments, soit $v(x) \leqslant 3$.

b) On a $v(x) = (\operatorname{Re} x)^2 + (\operatorname{Im} x)^2 \leqslant 3$. On en déduit que $|\operatorname{Re} x| \leqslant \sqrt{3}$ et $|\operatorname{Im} x| \leqslant \sqrt{3}$. En particulier, $x \notin \mathbb{Z}$ (puisque $x \notin \{0, -1, 1\}$) et $\operatorname{Im} x \neq 0$. Or $x = a + b\tau$ avec $a, b \in \mathbb{Z}$. Il vient $|b| \geqslant 1$. Comme $|\operatorname{Im} x| = |b| \operatorname{Im} \tau$, il vient $\operatorname{Im} \tau \leqslant \sqrt{3}$.

Exercice 2.6.

1. Puisque $\alpha \in G$ et G est un sous-groupe de $(\mathbb{C}, +)$, il vient $\mathbb{Z}\alpha \subset G$, donc $\mathbb{Z}\alpha \subset G \cap \mathbb{R}\alpha$. Soit $t \in \mathbb{R}$ tel que $t\alpha \in G$ et notons n sa partie entière. Alors $t\alpha - n\alpha \in G$. Or $|t\alpha - n\alpha|^2 = |t-n|^2|\alpha|^2 < |\alpha|^2$; il vient $t\alpha - n\alpha = 0$ par minimalité de $|\alpha|$.

2. Posons $\dfrac{\beta}{\alpha} = u$. Puisque $|\alpha| \leqslant |\beta|$, il vient $|u| \geqslant 1$. Puisque $|\beta - \alpha| \geqslant |\beta|$, on a $|u-1| \geqslant |u|$, donc $\operatorname{Re} u \leqslant 1/2$; de même $|\beta + \alpha| \geqslant |\beta|$ donc $\operatorname{Re} u \geqslant -1/2$.

3. Posons $y = \dfrac{x}{\alpha}$. Soit n l'entier le plus proche de $\dfrac{\operatorname{Im} y}{\operatorname{Im} u}$. On a donc $\left|\dfrac{\operatorname{Im} y}{\operatorname{Im} u} - n\right| \leqslant 1/2$, soit $|\operatorname{Im}(y - nu)| \leqslant (\operatorname{Im} u)/2$.

Soit alors m l'entier le plus proche de $\operatorname{Re}(y - nu)$. On a $|\operatorname{Re}(y - nu - m)| \leqslant 1/2$. Il vient $|y - nu - m|^2 = |\operatorname{Re}(y - nu - m)|^2 + |\operatorname{Im}(y - nu)|^2 \leqslant 1/4(1 + (\operatorname{Im} u)^2) \leqslant |u|^2/2$. On a donc $|y - nu - m| < |u|$, soit $|x - (m\alpha + n\beta)| < |\beta|$.

Par minimalité de $|\beta|$, il vient $x - (m\alpha + n\beta) \in \mathbb{Z}\alpha$. Or $\left|\operatorname{Re}\dfrac{x - (m\alpha + n\beta)}{\alpha}\right| < 1$, donc $x = m\alpha + n\beta$.

5. Remarquons que m divise l'ordre de $(\mathbb{Z}/p^n\mathbb{Z})^*$ qui est égal à $\varphi(p^n) = (p-1)p^{n-1}$, donc d est de la forme p^k avec $k \leqslant n-1$.

Exercice 2.7.

1. On a $\tau\alpha \in J$ et $\tau\beta \in J$!
2. On a $\tau = a + b\dfrac{\beta}{\alpha}$ et, comme les parties imaginaires de τ et $\dfrac{\beta}{\alpha}$ sont positives, $b > 0$.
3. On a $M\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \tau\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$; donc τ est une valeur propre de M. L'autre valeur propre est donc $\overline{\tau}$ et les espaces propres respectifs sont $\mathbb{C}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ et $\mathbb{C}\begin{pmatrix}\overline{\alpha}\\ \overline{\beta}\end{pmatrix}$.

   La trace et le déterminant de cette matrice sont donc $a + d = \tau + \overline{\tau} = 1$ et $ad - bc = \tau\overline{\tau} = 5$. Comme a et d sont entiers et $a + d = 1$, ces deux nombres ne peuvent être strictement positifs ou strictement négatifs. Leur produit est négatif ou nul. Par ailleurs a et d ne sont pas de même parité (leur somme est impaire) donc ad est pair. Comme $ad - bc = 5$ est impair, bc est impair, bonc b et c sont impairs. Enfin, $4bc + (a - d)^2 = 4(bc - ad) + (a + d)^2 = -20 + 1 = -19$.
4. Divisant par α les égalités $\tau\alpha = a\alpha + b\beta$ et $\tau\beta = c\alpha + d\beta$, il vient $\begin{pmatrix}a + bx\\ c + dx\end{pmatrix} = \tau\begin{pmatrix}1\\ x\end{pmatrix}$. Ces deux vecteurs étant proportionnels, on obtient la nullité du déterminant. Donc
   a) $bx^2 + (a - d)x - c = 0$; l'autre racine du trinôme $bX^2 + (a - d)X - c$ est $\overline{x}$.
   b) Le produit $\overline{x}x$ de ces racines est $-\dfrac{c}{b}$, et la somme $x + \overline{x}$ des racines est $\dfrac{a - d}{b}$.
5. Ces inégalités proviennent des inégalités $|x| \geqslant 1$ et $|\operatorname{Re} x| \leqslant \dfrac{1}{2}$.
   - On a $-4bc \geqslant 4b^2$ et $(a - d)^2 \leqslant b^2$, donc $19 = -4bc - (a - d)^2 \geqslant 4b^2 - b^2 = 3b^2$.
   - Puisque b est impair et $3b^2 \leqslant 19$, il vient $b = 1$.
6. Donc $\beta = (\tau - a)\alpha$. On en déduit que le sous-groupe de J de base $(\alpha, \tau\alpha)$ contient β : c'est J. Par suite $J = \alpha\mathbb{Z}[\tau]$. Ceci étant vrai pour tout idéal, $\mathbb{Z}[\tau]$ est principal. D'après l'exercice 2.5, il n'est pas euclidien.

Exercice 2.8.

1. L'idéal J engendré par 2 et X est l'ensemble des $P \in \mathbb{Z}[X]$ tels que $P(0)$ est pair. Si $P \in J$ qui divise 2 alors $\partial P \leqslant \partial 2 = 0$, donc P est un polynôme constant, et comme $P \in J$ et $P|2$, il vient $P = \pm 2$; donc P ne divise pas X (dans $\mathbb{Z}[X]$). L'idéal J n'est pas engendré par P.
2. Remarquons que, si la partie imaginaire de τ est $> \sqrt{2}$, alors l'élément 2 est irréductible dans $\mathbb{Z}[\tau]$: si $2 = uv$ avec $u, v \in \mathbb{Z}[\tau]$, alors $u\overline{u}v\overline{v} = 4$ et puisque $u\overline{u}, v\overline{v} \in \mathbb{Z}[\tau] \cap \mathbb{R}_+ = \mathbb{N}$, $u\overline{u} \leqslant 2$, ou $v\overline{v} \leqslant 2$. La partie imaginaire de tout élément de $\mathbb{Z}[\tau]$ est un multiple de celle de τ qui est $> \sqrt{2}$. Donc si $u\overline{u} \leqslant 2$, alors $u \in \mathbb{Z}$, donc $u = \pm 1$. Donc 2 est bien irréductible. Si $\mathbb{Z}[\tau]$ est factoriel, une écriture $x\overline{x} = 2b$ avec $x \in \mathbb{Z}[\tau]$ et $b \in \mathbb{N}$ impose que 2 divise un des facteurs, donc $x/2 \in \mathbb{Z}[\tau]$.
   Si $\tau = i\sqrt{2k}$ avec $k \geqslant 2$, on a $\tau\overline{\tau} = 2k$; si $\tau = i\sqrt{2k + 1}$, avec $k \geqslant 1$, on a $(1+\tau)(1+\overline{\tau}) = 2(k+1)$, et puisque $\dfrac{\tau}{2} \notin \mathbb{Z}[\tau]$ et $\dfrac{1 + \tau}{2} \notin \mathbb{Z}[\tau]$. On en déduit que $\mathbb{Z}[\tau]$ n'est pas factoriel. Même raisonnement pour $\tau = \dfrac{1 + i\sqrt{15}}{2}$ vu que $\tau\overline{\tau} = 4$.

Exercice 2.9.

1. Si P est un polynôme non nul à coefficients dans K tel que $P(x) = 0$, alors $P \in K_1[X]$, donc x est algébrique sur K_1 !
2. Remarquons qu'un sous-anneau A de L contenant K et qui est un K-espace vectoriel de dimension finie est un corps. En effet, si $a \in A$ n'est pas nul, l'application K-linéaire $y \mapsto ay$ de A dans A est injective (vu que A est intègre : c'est un sous-anneau de l'anneau intègre K), donc bijective puisque A est de dimension finie ; il existe donc $b \in A$ tel que $ab = 1$, ce qui prouve que $a^{-1} \in A$.

Si x est algébrique sur K, alors l'ensemble $\{P(x);\ P \in K[X]\}$ est un sous-corps de L isomorphe à $K[X]/\varpi$ où ϖ est le polynôme minimal de x. Il est de dimension finie sur x et contient x.

Si A est un sous-anneau de L contenant K et x et qui est un K-espace vectoriel de dimension finie disons n. Alors $(1, x, \dots, x^n)$ sont liés : il existe donc un polynôme P de degré $\leqslant n$ tel que $P(x) = 0$.

3. Si K_2 est de dimension finie sur K, alors le K-espace vectoriel K_1 qui est un sous-K-espace vectoriel de K_2 est de dimension finie. Tout système générateur $(a_1, \dots, a_m) \in K_2^m$du K-espace vectoriel K_2 est un système générateur du K_1-espace vectoriel K.

   Inversement, soit $(a_1, \dots, a_p)$ une base du K espace vectoriel K_1 et $(b_1, \dots, b_q)$ une base du K_1-espace vectoriel K_2. On démontre que $(a_i b_j)_{1\leqslant i\leqslant p;\ 1\leqslant j\leqslant q}$ est une base du K-espace vectoriel K_2, ce qui démontrera que K_2 est un K-espace vectoriel de dimension pq.

   Soit $x \in K_2$. Il existe $(\mu_1, \dots, \mu_q) \in K_1^q$ tels que $x = \sum_{j=1}^{n} \mu_j b_j$ et, pour chaque j, il existe $(\lambda_{1,j}, \dots, \lambda_{p,j}) \in K^p$ tels que $\mu_j = \sum_{i=1}^{p} \lambda_{i,j} a_i$. on a alors $x = \sum_{j=1}^{q}\sum_{i=1}^{p} \lambda_{i,j} a_i b_j$ donc le système $(a_i b_j)_{1\leqslant i\leqslant p;\ 1\leqslant j\leqslant q}$ est générateur.

   Soient $(\lambda_{i,j}) \in K^{pq}$ tels que $\sum_{j=1}^{q}\sum_{i=1}^{p} \lambda_{i,j} a_i b_j = 0$; posons $\mu_j = \sum_{i=1}^{p} \lambda_{i,j} a_i$; il vient $\sum_{j=1}^{n} \mu_j b_j = 0$ et puisque (b_j) est libre (sur K_1) il vient $\mu_j = 0$ pour tout j ; enfin puisque (a_i) est libre (sur K) il vient $\lambda_{i,j} = 0$ pour tout i, j. Donc le système $(a_i b_j)_{1\leqslant i\leqslant p;\ 1\leqslant j\leqslant q}$ est libre.

4. a) On a $\alpha^{-1} \in K_1$, donc α^{-1} est algébrique.

   b) Comme β est algébrique sur K donc sur K_1, il existe un sous-corps K_2 de L contenant β et K_1 de dimension finie sur K_1 donc sur K. Alors $\alpha + \beta \in K_2$ et $\alpha\beta \in K_2$, donc $\alpha + \beta$ et $\alpha\beta$ sont algébriques sur K.

5. La première assertion est claire. Si x est algébrique sur K', il existe $P \in K'[X]$ non nul tel que $P(x) = 0$; écrivons $P = \sum_{k=0}^{n} a_k X^k$. On démontre immédiatement par récurrence sur $n \in \mathbb{N}$ qu'il existe un sous-corps K_1 de L contenant $a_0, \dots, a_n$ et K de dimension finie sur K. Alors x est algébrique sur K_1 donc sur K.

11.3 Polynômes et fractions rationnelles

Exercice 3.1. Si p/q est racine avec p et q premiers entre eux, on écrit $0 = q^n P(p/q) = \sum_{k=0}^{n} a_k p^k q^{n-k}$.

Comme p et q divisent cette somme, il vient $p|q^n a_0$ et $q|p^n a_n$, donc $p|a_0$ et $q|a_n$ d'après le théorème de Gauss.

Exercice 3.2. Successivement sur $\mathbb{Q}$ sur $\mathbb{R}$ et sur $\mathbb{C}$, on trouve

$$\begin{aligned} P &= (X-1)(X^2+5)(X^2-3X+1) \\ &= (X-1)(X-\frac{3+\sqrt{5}}{2})(X-\frac{3-\sqrt{5}}{2})(X^2+5) \\ &= (X-1)(X-\frac{3+\sqrt{5}}{2})(X-\frac{3-\sqrt{5}}{2})(X+i\sqrt{5})(X-i\sqrt{5}) \end{aligned}$$

Exercice 3.3. On trouve $F = \frac{2}{X^3} + \frac{4}{X^2} + \frac{7}{X} - \frac{7}{X-1} + \frac{3}{(X-1)^2}\cdot$ Donc une primitive de $t \mapsto F(t)$ est $t \mapsto -\frac{1}{t^2} - \frac{4}{t} - \frac{3}{t-1} + 7\ln\left|\frac{t}{t-1}\right| + c$ où c est une constante.

Exercice 3.4. Les conditions $P(0) = 1$ et $P'(0) = 0$ s'écrivent $P = 1 + aX^2 + bX^3$. On a alors $P(1) = 1 + a + b = 0$ et $P'(1) = 2a + 3b = 1$, donc $a = -4$ et $b = 3$.

Le polynôme $Q - P$ s'annule en 0 et en 1 ainsi que sa dérivée si et seulement s'il est divisible par $X^2(X-1)^2$. Donc les polynômes qui conviennent sont $1 - 4X^2 + 3X^3 + X^2(X-1)^2B$ avec $B \in K[X]$.

Exercice 3.5.

a) On a $\dfrac{1}{x^4 - x^2 - 2} = \dfrac{1}{3}\Big(\dfrac{1}{x^2-2} - \dfrac{1}{x^2+1}\Big) = \dfrac{1}{6\sqrt{2}}\Big(\dfrac{1}{x-\sqrt{2}} - \dfrac{1}{x+\sqrt{2}}\Big) - \dfrac{1}{3(x^2+1)}$. Une primitive est $x \mapsto \dfrac{1}{6\sqrt{2}} \ln\Big|\dfrac{x-\sqrt{2}}{x+\sqrt{2}}\Big| + \dfrac{1}{3}\mathrm{Arctan}\, x + c$.

b) On a $\displaystyle\int \frac{x\,dx}{(x^2+1)^2} = -\frac{1}{2(x^2+1)} + c$. Or, la dérivée de $x \mapsto \dfrac{x}{x^2+1}$ est $x \mapsto \dfrac{(x^2+1) - 2x^2}{(x^2+1)^2} = \dfrac{2}{(x^2+1)^2} - \dfrac{1}{x^2+1}$, donc $\displaystyle\int \frac{dx}{(x^2+1)^2} = \frac{x}{2(x^2+1)} + \frac{1}{2}\mathrm{Arctan}\, x + c$.

c) Posons $y = 1 - x$. On a $\dfrac{2-y}{(1-y)y^6} = \dfrac{1}{1-y} + \dfrac{2-y-y^6}{(1-y)y^6} = \dfrac{1}{1-y} + \dfrac{2+y+y^2+y^3+y^4+y^5}{y^6}$.
Donc $\displaystyle\int \frac{x+1}{x(x-1)^6} = \ln\Big|\frac{x}{x-1}\Big| + \frac{1}{1-x} + \frac{1}{2(1-x)^2} + \frac{1}{3(1-x)^3} + \frac{1}{4(1-x)^4} + \frac{2}{5(1-x)^5} + c$.

d) (Règles de Bioche : on pose $u = \sin x$) $\displaystyle\int \frac{dx}{\cos^3 x} = \int \frac{\cos x\,dx}{\cos^4 x} = \int \frac{du}{(1-u^2)^2}$.
Or $\dfrac{1}{(1-u^2)^2} = \dfrac{1}{4(u-1)^2} + \dfrac{1}{4(u+1)^2} + \dfrac{1}{4(u+1)} - \dfrac{1}{4(u-1)}$.
Donc $\displaystyle\int \frac{dx}{\cos^3 x} = \frac{1}{4}\ln\frac{1+\sin x}{1-\sin x} + \frac{1}{4}\Big(\frac{1}{1-\sin x} - \frac{1}{1+\sin x}\Big) + c$.

Exercice 3.6. On a

$$\begin{aligned} x^3+y^3+z^3-3xyz &= (x+y+z)((x^2+y^2+z^2)-(xy+yz+zx)) \\ &= (x+y+z)((x+y+z)^2 - 3(xy+yz+zx)). \end{aligned}$$

On en déduit que $3xyz = x^3+y^3+z^3-(x+y+z)((x+y+z)^2-3(xy+yz+zx)) = 15-3(9-3) = -3$. Donc x, y, z sont les trois racines du polynôme $X^3 - 3X^2 + X + 1$. Ce polynôme possède la racine « évidente » 1, donc $X^3 - 3X^2 + X + 1 = (X-1)(X^2-2X-1) = (X-1)(X-1-\sqrt{2})(X-1+\sqrt{2})$. Donc x, y, z sont égaux à permutation près à $1, 1+\sqrt{2}, 1-\sqrt{2}$.

Exercice 3.7. Notons d le PGCD de a et b.

1. Remarquons d'abord que, pour tout $p, q \in \mathbb{N}$, le polynôme $X^p - 1$ divise le polynôme $X^{pq} - 1$. Notons $a = bq + r$ la division euclidienne de a par b. On a $X^a - 1 = X^r(X^{bq} - 1) + X^r - 1$. Puisque $X^b - 1$ divise $X^r(X^{bq} - 1)$ et $r < b$, le reste de la division euclidienne de $X^a - 1$ par $X^b - 1$ est $X^r - 1$.
2. On peut supposer que $a \geqslant b > 0$. Effectuons l'algorithme d'Euclide : on obtient une suite décroissante $r_0 = a \geqslant r_1 = b > r_2 > \ldots > r_n = d$ tels que, pour $2 \leqslant j \leqslant n$, r_j soit le reste de la division euclidienne de r_{j-2} par r_{j-1} et r_n divise r_{n-1}. On déduit de la question 1, que le reste de la division euclidienne de $X^{r_{j-2}} - 1$ par $X^{r_{j-1}} - 1$ est $X^{r_j} - 1$; de plus $X^{r_n} - 1$ divise $X^{r_{n-1}} - 1$. D'après l'algorithme d'Euclide, le PGCD de $X^a - 1$ et $X^b - 1$ est donc $X^d - 1$.
3. Donnons-nous une relation de Bézout $au - bv = d$. On a donc $(X^{au} - 1) - X^d(X^{bv} - 1) = X^d - 1$. Puisque $X^a - 1$ divise $X^{au} - 1$ et $X^b - 1$ divise $X^{bv} - 1$ cette égalité est une relation de Bézout.

4. Les polynômes A et B sont scindés à racines simples sur $\mathbb{C}$. Les racines communes sont les $\lambda \in \mathbb{C}$ tels que $\lambda^a = \lambda^b = 1$ c'est à dire les éléments de $\mathbb{C}^*$ dont l'ordre dans le groupe $\mathbb{C}^*$ divise à la fois a et b, *i.e.* qui divise d. On en déduit que le PGCD de A et B vus comme polynômes sur $\mathbb{C}$ est $\prod_{k=0}^{d-1}(X - e^{\frac{2ik\pi}{d}}) = X^d - 1$.
Pour finir, démontrons le résultat fort utile suivant :

Théorème. *Soit L un corps commutatif et K un sous-corps de L. Soient $A, B \in K[X]$. Notons D leur PGCD vus comme polynômes sur K. Alors D est le PGCD de A et B vus comme polynômes sur L.*

Démonstration. On a une relation de Bézout $D = AU + BV$ avec $U, V \in K[X] \subset L[X]$, et puisque D est un diviseur commun de A et B (sur K donc sur L) c'est leur PGCD. □

Exercice 3.8.

1. Notons $\lambda_1, \ldots, \lambda_k$ les racines de P de partie imaginaire strictement positive écrites avec leur multiplicité. On a $P = \prod_{j=1}^{k}(X - \lambda_j)(X - \overline{\lambda_j}) = A\overline{A}$ où $A = \prod_{j=1}^{k} X - \lambda_j$. Les polynômes A et $\overline{A}$ n'ont pas de racines communes : ils sont premiers entre eux.
2. Existence : Comme A et $\overline{A}$ sont premiers entre eux, il existe $U, V \in \mathbb{C}[X]$ tels que $AU + \overline{A}V = 1$. Alors AU est congru à 1 modulo $\overline{A}$, donc $i(1 - 2AU)$ est congru à i modulo A, et à $-i$ modulo $\overline{A}$. Écrivons $i(1 - 2AU) = PQ + J$ la division euclidienne de $i(1 - 2AU)$ par P. Alors J convient.
Unicité : Si J_1 et J_2 vérifient ces conditions alors $J_1 - J_2$ est divisible par A et $\overline{A}$ donc par leur PPCM qui est P - puisque A et $\overline{A}$ sont premiers entre eux. Comme $J_1 - J_2$ est de degré $< 2k$, il vient $J_1 - J_2 = 0$.
3. Le polynôme $\overline{J}$ vérifie les mêmes conditions : écrivons $J - i = AB$: et $J + i = \overline{A}C$ il vient $\overline{J} + i = \overline{AB}$ et $\overline{J} - i = A\overline{C}$. Donc $J = \overline{J}$ (d'après l'unicité) soit $J \in \mathbb{R}[X]$.
Enfin $J^2 \equiv -1$ modulo A et modulo $\overline{A}$ donc $J^2 \equiv -1$ $[P]$.
4. Il s'agit de vérifications plutôt longues - mais sans surprises...
5. Soit $P \in \mathbb{R}[X]$ un polynôme unitaire annulateur de f sans racines réelles : par exemple le polynôme minimal ou le polynôme caractéristique de f. Soit $J \in \mathbb{R}[X]$ comme ci-dessus. On pose $j = J(f)$. Puisque $P | J^2 + 1$, il vient $j^2 = -\mathrm{id}_E$; enfin $fJ(f) = J(f)f$, d'où le résultat.

Exercice 3.9.

1. Si A et B sont deux polynômes, on a $\frac{(AB)'}{AB} = \frac{A'}{A} + \frac{B'}{B}$. Décomposons P en facteurs irréductibles : $P = a\prod_{i=1}^{k} P_i^{m_i}$. On a $\frac{P'}{P} = \sum_{i=1}^{k} \frac{m_i P_i'}{P_i}$.
2. *Théorème de Lucas.* Écrivons $P = a\prod_{i=1}^{k}(X - \lambda_i)^{m_i}$. Si z est une racine de P' qui n'est pas un des λ_i, on a
$$0 = \frac{P'(z)}{P(z)} = \sum_{i=1}^{k} \frac{m_i}{z - \lambda_i} = \sum_{i=1}^{k} \frac{m_i\overline{(z - \lambda_i)}}{|z - \lambda_i|^2}.$$
Prenant le complexe conjugué de cette égalité, on trouve $\sum_{i=1}^{k} \frac{m_i(z - \lambda_i)}{|z - \lambda_i|^2} = 0$, donc z est barycentre des λ_i affectés des coefficients strictement positifs $\frac{m_i}{|z - \lambda_i|^2}$.

3. a) Le triplet $(1, j, j^2)$ est un repère affine d'où l'existence et unicité de ℓ. Toute application affine est de cette forme... On peut aussi résoudre le système et trouver $a = \dfrac{\alpha + j^2\beta + j\gamma}{3}$, $b = \dfrac{\alpha + j\beta + j^2\gamma}{3}$ et $c = \dfrac{\alpha + \beta + \gamma}{3}$.

   Pour $z = 1, j, ouj^2$, posons $u = az$ et $v = b\overline{z}$. Écrivant $(u+v)^3 = 3uv(u+v) + u^3 + v^3$, on trouve immédiatement que α, β et γ sont racines de $(X-c)^3 - 3ab(X-c) - a^3 - b^3$.

   b) Convenons d'appeler *ellipse de Steiner* d'un triangle toute ellipse tangente au milieu des trois côtés du triangle. Nous devons donc établir l'existence et unicité d'une ellipse de Steiner.
   - La transformation ℓ transforme le cercle inscrit $\mathcal{C}$ du triangle équilatéral $(1, j, j^2)$ en une ellipse de Steiner - d'où son existence.
   - Si $\mathcal{E}$ est une ellipse de Steiner du triangle $T = (\alpha, \beta, \gamma)$, il existe une transformation affine ℓ' telle que $\ell'(\mathcal{E})$ soit un cercle. C'est le cercle inscrit du triangle $\ell'(T)$, et une ellipse de Steiner pour ce triangle. Notons (A, B, C) le triangle $\ell'(T)$ et A', B', C' les milieux et points de tangence. On a $AC' = BC'$, $AB' = CB'$ et $BA' = CA'$ (milieu) et $AB' = AC'$, $BA' = BC'$ et $CA' = CB'$ (cercle inscrit). Donc $\ell'(T)$ est équilatéral. Alors, $\ell' \circ \ell$ est une similitude, donc $\ell' \circ \ell(\mathcal{C})$ est le cercle inscrit $\ell'(\mathcal{E})$, donc $\mathcal{E} = \ell(\mathcal{C})$, d'où l'unicité.

   Enfin, écrivons $a = |a|uv$ et $b = |b|u\overline{v}$ où u et v sont des nombres complexes de module 1. On a $\ell = T_c \circ R_u \circ D \circ R_v$ où R_u, R_v sont des rotations $R_v(z) = vz$, $R_u(z) = uz$, T_c est la translation $T(z) = z + c$; enfin $D(z) = |a|z + |b|\overline{z}$, soit $D(x+iy) = (|a|+|b|)x + i(|a|-|b|)y$. Notons que comme α, β, γ ne sont pas alignés, ℓ est bijective, donc $|a| \neq |b|$.

   On a $R_v(\mathcal{C}) = \mathcal{C}$; l'image par D de ce cercle de centre 0 et de rayon $1/2$ est l'ellipse d'équation $\left(\dfrac{x}{|a|+|b|}\right)^2 + \left(\dfrac{y}{|a|-|b|}\right)^2 = \dfrac{1}{4}$; ses foyers ont donc comme coordonnées $y = 0$ et $x = \pm\dfrac{\sqrt{(|a|+|b|)^2 - (|a|-|b|)^2}}{2} = \pm\sqrt{|ab|}$.

   Enfin $T_c \circ R_u$ est une isométrie donc les foyers de l'ellipse de Steiner ont pour affixes $c \pm u\sqrt{|ab|} = c \pm z$ où z est une racine carrée de $ab = u^2|ab|$.

Dans une ellipse d'équation $\dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} = 1$ (dans un repère orthonormé) de demi grand axe a et demi petit axe b (avec $a > b > 0$), les foyers ont pour coordonnées $(\pm\sqrt{a^2 - b^2}, 0)$. Pour se le rappeler, notons $A = (a, 0)$ et $B = (0, b)$. Si F et F' sont les foyers de coordonnées $(\pm c, 0)$, on a $AF + AF' = 2a = BF + BF' = 2\sqrt{b^2 + c^2}$.

Exercice 3.10. Fixons un repère orthonormé $(0, i, j)$ dans lequel l'équation de H soit $xy = c$. Notons (p, q) les coordonnées de P dans ce repère. On a $c = pq$. Celles de P' sont donc $(-p, -q)$. Quitte à changer i en son opposé, on peut supposer que $p > 0$. L'équation du cercle $\mathcal{C}$ est $x^2 + y^2 - 2px - 2qy = 3(p^2 + q^2)$. Le point de coordonnées (x, y) est dans l'intersection $H \cap \mathcal{C}$ si et seulement si $xy = pq$ et $x^2 + y^2 - 2px - 2qy = 3(p^2 + q^2)$. Multipliant par x^2, on trouve (puisque $xy = pq$)

$$x^4 + p^2q^2 - 2px^3 - 2pq^2x - 3(p^2 + q^2)x^2 = 0.$$

Posons $g(x) = x^4 - 2px^3 - 3(p^2 + q^2)x^2 - 2pq^2x + p^2q^2$. Les points d'intersection de $H \cap \mathcal{C}$ sont les couples $(x, \dfrac{pq}{x})$, avec $x \in \mathbb{R}^*$ racine de g. On sait déjà que $-p$ est un racine de cette équation.

1. On a $g(0) = p^2q^2 > 0$ et $g(p) = -p^2(p^2 + q^2) < 0$, enfin $\lim\limits_{x \to \pm\infty} g(x) = +\infty$. On en déduit que g a une racine dans $]0, p[$, une racine dans $]p, +\infty[$ et un nombre pair de racines (avec leur multiplicité) dans $]-\infty, 0[$. Comme $-p$ est racine, ce polynôme du 4e degré est scindé sur $\mathbb{R}$.
2. Les trois autres racines satisfont $x_A + x_B + x_C - p = 2p$, donc $x_A + x_B + x_C = 3p$. Par symétrie $(x, y) \mapsto (y, x)$, on trouve que les ordonnées des points d'intersection vérifient $y_A + y_B + y_C = 3q$. [Ou, mieux, $y_A + y_B + y_C - q = \dfrac{pq}{x_A} + \dfrac{pq}{x_B} + \dfrac{pq}{x_C} - \dfrac{pq}{p} = \dfrac{pq\sigma_3}{\sigma_4} = 2q$.] Cela prouve que P est le centre de gravité du triangle ABC. Par ailleurs, P étant le centre du cercle circonscrit du triangle ABC, médianes et médiatrices sont confondues. Donc ABC est équilatéral.

Exercice 3.11.

1. a) Le plus simple est d'utiliser la matrice compagnon de P : c'est une matrice à coefficients entiers $A \in M_n(\mathbb{Z})$ dont le polynôme caractéristique est $(-1)^n P$. Alors le polynôme caractéristique de A^ℓ est $(-1)^n P_\ell$ (il suffit pour voir cela de trigonaliser A). Il est à coefficients entiers.

   b) On sait que $(-1)^{n-j}a_j$ est la somme des produits $x_{i_1}\dots x_{i_j}$ où $1 \leqslant i_1 < i_2 < \dots < i_j \leqslant n$. Il y en a $\binom{n}{j}$ tous de module 1.

   On peut aussi raisonner par récurrence sur n, écrivant $Q = (X - x_n)Q_1$ où $Q_1 = \prod_{j=1}^{n-1} X - x_j$.

   Si on écrit $Q_1 = \sum_{j=0}^{n} b_j X_j$ (avec $b_n = 1$), on a $a_0 = -x_n b_0$ et, pour $j \neq 1$, $a_j = b_{j-1} - x_n b_j$.

   Donc $|a_0| \leqslant 1$ (en fait $|a_0| = 1$) et $|a_j| \leqslant |b_j| + |b_{j-1}|$; d'après l'hypothèse de récurrence, il vient $|a_j| \leqslant \binom{n-1}{j} + \binom{n-1}{j-1} = \binom{n}{j}$.

   c) D'après b), il y a un nombre fini de polynômes unitaires de degré n à coefficients entiers dont toutes les racines (complexes) sont de module 1. L'application ℓ mapsto P_ℓ n'est donc pas injective.

   d) On a $\prod_{k=1}^{n} X - x_k^\ell = \prod_{k=1}^{n} X - x_k^m$. L'énoncé résulte de l'unicité de la décomposition en facteurs irréductibles.

   e) Établissons cette propriété par récurrence sur r. Elle est vraie pour $r = 0$ et 1. Supposons-la vérifiée pour r. Soit alors $k \in \{1, \dots, n\}$ et posons $j = \sigma(k)$. On a

   $$(x_k)^{\ell^{r+1}} = (x_k^\ell)^{\ell^r} = (x_j^m)^{\ell^r} = (x_j^{\ell^r})^m = \left(x_{\sigma^r(j)}^{m^r}\right)^m = x_{\sigma^{r+1}(k)}^{m^{r+1}}.$$

   f) Notons r l'ordre de la permutation σ. On a $x_k^{m^r - \ell^r} = 1$.

   Remarque. En utilisant le fait que les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$, on peut en déduire que P est un produit de polynômes cyclotomiques.

2. En effet, il existe $Q \in \mathbb{Z}[X]$ unitaire de degré $2n$ tel que $x^n P(x + 1/x) = Q(x)$ pour tout $x \in \mathbb{C}^*$. Écrivant $P = \prod_{j=1}^{n}(X - b_j)$, on a $Q = \prod_{j=1}^{n}(X^2 - b_j X + 1)$. Puisque on a $b_j \in \mathbb{R}$ et $|b_j| \leqslant 2$, le polynôme $X^2 - b_j X + 1$ a deux racines complexes conjuguées x_j et $\overline{x}_j$ de module 1 (éventuellement toutes deux égales à 1 ou -1).

   D'après ce qui précède, x_j est une racine de l'unité $x_j = e^{iq_j\pi}$ avec $q_j \in \mathbb{Q}$, donc $b_j = x_j + \overline{x}_j = 2\cos q_j\pi$.

3. Les racines du polynôme caractéristique de A sont réelles et comprises entre -2 et 2. Elles sont donc de la forme $2\cos q\pi$ avec $q \in \mathbb{Q}$ d'après la question précédente.

Exercice 3.12.

1. Si f est surjective, il existe $P \in E_n$ et $Q \in E_m$ tels que $f_{A,B}(P, Q) = 1$ donc A et B sont premiers entre eux. Donc (ii)⇒(i).

   Si A et B sont premiers entre eux et $f_{A,B}(P, Q) = 0$, alors $AP = -BQ$; ce polynôme est un multiple commun de A et B, donc de leur PPCM AB. Comme son degré est $< m + n$, il est nul, donc $P = Q = 0$; l'application linéaire f est alors injective, donc surjective par égalité des dimensions. Donc (i)⇒(ii).

   La matrice de $f_{A,B}$ de la base $\mathcal{B}_0 = ((1,0),(X,0),\dots,(X^{n-1},0),(0,1),(0,X),\dots,(0,X^{m-1}))$ de $E_n \times E_m$ dans la base $\mathcal{B}_1 = (1, X, \dots, X^{m+n-1})$ de E_{n+m} est la matrice carrée de colonnes $C_0, \dots, C_{n-1}, D_0, \dots, D_{m-1}$. L'équivalence (ii) $\iff$ (iii) en résulte.

2. Le polynôme A a des racines multiples si et seulement si A et A' ne sont pas premiers entre eux, donc si et seulement si $\mathrm{Res}_{A,A'} = 0$.

3. a) Dans ce cas $\mathrm{Res}_{A,B} = \begin{vmatrix} c & b & 0 \\ b & 2a & b \\ a & 0 & 2a \end{vmatrix} = -a(b^2 - 4ac)$.

   b) On a $\mathrm{Res}_{A,B} = \begin{vmatrix} q & 0 & p & 0 & 0 \\ p & q & 0 & p & 0 \\ 0 & p & 3 & 0 & p \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix} = 4p^3 + 27q^2$.

   c) Démontrons par récurrence sur le degré n de A que $\mathrm{Res}_{A,X-b} = A(b)$.

   Pour $n = 1$, on a $\mathrm{Res}(a_0 + a_1X, X - b) = \begin{vmatrix} a_0 & -b \\ a_1 & 1 \end{vmatrix} = a_0 + a_1b$.

   Écrivons $A = \sum_{k=0}^{n} a_kX^k = a_0 + XA_1$, où $A_1 = \sum_{k=1}^{n} a_kX^{k-1}$.

   On a

$$\mathrm{Res}(A, X - b) = \begin{vmatrix} a_0 & -b & 0 & \dots & 0 & 0 \\ a_1 & 1 & -b & \dots & 0 & 0 \\ a_2 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1} & 0 & 0 & \dots & 1 & -b \\ a_n & 0 & 0 & \dots & 0 & 1 \end{vmatrix}.$$

   Développant par la première ligne, il vient $\mathrm{Res}(A, X - b) = a_0 + b\mathrm{Res}(A_1, X - b)$. D'après l'hypothèse de récurrence il vient $\mathrm{Res}(A, X - b) = a_0 + bA_1(b) = A(b)$.

   NB On peut aussi développer par rapport à la dernière ligne, ou la première colonne...

   On peut aussi effectuer un changement de base :

   Considérons la base $\mathcal{B}_2 = (1, X-b, X(X-b), X^2(X-b), \dots, X^{n-1}(X-b))$. Décomposons A dans cette base en écrivant $A = A(b) + \sum_{k=0}^{m-1} \alpha_kX^k(X - b)$. La matrice de passage de $\mathcal{B}_1$ à $\mathcal{B}_2$ est triangulaire supérieure avec des 1 sur la diagonale. Donc $\mathrm{Res}_{A,B}$ est égal au déterminant de la matrice de f allant de la base $\mathcal{B}_0$ dans la base $\mathcal{B}_2$:

$$Mat_{\mathcal{B}_2,\mathcal{B}_0}(f) = \begin{pmatrix} A(b) & 0 & 0 & \dots & 0 \\ \alpha_0 & 1 & 0 & \dots & 0 \\ \alpha_1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1} & 0 & 0 & \dots & 1 \end{pmatrix}$$

   donc $\mathrm{Res}_{A,(X-b)} = A(b)$.

4. a) Echanger A et B revient à permuter les colonnes de la matrice par la permutation σ définie par $\sigma(i) = m + i$ si $1 \leqslant i \leqslant n$ et $\sigma(i) = i - n$ si $n + 1 \leqslant i \leqslant m + n$. La signature de cette permutation est $(-1)^{mn}$.

   b) Remplacer B par bB revient à multiplier les m dernières colonnes par b.

   c) À l'aide de (b), on peut supposer que B_1 est unitaire. Notons n_1 et n_2 les degrés respectifs de B_1 et B_2 et posons $B = B_1B_2$ et $n = n_1 + n_2$.

   Considérons les applications linéaires

$$\begin{array}{lll} \varphi : E_{n_1} \times E_{n_2} \times E_m \to E_n \times E_m, & \text{définie par} & \varphi(P_1, P_2, Q) = (P_1 + B_1P_2, P) \\ g : E_{n_1} \times E_{n_2} \times E_m \to E_{n_1} \times E_{m+n_2}, & \text{définie par} & g(P_1, P_2, Q) = (P_1, AP_2 + B_2Q) \\ h : E_{n_1} \times E_{m+n_2} \to E_{m+n}, & \text{définie par} & h(P_1, R) = AP_1 + B_1R, \end{array}$$

de sorte que $f_{A,B} \circ \varphi = h \circ g$.

On considère les matrices de ces applications dans les bases $\mathcal{B}_0$ de $E_n \times E_m$ et et $\mathcal{B}_1$ de E_{m+n}, ainsi que les bases analogues $\hat{\mathcal{B}}$ de $E_{n_1} \times E_{m+n_2}$ et $\tilde{\mathcal{B}}$ de $E_m \times E_{n_1} \times E_{n_2}$:

$$\hat{\mathcal{B}} = ((1,0),(X,0),\ldots,(X^{n_1-1},0),(0,1),(0,X),\ldots,(0,X^{m+n_2-1}))$$

$$\tilde{\mathcal{B}} = ((1,0,0),(X,0,0),\ldots,(X^{m-1},0,0),(0,1,0),\ldots,(0,X^{n_1-1},0),(0,0,1),\ldots,(0,0,X^{n_2-1}))$$

Dans ces bases :

- la matrice $Mat(\varphi)$ de φ est triangulaire supérieure avec des 1 sur la diagonale et son déterminant vaut 1 (car le polynôme B_1 est supposé unitaire) ;
- la matrice $Mat(g)$ de g est diagonale par blocs $Mat(g) = \begin{pmatrix} I_{n_1} & 0 \\ 0 & Mat(f_{A,B_2}) \end{pmatrix}$; son déterminant vaut R_{A,B_2} ;
- celle de h est triangulaire par blocs de la forme $Mat(h) = \begin{pmatrix} Mat(f_{A,B_2}) & Q \\ 0 & T \end{pmatrix}$ où T est triangulaire supérieure avec des 1 sur la diagonale et son déterminant vaut 1 (car B_1 est supposé unitaire).

Les formules (d), (e) et (f) en résultent facilement.

Exercice 3.13.

1. Tout diviseur commun de P_{k+1} et P_k divise $P_{k-1} = Q_{k+1}P_k - P_{k+1}$, donc il divise P_{k-2} et par récurrence, il divise P et P'. Or P et P' sont supposés premiers entre eux.
2. Sur tout intervalle ne rencontrant pas A, les polynômes P_k gardent un signe constant. Le dernier reste non nul est le pgcd de P et P'. Il est constant (et non nul).
3. Puisque P_k et P_{k+1} sont premiers entre eux, ils n'ont pas de racines communes, donc $P_{k+1}(x) \neq 0$. Comme $P_{k-1}(x) = Q_{k+1}(x)P_k - P_{k+1}(x) = -P_{k+1}(x)$, $P_{k-1}(x)$ et $P_{k+1}(x)$ sont non nuls et (de signes) opposés. L'ensemble A est fini. Il existe donc un intervalle ouvert J contenant x tel que $J \cap A = \{x\}$.
   a) Sur l'intervalle J les polynômes P_{k-1} et P_{k+1} gardent des signes contraires ; donc pour $y \in J \setminus \{x\}$, quel que soit le signe de $P_k(y)$, le nombre de changements de signe dans la suite $P_{k-1}(y), P_k(y), P_{k+1}(y)$ est égal à 1.
   b) Notons $N_x = \{k;\ \ 1 \leqslant k < m;\ P_k(x) = 0\}$ et écrivons $N_x = \{k_1,\ldots,k_r\}$, avec $r \geqslant 1$ et $0 < k_1 < \ldots < k_r < m$. Par (a), si $r \geqslant 2$ et $1 \leqslant j < r$, alors $k_{j+1} \geqslant k_j + 2$; de plus, pour $y \in J \setminus \{x\}$, $n(y)$ est le nombre de changements de signes dans la suite formée de $P_j(y)$ pour $j \notin N_x$. Il est constant sur J.
4. Comme ci-dessus, posons $N_x = \{k,\ 1 \leqslant k < m;\ P_k(x) = 0\}$. Par 3.a), $1 \notin N_x$ et le nombre n_0 de changements de signes dans la suite formée de $P_j(y)$ pour $1 \leqslant j \leqslant m,\ j \notin N_x$ est constant sur J. De plus, si $P'(x) > 0$ (*resp.* $P'(x) < 0$), alors P est croissante (*resp.* décroissante) sur J, donc pour $y \in J$, $P(y)$ est de même signe que $P'(y)$ si $y > x$ et de signe opposé si $y < x$. Il s'ensuit que $n_d(x) = n_0$ et $n_g(x) = n_0 + 1$.
5. Notons $x_1 < \ldots < x_p$ les points de $A \cap]a,b[$. On a $n(a) = n_g(x_1)$, $n_d(x_j) = n_g(x_{j+1})$ et $n_d(x_p) = n(b)$. Donc $n(a) - n(b) = \sum_{j=1}^{p} n_g(x) - n_d(x)$. Notons $B \subset A$ l'ensemble des racines de P. On a $n_g(x) - n_d(x) = 0$ si $x \notin B$ et $n_g(x) - n_d(x) = 1$ pour $x \in B$. Le théorème de Sturm en résulte.

Exercice 3.14.

1. Écrivons $P = \prod_{i=1}^{4} X - z_i = X^4 - aX^3 + bX^2 - cX + d$ et $\prod_{i=1}^{3} X - u_i = X^3 - \alpha X^2 + \beta X - \gamma$ où $a = z_1+z_2+z_3+z_4$, $b = z_1z_2+z_1z_3+z_1z_4+z_2z_3+z_2z_4+z_3z_4$, $c = z_1z_2z_3+z_1z_2z_4+z_1z_3z_4+z_2z_3z_4$ et $d = z_1z_2z_3z_4$; $\alpha = u_1+u_2+u_3$, $\beta = u_1u_2+u_1u_3+u_2u_3$ et $\gamma = u_1u_2u_3$.
On trouve

$$\begin{aligned}
\alpha &= b \\
\beta &= z_1^2(z_2z_3+z_2z_4+z_3z_4) + z_2^2(z_1z_3+z_1z_4+z_3z_4) + z_3^2(z_1z_2+z_1z_4+z_2z_4) + \\
&\qquad + z_4^2(z_1z_2+z_1z_3+z_2z_3) \\
&= ac - 4d \\
\gamma &= z_1^2z_2^2z_3^2 + z_1^2z_2^2z_4^2 + z_1^2z_3^2z_4^2 + z_2^2z_3^2z_4^2 + z_1^3z_2z_3z_4 + z_1z_2^3z_3z_4 + z_1z_2z_3^3z_4 + z_1z_2z_3z_4^3 \\
&= (c^2 - bd) + (a^2 - 2b)d
\end{aligned}$$

2. Une fois trouvé les u_i, on peut trouver $(z_1+z_2)(z_3+z_4) = u_2+u_3$, et puisque on connait aussi $z_1+z_2+z_3+z_4 = a$ on trouve z_1+z_2 et z_3+z_4. De même on trouve z_i+z_j pour $i \neq j$. Donc on trouve enfin $2z_1 = (z_1+z_2)+(z_1+z_3)+(z_1+z_4)-a$.

Exercice 3.15.

1. D'après le (petit) théorème de Fermat, tout élément de $\mathbb{F}_p$ est racine du polynôme $X^p - X$. Donc $\prod_{x\in\mathbb{F}_p}(X-x)$ divise $X^p - X$. Ces polynômes sont donc égaux car ils sont unitaires et ont même degré.
2. On a donc $X^{p-1} - 1 = \prod_{x\in\mathbb{F}_p^*}(X-x)$, et prenant la valeur en 0, il vient $-1 \equiv (-1)^{p-1}(p-1)!\ \ [p]$.

Exercice 3.16.

1. Notons $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ la réduction modulo p. C'est un morphisme d'anneaux. Si p divise tous les c_k, on a $\pi(AB) = 0$, et comme $\mathbb{F}_p[X]$ est intègre il vient $\pi(A) = 0$ ou $\pi(B) = 0$.
2. Si $c(A) = c(B) = 1$, aucun nombre premier ne divise tous les a_j ou tous les b_j. Donc par 1., aucun nombre premier ne divise tous les c_j, donc $c(AB) = 1$. Dans le cas général, on peut écrire $A = c(A)A_1$ et $B = c(B)B_1$ avec $A_1, B_1 \in \mathbb{Z}[X]$ de contenu 1. On a alors $AB = c(A)c(B)A_1B_1$ et donc $c(AB) = c(A)c(B)c(A_1B_1) = c(A)c(B)$.
3. Il existe $a, b \in \mathbb{N}^*$ tels que $aA \in \mathbb{Z}[X]$ et $bB \in \mathbb{Z}[X]$ (prendre les PPCM des dénominateurs des coefficients de A et B respectivement). Écrivons $aA = c(aA)A_1$ et $bB = c(bB)B_1$. Posons $q = \dfrac{a}{c(aA)}$ et $q' = \dfrac{b}{c(bA)}$ de sorte que $qA = A_1 \in \mathbb{Z}[X]$ et $q'B = B_1 \in \mathbb{Z}[X]$. On a alors $c(aA)c(bB) = c(abAB) =) = abc(AB)$ de sorte que $qq'c(AB) = 1$ et $\dfrac{1}{q} = q'c(AB)$. Donc $\dfrac{1}{q}B = c(AB)B_1 \in \mathbb{Z}[X]$.
4. Soit $P \in \mathbb{Z}[X]$ non scalaire. Si P n'est pas irréductible sur $\mathbb{Q}$, il existe $A, B \in \mathbb{Q}[X]$ non scalaires tels que $AB = P$. D'après la question précédente, P est produit de polynômes qA et $\dfrac{1}{q}B$ à coefficients dans $\mathbb{Z}$ donc P n'est pas irréductible sur $\mathbb{Z}$.

Exercice 3.17. Supposons que $P = AB$ avec $A, B \in \mathbb{Q}[X]$. Alors, d'après l'exercice 3.16, il existe $q \in \mathbb{Q}^*$ tel que $A_1 = qA \in \mathbb{Z}[X]$ et $B_1 = \dfrac{1}{q}B \in \mathbb{Z}[Z]$ Remarquons que le coefficient directeur de P étant le produit des coefficients directeurs de A_1 et B_1, on en déduit que ceux-là ne sont pas divisibles par p. Remarquons aussi que, puisque $P_1(0) = A_1(0)B_1(0)$, l'un de ces deux nombres n'est pas divisible par p, par exemple $A_1(0)$.

Notons $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ la réduction modulo p. C'est un morphisme d'anneaux. On a $\pi(P) = \pi(A_1)\pi(B_1)$. Or $\pi(P_1)$ est associé à un X^n. D'après l'unicité de la décomposition en polynômes irréductibles dans $\mathbb{F}_p(X)$, on en déduit que $\pi(A_1)$ est de la forme vX^k avec $v \in \mathbb{F}_p^*$ et donc ne peut avoir deux coefficients non nuls. Or, le coefficient directeur et le coefficient constant de $\pi(A_1)$ sont non nuls : cela impose que le degré de A_1 est 0.

Application. Posons $P = \Phi_p(X+1)$. On a $(X-1)\Phi_p = X^p - 1$, donc $XP = (X+1)^p - 1$. Il vient $X\pi(P) = X^p + 1 - 1 = X^p$, donc $\pi(P) = X^{p-1}$. Par ailleurs $P(0) = \Phi_p(1) = p$. On peut appliquer le critère d'Eisenstein : P est irréductible sur $\mathbb{Q}$, donc Φ_p est irréductible sur $\mathbb{Q}$.

Exercice 3.18.

1. Les racines multiples sont les racines du pgcd de P et P'.
2. Comme $X^p - X = \prod_{a \in \mathbb{F}_p} X - a$, le pgcd de P et $X^p - X$ est le produit des $X - a$ pour a racine de P.
3. a) On pose $A = \mathrm{pgcd}(P, X^{\frac{p+1}{2}} - X)$ et $B = \mathrm{pgcd}(P, X^{\frac{p-1}{2}} + 1)$.
   b) Pour $x \in \mathbb{F}_p^*$, on a $x^{\frac{p-1}{2}} \in \{-1, 1\}$. On a donc l'équivalence entre les assertions suivantes
      (i) Q sépare a et b ;
      (ii) $(a-c)^{\frac{p-1}{2}} \neq (b-c)^{\frac{p-1}{2}}$;
      (iii) $\left(\frac{c-a}{c-b}\right)^{\frac{p-1}{2}} = -1$;
      (iv) $\frac{c-a}{c-b}$ n'est pas un carré.

      L'application $c \mapsto \frac{c-a}{c-b}$ est une bijection de $\mathbb{F}_p \setminus \{a, b\}$ sur $\mathbb{F}_p \setminus \{0, 1\}$. Donc on a bien (un peu plus d') une chance sur deux de séparer a et b en prenant c au hasard.
   c) En prenant c au hasard puis en regardant le pgcd de P et $Q_c = (X-c)^{\frac{p-1}{2}} - 1$ on a beaucoup de chances de se retrouver avec deux facteurs de degré plus petit. Puis on recommence avec un nouveau c...

Exercice 3.19. Solution très rapide...

1. a) est clair une fois que l'on remarque que m et n étant premiers entre eux, si mn a des facteurs carrés, alors m ou n aussi.
   b) On démontre que, pour tout $n \in \mathbb{N}^*$, les matrices $U = (u_{i,j}) \in M_n(\mathbb{C})$ et $V = (v_{i,j}) \in M_n(\mathbb{C})$ définie par $u_{i,j} = 1$ si $j|i$ et 0 sinon et $v_{i,j} = \mu(i/j)$ si $i \neq j$ sont inverse l'une de l'autre. En effet, $UV = (w_{i,j})$, où $w_{i,j} = \sum_k u_{i,k}v_{k,j}$. Donc $w_{i,j} = 0$ si j ne divise pas i, $w_{i,i} = 1$ et, pour $q \in \mathbb{N}$, $q \geqslant 2$, on a $w_{jq,j} = \sum_{d|q} \mu(d)$. Or on démontre (en décomposant q en produit de nombres premiers) que, pour tout $q \geqslant 2$, on a $\sum_{d|q} \mu(d) = 0$.
2. a) La première égalité résulte de ce qu'il y a exactement p^n polynômes unitaires de degré n ; la dernière est un regroupement des polynômes irréductibles par leur degré. Écrivant $(R_k)_{k\in\mathbb{N}}$ les polynômes irréductibles unitaires, on a

$$\prod_{k=0}^{m} \frac{1}{1 - t^{\partial R_k}} = \prod_{k=0}^{m} \sum_{j_k=0}^{+\infty} t^{j_k \partial R_k} = \sum_{(j_0,\dots,j_m)\in\mathbb{N}^{m+1}} t^{\sum_{k=1}^m j_k \partial R_k} = \sum_{(j_0,\dots,j_m)\in\mathbb{N}^{m+1}} t^{\partial(\prod_{k=1}^m R_k^{j_k})} = \sum_{A \in Q_m} t^{\partial A}$$

où l'on a noté Q_m l'ensemble des polynômes n'ayant d'autres diviseurs irréductibles que $R_0, \dots, R_m$ et qui donc s'écrivent de manière unique sous la forme $\prod_{k=1}^{m} R_k^{j_k}$, d'où l'égalité du milieu, en prenant la limite quand $m \to \infty$.

Cela dit, il faut bien justifier ces formules qui convergent absolument pour $|t| < 1/p$.

b) On a $\dfrac{(fg)'}{fg} = \dfrac{f'}{f} + \dfrac{g'}{g}$, d'où (après justification du passage à la limite), $\dfrac{p}{1-pt} = \displaystyle\sum_{n=1}^{+\infty} \frac{nN_n t^{n-1}}{1-t^n}$.

Multipliant par t, on trouve $\displaystyle\sum_{k=1}^{+\infty} p^k t^k = \sum_{n=1}^{+\infty}\sum_{k=1}^{+\infty} nN_n t^{kn}$. Donc, prenant le terme d'ordre ℓ dans cette série entière $p^\ell t^\ell = \displaystyle\sum_{n|\ell} nN_n$.

c) résulte immédiatement de 1.b) et 2.b).

d) On a donc $nN = p^n + \displaystyle\sum_{d|n; d\neq n} \mu(\frac{n}{d}) p^d \geqslant p^n - \sum_{d|n;\ d\neq n} p^d \geqslant p^n - \sum_{1\leqslant d\leqslant n/2} p^d \geqslant p^n - (n/2)p^{n/2}$.

On a $p^{n/2} > n/2$, d'ou $N_n > 0$.

e) Il existe donc au moins un polynôme irréductible P de degré n dans $\mathbb{F}_p[X]$. Alors $\mathbb{F}_p[X]/(P)$ est un corps à p^n éléments.

II. Algèbre linéaire sur un sous-corps de $\mathbb{C}$

11.4 Définitions et généraliés

Exercice 4.1.

1. Par définition de l'application s, s est surjective si et seulement si $E = F + G$.
   On a $\ker s = \{(x, y) \in E \times F;\ x + y = 0\} = \{(x, -x);\ x \in E \cap F\}$ donc $\ker s = \{(0, 0)\}$ si et seulement si $E \cap F = \{0\}$.
   Par suite, s est bijective si et seulement F et G sont supplémentaires.
2. Notons $s : E_1 \times \ldots \times E_n \to E$ l'application $(x_1, \ldots, x_n) \mapsto \sum_{i=1}^{n} x_i$.
   Supposons que la somme n'est pas directe ; alors s n'est pas injective, donc il existe $(x_1, \ldots, x_n) \in \ker s$ non nul. Soit k le plus grand des indices i tel que $x_i \neq 0$. Alors $x_k = \sum_{i=1}^{k-1}(-x_i) \in E_k \cap (E_1 + \ldots + E_{k-1})$ qui n'est donc pas réduit à $\{0\}$.
   Supposons s injective et soient $k \in \{2, \ldots, n\}$ et $x \in (E_1 + \ldots + E_{k-1}) \cap E_k$. Alors il existe $(x_1, \ldots, x_{k-1}) \in (E_1 \times \ldots \times E_{k-1})$ tels que $x = \sum_{i=1}^{k-1} x_i$. On en déduit que $(x_1, \ldots, x_{k-1}, -x, 0, \ldots, 0) \in \ker s$. Il vient $(x_1, \ldots, x_{k-1}, -x, 0, \ldots, 0) = (0, \ldots, 0)$ (puisque s est injective) donc $x = 0$.

Exercice 4.2.

1. L'ensemble E est un sous-espace vectoriel de l'espace vectoriel $\mathbb{R}^{\mathbb{R}}$.
2. Les ensembles P et I contiennent tous deux la fonction nulle et sont trivialement stables par combinaison linéaire, ce sont donc des sous-espaces vectoriels de E.
   Si $f \in F \cap P$, alors f est à la fois paire et impaire, donc pour tout réel x, on a : $f(x) = -f(x)$, d'où $f = 0$.
   Toute fonction continue de E se décompose en $f = p + i$, où $p \in P$ et $i \in I$ sont définies par : $\forall x \in \mathbb{R}$, $p(x) = \dfrac{f(x) + f(-x)}{2}$ et $i(x) = \dfrac{f(x) - f(-x)}{2}$.
3. - exemple : $f(x) = e^x$ se décompose en $f = p + i$ avec $p(x) = ch(x)$ et $i(x) = sh(x)$.
   - autre exemple : pour $f(x) = \cos(x+a)$, avec $a \in \mathbb{R}$; $p(x) = \cos(x)\cos(a)$ et $i(x) = -\sin(x)\sin(a)$.

Exercice 4.3. D'après l'énoncé, on a $G \subset H$; démontrons l'inclusion réciproque. Soit h un élément de H, alors $h = h + 0 \in F + H \subset F + G$, donc il existe un couple $(f, g) \in F \times G$ tel que $h = f + g$. Donc $f = h - g$, avec $h \in H$ et $g \in G \subset H$. Ainsi, puisque H est un sous-espace vectoriel de E, $f \in F \cap H \subset F \cap G \subset G$. D'où $h = f + g \in G$. Par suite, $H \subset G$, puis $H = G$.

Exercice 4.4.

1. S'il existe $x \in G \setminus F$ et $y \in F \setminus G$, alors $x + y \notin F$ (sinon $x = (x + y) - y \in F$) et $x + y \notin G$ (sinon $y = (x + y) - x \in G$). Par suite, $G \cup F$ n'est pas un sous-espace vectoriel de E.
2. a) Soient $\lambda, \mu \in K$. Si $y + \lambda x \in F_{k+1}$ et $y + \mu x \in F_{k+1}$, alors leur différence $(\lambda - \mu)y \in F_{k+1}$ ce qui implique $\lambda = \mu$, puisque $y \notin F_{k+1}$. De même si, pour $j \leqslant k$, on a $y + \lambda x \in F_j$ et $y + \mu x \in F_j$, alors $(\lambda - \mu)x = \lambda(y + \mu x) - \mu(y + \lambda x) \in F_j$ ce qui implique $\lambda = \mu$, puisque $x \notin F_j$.

b) On raisonne par récurrence sur n. Si $n = 1$, puisque $F_1 \neq E$, il existe $x \in E \setminus F_1$.
Si on connait cette propriété pour $n-1$, il existe, d'après l'hypothèse de récurrence $x \in E$ tel que $x \notin \bigcup_{j=1}^{n-1} F_j$. Soit $y \in E \setminus F_n$. Puisque K a une infinité d'éléments, il existe d'après a) $\lambda \in K$ tel que pour $j \in \{1, \dots, n\}$ on ait $y + \lambda x \in F_j$, *i.e.* $y + \lambda x \notin \bigcup_{j=1}^{n} F_j$.

Exercice 4.5. Les applications $p : (x, y) \mapsto x$ et $q : (x, y) \mapsto y$ de $E \times F$ dans E et F respectivement sont linéaires. Si f est linéaire, alors $q - f \circ p$ est aussi linéaire et son noyau G_f est un sous-espace vectoriel de $E \times F$.

Réciproquement, supposons que G_f est un sous-espace vectoriel de $E \times F$; notons $p_1 : G_f \to E$ et $q_1 : G_f \to F$ les restrictions de p et q à G_f. Elles sont linéaires, comme restrictions d'applications linéaires - et p_1 est bijective. Alors p_1^{-1} est linéaire et $f = q_1 \circ p_1^{-1}$ est bien linéaire.

Exercice 4.6.
- Démontrons que $\ker g \cap \operatorname{im} f \subset f(\ker g \circ f)$. Soit $y \in \ker g \cap \operatorname{im} f$; il existe alors un élément x de E tel que $y = f(x)$. De plus, $y \in \ker g$ donc $0 = g(y) = g(f(x)) = g \circ f(x)$ et $x \in \ker g \circ f$. Par suite, $\ker g \cap \operatorname{im} f \subset f(\ker g \circ f)$.
- Démontrons l'inclusion réciproque. Soit $y \in f(\ker g \circ f)$, alors il existe $x \in \ker g \circ f$ tel que $y = f(x)$. Donc $y \in \operatorname{im} f$ et $g(y) = g(f(x)) = g \circ f(x) = 0$. Par suite, $f(\ker g \circ f) \subset \ker g \cap \operatorname{im} f$.

Exercice 4.7.

1. Il est clair que E contient la suite nulle.
   Soient $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ des éléments de E et $\lambda \in K$. Alors, pour tout $n \geqslant 2$, on a $x_n + y_n = ax_{n-1} + bx_{n-2} + ay_{n-1} + by_{n-2} = a(x_{n-1} + y_{n-1}) + b(x_{n-2} + y_{n-2})$, donc $(x_n + y_n)_{n\in\mathbb{N}} \in E$. De plus, $\lambda x_n = \lambda(ax_{n-1} + bx_{n-2}) = a(\lambda x_{n-1}) + b(\lambda x_{n-2})$, donc $(\lambda x_n)_{n\in\mathbb{N}} \in E$. Par suite, E est bien un sous-espace vectoriel de $K^{\mathbb{N}}$.
2. Démontrons par récurrence que pour tout $n \in \mathbb{N}$ on a $x_n = x_{n+1} = 0$:
   - On a par hypothèse $x_0 = x_1 = 0$.
   - Soit $n \geqslant 1$ et supposons $x_{n-1} = x_n = 0$, alors $x_{n+1} = ax_n + bx_{n-1} = 0 = x_n$.

   Ainsi, on obtient : $x_n = 0$ pour tout $n \in \mathbb{N}$.
3. a) On a $\begin{pmatrix} u_{n+1} \\ v_{n+1} \end{pmatrix} = A^{n+1} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = AA^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = A \begin{pmatrix} u_n \\ v_n \end{pmatrix} = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix} \begin{pmatrix} u_n \\ v_n \end{pmatrix} = \begin{pmatrix} au_n + bv_n \\ u_n \end{pmatrix}$.
   Donc pour tout $n \in \mathbb{N}$ on a $v_{n+1} = u_n$ et $u_{n+1} = au_n + bv_n$.

   b) D'après la question précédente, pour tout $n \geqslant 2$, $u_n = au_{n-1} + bv_{n-1} = au_{n-1} + bu_{n-2}$ et $v_n = u_{n-1} = au_{n-2} + bv_{n-2} = av_{n-1} + bv_{n-2}$, donc $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ sont des éléments de E.

   c) On a $v_0 = 0$, $u_0 = v_1 = 1$ et $u_1 = a$.
   Soient $(x_n)_{n\in\mathbb{N}} \in E$ et $(\lambda, \mu) \in K^2$. Posons $y_n = x_n - \lambda u_n - \mu v_n$. Comme E est un sous-espace vectoriel de $K^{\mathbb{N}}$, on a $(y_n)_{n\in\mathbb{N}} \in E$, donc $(y_n)_{n\in\mathbb{N}}$ est la suite nulle si et seulement si $y_0 = y_1 = 0$ d'après la question 2. Or $y_0 = x_0 - \lambda$ et $y_1 = x_1 - \lambda a - \mu$, donc $(x_n)_{n\in\mathbb{N}} = \lambda(u_n)_{n\in\mathbb{N}} + \mu(v_n)_{n\in\mathbb{N}}$ si et seulement si $\lambda = x_0$ et $\mu = x_1 - ax_0$. Cela prouve qu'il existe un et un seul couple $(\lambda, \mu) \in K^2$ tel que $(x_n)_{n\in\mathbb{N}} = \lambda(u_n)_{n\in\mathbb{N}} + \mu(v_n)_{n\in\mathbb{N}}$. Donc $(u_n)_{n\in\mathbb{N}}$ et $(v_n)_{n\in\mathbb{N}}$ forment une base de E.
4. D'après la question 2., $E \cap F = \{0\}$.
   Soit $(x_n)_{n\in\mathbb{N}} \in K^{\mathbb{N}}$. Posons $\lambda = x_0$ et $\mu = x_1 - ax_0$; enfin, pour $n \in \mathbb{N}$, posons $y_n = x_n - \lambda u_n - \mu v_n$. On a $y_0 = y_1 = 0$, donc $(y_n)_{n\in\mathbb{N}} \in F$. Ainsi $(x_n)_{n_i n\mathbb{N}} = \lambda(u_n)_{n\in\mathbb{N}} + \mu(v_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} \in E + F$.

11.5 Théorie de la dimension

Exercice 5.1.

1. Par définition de i_0, on a : $0 = \sum_{j=1}^{n} \lambda_j x_j = \lambda_{i_0} x_{i_0} + \sum_{j=1}^{i_0-1} \lambda_j x_j$, et $\lambda_{i_0} \neq 0$. Donc $x_{i_0} = -\sum_{j=1}^{i_0-1} \frac{\lambda_j}{\lambda_{i_0}} x_j \in \text{Vect}\{x_j;\ j < i\}$. Par suite,$i_0 \notin I$.
2. On démontre cette propriété par récurrence « forte » sur j. Remarquons que si $j \in I$, alors $x_j \in \text{Vect}\{x_i;\ i \in \{1, \dots j\} \cap I\}$; il reste à traiter le cas $j \notin I$.
   - Si $1 \notin I$, alors $x_1 = 0$, donc $x_1 \in \text{Vect}(\emptyset) = \{0\}$...
   - Soit $j \notin I$ et supposons que, pour tout $k < j$, on a $x_k \in \text{Vect}\{x_i;\ i \in \{1, \dots k\} \cap I\}$, alors $\text{Vect}\{x_i;\ i \in \{1, \dots j\} \cap I\}$ contient x_k pour tout $k < j$, donc $\text{Vect}\{x_k;\ 1 \leqslant k < j\}$, et donc $x_j \in \text{Vect}\{x_i;\ i \in \{1, \dots j\} \cap I\}$ - puisque $j \notin I$.
3. D'après 2, $\text{Vect}\{x_i;\ i \in I\}$ contient tous les x_j donc le système $(x_i)_{i\in I}$ est générateur. D'après 1, si $\lambda \in K^I$ est tel que $\sum_{i\in I} \lambda_i x_i = 0$, l'ensemble $\{j \in I;\ \lambda_j \neq 0\}$ n'a pas de plus grand élément : il est donc vide... Le système $(x_i)_{i\in I}$ est donc libre.

Exercice 5.2. Tout automorphisme de E tel que $f(F) = G$ est un isomorphisme de F sur G qui envoie une base de F sur une base de G ; donc F et G ont même dimension.

Si $\dim F = \dim G = k$, notons $(e_1, \dots, e_k)$ une base de F ; complétons la en une base $(e_1, \dots, e_n)$ de E. De même on obtient une base $(e'_1, \dots, e'_n)$ de E telle que $(e'_1, \dots, e'_k)$ soit une base de G. Comme $(e_1, \dots, e_n)$ est une base de E, il existe une unique application linéaire de E dans E telle que $f(e_i) = e'_i$ pour tout i. Comme l'image de la base $(e_1, \dots, e_n)$ est une base, f est un automorphisme de E ; l'image par f de l'espace vectoriel F engendré par $(e_1, \dots, e_k)$ est l'espace vectoriel engendré par $(f(e_1), \dots, f(e_k))$, c'est-à-dire G.

Exercice 5.3.

1. On suppose que G_1 et G_2 sont tous les deux supplémentaires de F ; notons $p_i : E \to G_i$ la projection sur G_i parallèlement à F. Soit $x \in E$. Comme $x - p_1(x) \in F = \ker p_2$, on a $p_2(x) = p_2(p_1(x))$, soit $p_2 \circ p_1 = p_2$; de même, $p_1 \circ p_2 = p_1$. Donc pour $x \in G_1$, on a $p_1(p_2(x)) = p_1(x) = x$ et pour $x \in G_2$, on a $p_2(p_1(x)) = p_2(x) = x$. La restriction de p_2 à G_1 est donc un isomorphisme : son inverse est la restriction de p_1 à G_2.
2. D'après le corollaire 5.11, F admet un supplémentaire G ; les dimensions de F et G sont finies et on a $\dim E = \dim F + \dim G = \dim F + \text{codim}\, F$.
3. Soit G un supplémentaire (de dimension finie) de F et F_1 un sous-espace de E contenant F. Soit G_1 un supplémentaire dans G de $G \cap F_1$. Alors
   - Comme $G_1 \subset G$, on a $G_1 \cap F_1 = G_1 \cap (G \cap F_1) = \{0\}$;
   - On a $E = F + G = F + (F_1 \cap G) + G_1$ et puisque $F \subset F_1$, $E = F_1 + G_1$.

   Donc $E = F_1 \oplus G_1$ et, puisque G_1 est un sous-espace de G, on a $\text{codim}\, F_1 = \dim G_1 \leqslant \dim G = \text{codim}\, F$.
4. Si $\ker f$ admet un supplémentaire F de dimension finie, alors la restriction de f est un isomorphisme de F sur $\text{im}\, f$ (prop. 4.17), donc $\text{rg} f = \text{codim}\, F$.

   Supposons inversement que $\text{rg} f$ est fini et soit $(e_1, \dots, e_k)$ une base de $\text{im}\, f$. Pour chaque i choisissons $x_i \in E$ tel que $f(x_i) = e_i$. Pour $x \in E$ et $(\lambda_1, \dots, \lambda_k) \in K^n$ on a

$$x - \sum_{i=1}^{k} \lambda_i x_i \in \ker f \iff f(x) = \sum_{i=1}^{k} \lambda_i e_i.$$

   Prenant $x = 0$, on en déduit que la famille $(x_1, \dots, x_k)$ est libre, puis que l'espace vectoriel $\text{Vect}\{x_1, \dots, x_k\}$ est un supplémentaire de $\ker f$.

Exercice 5.4. Remarquons que l'on a $\operatorname{im} g \circ f = g(\operatorname{im}(f))$.

1. Soit $g_1 : \operatorname{im} f \to G$ la restriction de g. On a $\operatorname{im} g \circ f = \operatorname{im} g_1$. Si $\operatorname{im} f$ est de dimension finie, g_1 est de rang fini et, d'après le théorème du rang, on a $\operatorname{rg} g \circ f = \operatorname{rg} g_1 = \dim \operatorname{im} f - \dim \ker g_1$; or $\ker g_1 = \{y \in \operatorname{im} f;\ g(y) = 0\} = \ker g \cap \operatorname{im} f$.
2. On a $\operatorname{im} g \circ f \subset \operatorname{im} g$; donc $\operatorname{rg} g \circ f \leqslant \operatorname{rg} g$. Puisque $\ker g$ est de codimension finie (dans F), il en va de même pour $\ker g + \operatorname{im} f$ (exerc. 5.3). Soit F_1 un supplémentaire (dans F) de $\ker g + \operatorname{im} f$. La restriction de g à F_1 est injective (puisque $\ker g \cap F_1 = \{0\}$), donc $\dim F_1 = \dim g(F_1)$. Démontrons que l'on a $g(F_1) \oplus \operatorname{im} g \circ f = \operatorname{im} g$; on aura $\operatorname{rg} g - \operatorname{rg} g \circ f = \dim g(F_1) = \operatorname{codim}(\ker g + \operatorname{im} f)$.
   - Si $z \in g(\operatorname{im} f) \cap g(F_1)$, alors il existe $y_1 \in F_1$ et $y \in \operatorname{im} f$ tels que $g(y_1) = g(y) = x$. Alors $y_1 = y + (y_1 - y) \in \operatorname{im} f + \ker g$ et puisque $y \in F_1$ et $F_1 \cap \ker g + \operatorname{im} f) = \{0\}$, il vient $y = 0$, donc $x = 0$.
   - On a bien sûr $g(F_1) \oplus \operatorname{im} g \circ f \subset \operatorname{im} g$. Soit $z \in \operatorname{im} g$, il existe $y \in F$ tel que $g(y) = z$, et puisque $F = F_1 + \ker g + \operatorname{im} f$, il existe $y_1 \in F_1$, $y_2 \in \ker g$ et $y_3 \in \operatorname{im} f$ tels que $y = y_1 + y_2 + y_3$; alors $z = g(y_1) + g(y_3) \in g(F_1) + g(\operatorname{im} f)$.

Exercice 5.5.

1. Il y a $p^n - 1$ éléments non nuls dans $\mathbb{F}_p^n$; chacun d'entre eux est contenu dans une et une seule droite ; chaque droite contient $p - 1$ éléments non nuls ; donc il y a $\dfrac{p^n - 1}{p - 1}$ droites. L'application $d \mapsto d^\perp$ est une bijection de l'ensemble des droites de $\mathbb{F}_p^n$ sur l'ensemble des hyperplans de son dual $(\mathbb{F}_p^n)^*$. Or $(\mathbb{F}_p^n)^*$ et $\mathbb{F}_p^n$ sont isomorphes. Ils ont même nombre d'yperplans.
2. - Le premier vecteur doit être non nul : on a $p^n - 1$ choix
   - Le deuxième, doit être non colinéaire au premier : $p^n - p$ choix.
   - Une fois choisis les j premiers vecteurs, ils engendrent un espace de dimension j - à p^j éléments ; donc pour le $j + 1$-ème, on a $p - n - p^j$ choix.

   Bref, on trouve qu'il y a $(p^n - 1)(p^n - p) \dots (p^n - p^{k-1})$ systèmes libres à k-éléments.

   En particulier, dans il y a $(p^n - 1)(p^n - p) \dots (p^n - p^{n-1})$ bases.
3. Notons L_k l'ensemble des systèmes libres à k éléments et G_k l'ensemble des sous-espaces de dimension k.

   L'application de L_k dans G_k qui à un système associe le sous-espace qu'il engendre (et dont il est une base) est donc surjective et l'image inverse de tout point F est l'ensemble de ses bases.

   On trouve donc que G_k a $\dfrac{(p^n - 1)(p^n - p) \dots (p^n - p^{k-1})}{(p^k - 1)(p^k - p) \dots (p^k - p^{k-1})} = \dfrac{(p^n - 1)(p^{n-1} - 1) \dots (p^{n-k+1} - 1)}{(p^k - 1)(p^{k-1} - 1) \dots (p - 1)}$ éléments.
4. La réponse à ces deux questions est la même. Dans $\mathbb{F}_p^3$ il y a $p^2 + p + 1$ plans ; chaque plan contient $p + 1$ droites. Deux droites sont contenues dans un et un seul plan.

   Choisissons une bijection f entre l'ensemble des 31 $(= 5^2 + 5 + 1)$ passagers et l'ensemble des droites de $\mathbb{F}_5^3$ et une bijection g entre l'ensemble des jours de la croisière et l'ensemble des plans de $\mathbb{F}_5^3$. Décidons que le jour y le capitaine invite un passager x si la droite $f(x)$ est contenue dans le plan $g(y)$.

   De même, choisissons une bijection f entre ensemble des $(57 = 49 + 7 + 1)$ symboles et l'ensemble des droites de $\mathbb{F}_7^3$ et une bijection g entre l'ensemble des cartes et l'ensemble des plans de $\mathbb{F}_7^3$. Décidons que la carte y contient le symbole x si la droite $f(x)$ est contenue dans le plan $g(y)$.

Exercice 5.6.

1. a) Notons $T \subset K^4$ l'ensemble des vecteurs ayant au moins deux composantes nulles (ce n'est bien sur pas un sous-espace vectoriel de K^4). Le noyau de g (*resp.* h) est formé des éléments de E dont les deux premières (*resp.* dernières) composantes sont nulles. D'après l'hypothèse $E \cap T = \{0\}$, donc g (*resp.* h) est injective. Elle est bijective puisque $\dim E = \dim K^2 = 2$.

La matrice A_E de $h \circ g^{-1}$ est inversible (d'inverse celle de $g \circ h^{-1}$). Par définition, de g et h, un élément $u = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \in K^4$ est dans E si et seulement si $u = g^{-1}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ ce qui a lieu si et seulement si $\begin{pmatrix} x_3 \\ x_4 \end{pmatrix} = A_E \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$. En particulier, écrivant $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ on trouve qu'une base de E est formé de $\begin{pmatrix} 1 \\ 0 \\ a \\ c \end{pmatrix}$ et $\begin{pmatrix} 0 \\ 1 \\ b \\ d \end{pmatrix}$. Ces deux vecteurs étant non nuls et appartenant à E doivent avoir trois coordonnées non nulles donc a, b, c, d sont non nuls.

b) Si $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est une telle matrice, alors les vecteurs $u = \begin{pmatrix} 1 \\ 0 \\ a \\ c \end{pmatrix}$ et $v = \begin{pmatrix} 0 \\ 1 \\ b \\ d \end{pmatrix}$ engendrent un espace E de dimension 2. Un vecteur non nul est de la forme $w = \alpha u + \beta v$ avec $\alpha, \beta \in K$ non tous les deux nuls. Si α ou β est nul - et pas l'autre, alors w est proportionnel à u ou v donc a trois composantes non nulles ; si α et β sont tous deux non nuls, alors les deux premières composantes de w sont α et β ; elles sont non nulles ; comme A est inversible, le vecteur $A\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ est non nul, autrement dit, une au moins parmi les deux dernières composantes de w n'est pas nulle.

2. a) Notons que $x, y \in \mathbb{F}_3^4$ ont deux composantes égales si et seulement si $x - y \in T$. Soit $f : \mathbb{F}_3^4 \to \mathbb{F}_3^2$ une application linéaire. Pour $x, y \in \mathbb{F}_3^4$, on a $f(x) = f(y) \iff x - y \in \ker f$. Alors f est un sudoku fort si et seulement si $x - y \in T \setminus \{0\} \Rightarrow x - y \notin \ker f$, soit $T \cap \ker f = \{0\}$.

b) Notons F le sous-espace de $\mathbb{F}_3^4$ formé des vecteurs dont les deux dernières coordonnées sont nulles. Un sudoku est donc donné par un sous-espace E de dimension 2 et tel que $T \cap E = \{0\}$ et une application linéaire f de noyau E. Soit E un tel sous-espace. Puisque $E \cap F = \{0\}$, on a $E \oplus F = \mathbb{F}_3^4$, donc une application linéaire de noyau E est déterminée par sa restriction à F qui est un isomorphisme $F \to \mathbb{F}_3^2$. Un tel isomorphisme est déterminé par une base de $\mathbb{F}_3^2$ (l'image d'une base de F). Une telle base est donnée par un vecteur non nul de $\mathbb{F}_3^2$ ($9-1=8$ choix) et un vecteur non colinéaire au premier ($9-3=6$ choix) soit au total $8 \times 6 = 48$ choix. L'espace E est lui-même donné par une matrice 2×2 inversible à coefficients tous non nuls. Une telle matrice est donnée par a, b, c non nuls ($2^3 = 8$) choix, puisque $d \neq 0$ et $d \neq \dfrac{bc}{a}$ est imposé. Au total, il y a donc $48 \times 8 = 384$ sudokus forts linéaires.

c) Le raisonnement ci-dessus démontre qu'une application linéaire $f : \mathbb{F}_3^4 \to \mathbb{F}_3^2$ est un sudoku si et seulement si $\ker f \cap T' = \{0\}$ où $T' = F_{1,2} \cup F_{3,4} \cup F_{1,3}$ en notant $F_{i,j} \subset \mathbb{F}_3^4$ l'espace vectoriel formé des vecteurs dont la i-ème et j-ème composante sont nulles (pour $1 \leqslant i < j \leqslant 4$). Remarquons que, comme dans la question 1, si E est un tel sous-espace, les applications $g : E \to K^2$ et $h : E \to K^2$ qui à $x \in E$ associent ses deux premières et ses deux dernières composantes respectivement sont bijectives, et ils sont déterminés par une matrice inversible $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. La condition $E \cap F_{1,3} = \{0\}$ impose alors $b \neq 0$. On vérifie comme dans 1 que cette condition est suffisante. Pour compter ces matrices, on dit qu'une telle matrice est déterminée par b (deux choix) a, d quelconques 9 choix et $c \neq \dfrac{ad}{b}$ (deux choix), soit 36 choix au total. On trouve qu'il y a $48 \times 36 = 1728$ sudokus linéaires.

11.6 Matrices et bases

Exercice 6.1. La matrice $B = \begin{pmatrix} I_r & 0 \\ -A_3A_1^{-1} & I_{n-r} \end{pmatrix}$ est inversible. Donc $BA = \begin{pmatrix} A_1 & A_2 \\ 0 & A_4 - A_3A_1^{-1}A_2 \end{pmatrix}$ a le même rang que A. Puisque A_1 est inversible, les r premières colonnes de la matrice BA sont indépendantes. La matrice BA est donc de rang r si et seulement si les $n-r$ colonnes suivantes sont contenues dans l'espace vectoriel engendré par ces r premières colonnes *i.e.* ont leurs $m-r$ derniers coefficients nuls.

Exercice 6.2. Soient $x \in E$ et $f \in E^*$. Notons X et X' les vecteurs-colonne formés par les colonnes de x dans les bases B et B' respectivement. On a $X = PX'$. De même notons Y et Y' les vecteurs-colonne formés par les colonnes de f dans les bases B^* et $(B')^*$ respectivement. On a $f(x) = {}^tYX = {}^t\,Y'X'$, donc ${}^tYPX' = {}^tY'X'$. Comme cela est vrai pour tout X', il vient ${}^tYP = {}^tY'$, soit ${}^tPY = Y'$, soit $Y = {}^tP^{-1}Y'$, donc la matrice de passage de B^* de B à $(B')^*$ est ${}^tP^{-1}$.

Exercice 6.3.

1. Soient $f, g \in E^*$. Alors g est nulle sur $\ker f$ si et seulement si $g \in (\ker f)^\perp = (\{f\}^o)^\perp = \mathrm{Vect}\{f\} = Kf$.
   Plus explicitement, soit $x \in E$ tel que $f(x) \neq 0$. Alors $E = \ker f \oplus Kx$. Si $\ker g = \ker f$, posons $\lambda = \dfrac{g(x)}{f(x)}$; les formes g et λf coïncident sur $\ker f$ et en x ; elles sont égales.
2. On a $\bigcap_{j=1}^{k} \ker f_j \subset \ker f$ si et seulement si $f \in \Big(\bigcap_{j=1}^{k} \ker f_j\Big)^\perp = (\{f_1, \ldots, f_k\}^o)^\perp = \mathrm{Vect}\{f_1, \ldots, f_k\}$.
   Autre solution. Il est d'abord clair que si $f = \sum_{j=1}^{k} \lambda_j f_j$, alors f est nulle sur $\bigcap_{j=1}^{k} \ker f_j$. Supposons inversement que $\bigcap_{j=1}^{k} \ker f_j \subset \ker f$ et démontrons par récurrence sur k que $f \in \mathrm{Vect}\{f_1, \ldots, f_k\}$.
   - Le cas $k = 1$ est la question 1.
   - Notons g_j et g les restrictions de f_j et f à $\ker f_k$. On a $\bigcap_{j=1}^{k-1} \ker g_j \subset \ker g$. L'hypothèse de récurrence implique qu'il existe $\lambda_1, \ldots, \lambda_{k-1} \in K$ tels que $g = \sum_{j=1}^{k-1} \lambda_j g_j$, donc $f - \sum_{j=1}^{k-1} \lambda_j f_j$ est nulle sur $\ker f_k$. Par la question 1, il existe $\lambda_k \in K$ tel que $f - \sum_{j=1}^{k-1} \lambda_j f_j = \lambda_k f_k$.

Exercice 6.4.

1. a) Remarquons que $\ker \varphi = \{x \in E;\ f_1(x) = \ldots = f_n(x) = 0\} = \{f_1, \ldots, f_n\}^o$. Puisque $(f_1, \ldots, f_n)$ est génératrice, on a $\{f_1, \ldots, f_n\}^o = (E^*)^o = \{0\}$. Cela prouve que φ est injective donc bijective par égalité des dimensions de E et K^n.
   b) L'image inverse de la base canonique $(e_1, \ldots, e_n)$ de $\mathbb{R}^n$ par l'application bijective φ est une base $(x_1, \ldots, x_n)$ de E. Pour $i \in \{1, \ldots, n\}$, on a $\varphi(x_i) = e_i$, soit $f_j(e_i) = \delta_{i,j}$; donc $(f_1, \ldots, f_n)$ est la base duale de $(x_1, \ldots, x_n)$.
2. résulte immédiatement de 1.
3. On a $\ker \varphi = \{f_1, \ldots, f_n\}^o$, donc $\mathrm{Vect}\{f_1, \ldots, f_n\} = (\{f_1, \ldots, f_n\}^o)^\perp = (\ker \varphi)^\perp$. Donc
   - φ est injective si et seulement si $\mathrm{Vect}\{f_1, \ldots, f_n\} = E^*$.

- Il vient $\mathrm{rg}\{f_1,\dots,f_n\} = \dim E - \dim\{f_1,\dots,f_n\}^o = \dim E - \dim\ker\varphi = \mathrm{rg}\varphi$. La famille $(f_1,\dots,f_n)$ est donc libre si et seulement si ce rang est égal à n, *i.e.* si φ est surjective.

Exercice 6.5.

1. On a $\mathrm{rg}\,{}^tf = \mathrm{rg}f$. Donc on a les équivalences
   - f est surjective $\iff \mathrm{rg}f = \dim F \iff {}^tf$ est injective ;
   - f est injective $\iff \mathrm{rg}f = \dim E \iff {}^tf$ est surjective.
2. Par définition $\ker {}^tf = \{\ell \in F^*;\ \ell\circ f = 0\} = \{\ell\in F^*;\ \mathrm{im}\, f \subset \ker\ell\} = (\mathrm{im}\, f)^\perp$.
   Si $g \in \mathrm{im}\,{}^tf$, il existe $\ell\in F^*$ telle que $g = \ell\circ f$, donc g est nulle sur $\ker f$, soit $g\in(\ker f)^\perp$. On en déduit l'égalité d'après l'égalité des dimensions : $\mathrm{rg}\,{}^tf = \mathrm{rg}f = \dim E - \dim\ker f = \dim(\ker f)^\perp$.

Exercice 6.6.

1. La bilinéarité est claire et la symétrie est la propriété de trace $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$. Notons $(E_{i,j})$ la base canonique de $\mathcal{M}_n(K)$. Pour $A = (a_{i,j})$, on a $\mathrm{Tr}(AE_{i,j}) = a_{j,i}$. Si $\mathrm{Tr}(AB) = 0$ pour tout B, il vient $a_{j,i} = 0$ pour tout i,j, donc $A = 0$. Cela prouve que b est non dégénérée.
2. L'hyperplan F est le noyau d'une forme linéaire. D'après 1. l'application $A\mapsto \mathrm{Tr}(A.)$ est bijective, donc il existe $A\in\mathcal{M}_n(K)$ tel que $F = \{B\in\mathcal{M}_n(K);\ \mathrm{Tr}(AB) = 0\}$.
   Il existe des matrices inversibles P,Q telles que $PAQ = \begin{pmatrix} I_r & 0\\ 0 & 0\end{pmatrix}$. Notons J une matrice de permutation circulaire. La diagonale de la matrice $(PAQ)J$ est nulle, donc $\mathrm{Tr}(PAQJ) = 0$. Or $\mathrm{Tr}(PAQJ) = \mathrm{Tr}(AQJP)$. Donc F contient la matrice inversible QJP.
3. Notons $\mathcal{S}$ et $\mathcal{A}$ les sous-espace vectoriels de $\mathcal{M}_n(\mathbb{R})$ formés des matrices symétriques et anti-symétriques respectivement. On a $\mathcal{M}_n(\mathbb{R}) = \mathcal{S}\oplus\mathcal{A}$. De plus, pour $M = (m_{i,j})\in\mathcal{M}_n(\mathbb{R})$, on a $\mathrm{Tr}({}^tMM) = \displaystyle\sum_{i,j} m_{i,j}^2 \geqslant 0$. On en déduit que la restriction de b à $\mathcal{S}$ (*resp.* à $\mathcal{A}$) est définie positive (*resp.* définie négative). Enfin, si $S\in\mathcal{S}$ et $A\in\mathcal{A}$, on a $b(S,A) = \mathrm{Tr}(SA) = \mathrm{Tr}({}^t(SA)) = \mathrm{Tr}({}^tA\,{}^tS) = \mathrm{Tr}(-AS) = -\mathrm{Tr}(SA)$. Donc $\mathcal{S}$ et $\mathcal{A}$ sont orthogonaux pour b. On en déduit que la signature de b est $(n(n+1)/2, n(n-1)/2)$.

Exercice 6.7.

1. Si $P(a) = P'(a) = 0$ alors $(X-a)^2|P$. De même, si $P(b) = P'(b) = 0$ alors $(X-b)^2|P$. Comme $(X-a)^2$ et $(X-b)^2$ sont premiers entre eux, si $P\in\{f_1,f_2,f_3,f_4\}^o$ alors $(X-a)^2(X-b)^2$ divise P, ce qui, vu que le degré de P est au plus 3, implique $P = 0$. Donc $\{f_1,f_2,f_3,f_4\}^o = \{0\}$.
2. On a $\mathrm{Vect}\{f_1,f_2,f_3,f_4\} = (\{f_1,f_2,f_3,f_4\}^o)^\perp = E^*$. Comme $\dim(E^*) = \dim(E) = 4$, on en déduit que la famille génératrice (f_1,f_2,f_3,f_4) est une base de E^*.
3. Soit (P_1,P_2,P_3,P_4) la base de E dont (f_1,f_2,f_3,f_4) est la base duale. On a $P_2(a) = P_2(b) = P_2'(b) = 0$, donc $(X-a)(X-b)^2|P_2$. Donc P_2 est de la forme $\alpha(X-a)(X-b)^2$ avec $\alpha\in K$. On trouve $1 = P_2'(a) = \alpha(a-b)^2$, donc $P_2 = \dfrac{(X-a)(X-b)^2}{(a-b)^2}$. De même (ou en intervertissant a et b), il vient $P_4 = \dfrac{(X-a)^2(X-b)}{(a-b)^2}$.
   On a $P_1(b) = P_1'(b) = 0$, donc P_1 est de la forme $(X-b)^2S$ où S est un polynôme du premier degré, donc il existe β et γ dans K tels que $P_1 = \beta(X-b)^2 + \gamma P_2$. Comme $P_1(a) = 1$, il vient $\beta(a-b)^2 = 1$; comme $P_1'(a) = 0$, il vient $2\beta(a-b)+\gamma = 0$. Enfin $P_1 = \dfrac{(X-b)^2(3a-b-2X)}{(a-b)^3}$.
   De même (ou en intervertissant a et b), il vient $P_3 = \dfrac{(X-a)^2(3b-a-2X)}{(b-a)^3}$.

Exercice 6.8.

1. Si u laisse toute droite invariante, pour tout $x \in E$, il existe $\lambda_x \in K$ tel que $u(x) = \lambda_x x$. Fixons $x \in E$ non nul et démontrons que u est l'homothétie de rapport λ_x. Soit $y \in E$.
   - S'il existe $\alpha \in K$ tel que $y = \alpha x$, alors $u(y) = u(\alpha x) = \alpha u(x) = \alpha\lambda_x x = \lambda_x y$.
   - Sinon, on a $u(x+y) = \lambda_{x+y}(x+y) = u(x) + u(y) = \lambda_x x + \lambda_y y$, et comme x, y est libre il vient $\lambda_y = \lambda_{x+y} = \lambda_x$, donc $u(y) = \lambda_x y$.
2. *Première méthode.*
   a) Si D est une droite de E^*, alors D^o est un hyperplan de E, donc est stable par u. Pour $x \in D^o$ et $\ell \in D$, on a $({}^t u(\ell))(x) = \ell(u(x)) = 0$, puisque $u(x) \in D^o$ et $\ell \in D$. Donc ${}^t u(\ell) \in (D^o)^\perp = D$. Par 1., ${}^t u$ est une homothétie.
   b) L'application $\tau : v \mapsto {}^t v$ est linéaire. Si ${}^t v = 0$, alors $(\operatorname{im} v)^\perp = \ker {}^t v = E^*$, donc $\operatorname{im} v = \{0\}$, soit $v = 0$. Cela prouve que τ est injective. Or il existe $\lambda \in K$ tel que ${}^t u = \lambda \mathrm{id}_{E^*} = {}^t(\lambda \mathrm{id}_E)$ donc $u = \lambda \mathrm{id}_E$.
3. *Deuxième méthode.* Soit D une droite de E. Il existe des hyperplans $H_1, \dots, H_m$ de E tels que $D = \bigcap_{k=1}^{m} H_k$. Si $x \in D$, alors pour tout k on a $x \in H_k$, donc $u(x) \in H_k$. Il vient $u(x) \in D$. Par 1., u est une homothétie.

Exercice 6.9.

1. Soit $\ell \in E^*_{\mathbb{C}}$, et posons $h = \mathrm{Re}(\ell)$, en d'autres termes, $h(x) = \mathrm{Re}(\ell(x))$. On a $\ell(ix) = i\ell(x)$, donc $h(ix) = -\mathrm{Im}(\ell(x))$. Cela prouve que $\ell(x) = h(x) - ih(ix)$. En particulier l'application $\ell \mapsto \mathrm{Re}(\ell)$ est injective.
   Soit $h \in E^*_{\mathbb{R}}$ et notons $\ell : E \to \mathbb{C}$ l'application $x \mapsto h(x) - ih(ix)$. L'application ℓ est clairement $\mathbb{R}$-linéaire et l'on a $\ell(ix) = h(ix) - ih(-x) = h(ix) + ih(x) = i\ell(x)$. Donc ℓ est $\mathbb{C}$-linéaire (autrement dit $\ell \in E^*_{\mathbb{C}}$) et l'on a $\mathrm{Re}(\ell) = h$. Cela prouve que $\ell \mapsto \mathrm{Re}(\ell)$ est surjective.
2. On veut définir l'action $\lambda.h$ de $\lambda \in \mathbb{C}$ sur $h \in E^*_{\mathbb{R}}$, de telle sorte que la bijection $\ell \mapsto \mathrm{Re}(\ell)$ soit $\mathbb{C}$-linéaire. Si $h = \mathrm{Re}(\ell)$, on aura $\lambda.h = \mathrm{Re}(\lambda\ell)$ ce qui donne $(\lambda.h)(x) = \mathrm{Re}(\lambda\ell(x)) = \mathrm{Re}(\ell(\lambda x)) = h(\lambda x)$.

Exercice 6.10.

1. Supposons F stable par f et soit $\varphi \in F^\perp$. Pour tout $x \in F$, puisque $f(x) \in F$, il vient $({}^t f(\varphi))(x) = \varphi \circ f(x) = 0$, donc ${}^t f(\varphi) \in F^\perp$. Par suite, $F^\perp$ est stable par ${}^t f$.
   Réciproquement, supposons $F^\perp$ stable par ${}^t f$ et soit $x \in F$. Pour tout $\varphi \in F^\perp$, puisque ${}^t f(\varphi) \in F^\perp$, il vient $\varphi \circ f(x) = ({}^t f(\varphi))(x) = 0$, donc $x \in (F^\perp)^o = F$ (*cf.* prop. 6.30.b). Par suite F est stable par f.
2. Pour $\lambda \in K$, on a ${}^t(f - \lambda \mathrm{id}_E) = {}^t f - \lambda \mathrm{id}_{E^*}$. Donc λ est une valeur propre de f si et seulement si c'est une valeur propre de ${}^t f$. Enfin ${}^t f$ possède une valeur propre si et seulement si ${}^t f$ possède une droite invariante, ce qui a lieu si et seulement si f a un hyperplan invariant d'après la question précédente.

Exercice 6.11.

1. Il existe $r \in \mathbb{N}$, $P \in GL_m(K) \subset GL_m(L)$ et $Q \in GL_n(K) \subset GL_n(L)$ tels que $PAQ = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$.
   Le rang de A sur K et sur L vaut r.
2. Le système $(x_1, \dots, x_k)$ est libre si et seulement si la matrice de vecteurs colonnes les x_i est de rang k.
3. Soit ϖ le polynôme minimal de M sur K. Puisque $\varpi(M) = 0$, le polynôme minimal sur L divise ϖ. Si k est le degré de ϖ, les matrices $(1, M, \dots, M^{k-1})$ sont libres sur K donc sur L ; on en déduit que le de gré du polynôme minimal de M sur L est k, d'où le résultat.

Exercice 6.12.

1. Il existe des matrices $P, Q \in GL(n, \mathbb{Q})$ telles que $PAQ = \begin{pmatrix} I_r & 0 \\ 0 & 0_{n-r} \end{pmatrix}$ de sorte que $\ker f_K = \{Q^{-1}X;\ X = (0, Z) \in K^k \times K^{n-k}\}$ et $\operatorname{im} f_K = \{PX;\ X = (Y, 0) \in K^k \times K^{n-k}\}$.
2. a) Pour $K = \mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$, notons f_K l'endomorphisme $M \mapsto AM - MB$ de $M_n(K)$. La matrice de ces endomorphismes dans la base $(E_{i,j})_{1 \leqslant i,j \leqslant n}$ de $M_n(K)$ est la même puisque $f_{\mathbb{Q}}(E_{i,j}) = f_{\mathbb{R}}(E_{i,j}) = f_{\mathbb{C}}(E_{i,j}) = \sum_{k=0}^{n} a_{k,i}E_{k,j} - \sum_{\ell=0}^{n} b_{j,\ell}E_{i,\ell}$. Le résultat découle de la question 1, puisqu'on a $E_K = \ker f_K$.

   b) Les matrices A et B sont semblables sur K si et seulement si E_K contient une matrice inversible. Or, $GL_n(\mathbb{R})$ est ouvert dans $M_n(\mathbb{R})$ donc $GL_n(\mathbb{R}) \cap E_{\mathbb{R}}$ est ouvert dans $E_{\mathbb{R}}$; si cet ouvert n'est pas vide, il rencontre le sous-ensemble dense $E_{\mathbb{Q}}$: si A et B sont semblables sur $\mathbb{R}$, elles le sont sur $\mathbb{Q}$.

   Si $E_{\mathbb{C}}$ contient une matrice inversible, celle-ci s'écrit $M + iN$ avec $M, N \in E_{\mathbb{R}}$. L'application $P : t \mapsto \det(M + tN)$ est polynomiale en t, et $P(i) \neq 0$. Donc, il existe $a \in \mathbb{R}$ tel que $P(a) \neq 0$, donc $M + aN \in E_{\mathbb{R}}$ est inversible.

11.7 Systèmes d'équations linéaires, déterminants

Exercice 7.1. En développant suivant la dernière ligne, on obtient (à l'aide d'une récurrence sur q) $\det \begin{pmatrix} A & B \\ 0_{q,p} & I_q \end{pmatrix} = \det A$ et de même $\det \begin{pmatrix} I_p & B \\ 0_{q,p} & C \end{pmatrix} = \det C$.

- Si A est inversible, on décompose M en le produit de matrices par blocs suivant : $M = \begin{pmatrix} A & B \\ 0_{q,p} & C \end{pmatrix} = \begin{pmatrix} A & 0_{q,p} \\ 0_{q,p} & I_q \end{pmatrix} \begin{pmatrix} I_p & A^{-1}B \\ 0_{q,p} & C \end{pmatrix}$. D'où $\det M = \det A \det C$.
- Si A n'est pas inversible ses vecteurs colonne sont liés et donc ceux de M aussi. Par suite, M n'est également pas inversible ; les déterminants de A et M sont tous deux nuls et l'égalité est encore vérifiée.

Exercice 7.2.

1. On a évidemment $\Delta_2(a_1, a_2) = a_2 - a_1$.
2. En développant par rapport à la dernière ligne, on voit que $\Delta_n(a_1, \ldots, a_{n-1}, x)$ est un polynôme en x de degré au plus $n-1$ et son coefficient de degré $n-1$ est $\Delta_{n-1}(a_1, \ldots, a_{n-1})$.

   Considérons deux cas :
   - s'il existe i, j avec $1 \leqslant i < j \leqslant n-1$ tels que $a_i = a_j$, alors les déterminants $\Delta_{n-1}(a_1, \ldots, a_{n-1})$ et $\Delta_n(a_1, \ldots, a_{n-1}, x)$ possèdent deux lignes égales, donc ils sont nuls ;
   - si les $(a_i)_{1 \leqslant i \leqslant n-1}$ sont deux à deux distincts, alors le polynôme $x \mapsto \Delta_n(a_1, \ldots, a_{n-1}, x)$ s'annule pour $x = a_k$ $(1 \leqslant k \leqslant n-1)$; il est donc de la forme $\prod_{k=1}^{n-1}(x - a_k)Q(x)$ où $Q \in K[x]$; comme le degré de $x \mapsto \Delta_n(a_1, \ldots, a_{n-1}, x)$ est $n-1$, on en déduit que Q est constant, et regardant les termes de degré $n-1$, il vient $Q = \Delta_{n-1}(a_1, \ldots, a_{n-1})$.
3. Immédiat par récurrence sur n.
4. Notons $E \subset K[X]$ le sous-espace vectoriel des polynômes de degré $\leqslant n-1$. Cette matrice représente l'application linéaire $P \mapsto \big(P(a_1), \ldots P(a_n)\big)$ dans les bases $(1, X, \ldots, X^{n-1})$ de E et la base canonique de K^n. Si les a_i sont deux à deux distincts, cette application est bijective - l'application réciproque est donnée par le polynôme d'interpolation de Lagrange.

Exercice 7.3. Démontrons ce résultat par récurrence sur n. C'est clair pour $n = 2$. Supposons ce résultat démontré pour $n-1$ et développons ce déterminant par sa première ligne. Ce déterminant est donc égal à

$$\lambda \begin{vmatrix} \lambda & 0 & \dots & 0 & a_1 \\ -1 & \lambda & \ddots & 0 & a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda & a_{n-2} \\ 0 & 0 & \dots & -1 & \lambda + a_{n-1} \end{vmatrix} + (-1)^{n+1} a_0 \begin{vmatrix} -1 & \lambda & 0 & \dots & 0 \\ 0 & -1 & \lambda & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \lambda \\ 0 & 0 & 0 & \dots & -1 \end{vmatrix}.$$

D'après l'hypothèse de récurrence, on a

$$\begin{vmatrix} \lambda & 0 & \dots & 0 & a_1 \\ -1 & \lambda & \ddots & 0 & a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda & a_{n-2} \\ 0 & 0 & \dots & -1 & \lambda + a_{n-1} \end{vmatrix} = \sum_{k=0}^{n-1} a_{k+1} \lambda^k$$

On trouve donc $\lambda \sum_{k=0}^{n-1} a_{k+1} \lambda^k + a_0 = P(\lambda)$.

Exercice 7.4.

1. Pour $j < n-1$, on a $T(X^j) = X^{j+1}$. Le reste de X^n dans la division euclidienne par P est $X^n - P = -\sum_{k=0}^{n-1} a_k X^k$. Donc la matrice de T dans la base $1, X, \dots, X^{n-1}$ est

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \ddots & 0 & -a_2 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}.$$

2. Écrivons $P = \sum_{k=0}^{n} b_k (X-\lambda)^k$. Remarquons que $b_n = 1$. On trouve de même que la matrice de $T - \lambda \mathrm{id}_{E_n}$ dans la base $1, (X-\lambda), \dots, (X-\lambda)^{n-1}$ est

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -b_0 \\ 1 & 0 & 0 & \dots & 0 & -b_1 \\ 0 & 1 & 0 & \ddots & 0 & -b_2 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 & -b_{n-2} \\ 0 & 0 & 0 & \dots & 1 & -b_{n-1} \end{pmatrix}.$$

3. Remarquons que $P(\lambda) = b_0$; développant la matrice trouvée dans la question précédente suivant à la première ligne, on trouve

$$\det(T - \lambda \mathrm{id}_{E_n}) = (-1)^{n+1}(-b_0) \det I_{n-1} = (-1)^n P(\lambda).$$

Exercice 7.5. Notons $D(x_1,\dots x_n,y_1\dots,y_n)$ ce déterminant. Retranchant la dernière ligne de toutes les autres, on voit que ce déterminant est égal à celui de la matrice $(a_{i,j})$ où

$$a_{i,j}=\begin{cases}\dfrac{1}{x_i+y_j}-\dfrac{1}{x_n+y_j}=\dfrac{x_n-x_i}{(x_i+y_j)(x_n+y_j)} & \text{si } i\neq n\\ \dfrac{1}{x_n+y_j} & \text{si } i=n\end{cases}$$

Mettant (x_n-x_i) en facteur dans la i-ème ligne et $\dfrac{1}{x_n+y_j}$ en facteur dans la j-ième colonne, il vient $D(x_1,\dots x_n,y_1\dots,y_n)=\dfrac{\prod_{i=1}^{n-1}(x_n-x_i)}{\prod_{j=1}^{n}(x_n+y_j)}\det(b_{i,j})$ où

$$b_{i,j}=\begin{cases}\dfrac{1}{x_i+y_j} & \text{si } i\neq n\\ 1 & \text{si } i=n\end{cases}$$

Retranchant la dernière colonne de toutes les autres, on trouve $\det(b_{i,j})=\det(c_{i,j})$ où

$$c_{i,j}=\begin{cases}\dfrac{1}{x_i+y_j}-\dfrac{1}{x_i+y_n}=\dfrac{y_n-y_j}{(x_i+y_j)(x_i+y_n)} & \text{si } i\neq n \text{ et } j\neq n\\ \dfrac{1}{x_i+y_n} & \text{si } i\neq n \text{ et } j=n\\ 0 & \text{si } i=n \text{ et } j\neq n\\ 1 & \text{si } i=j=n\end{cases}$$

Développant par rapport à la dernière ligne puis mettant (y_n-y_j) en facteur dans la j-ème colonne et $\dfrac{1}{x_i+y_n}$ en facteur dans la i-ième ligne, il vient

$$\det(c_{i,j})=\frac{\prod_{j=1}^{n-1}(y_n-y_j)}{\prod_{i=1}^{n-1}(x_i+y_n)}D(x_1,\dots,x_{n-1},y_1,\dots y_{n-1}).$$

Finalement

$$D(x_1,\dots x_n,y_1\dots,y_n)=\frac{\prod_{i=1}^{n-1}(x_n-x_i)}{\prod_{j=1}^{n}(x_n+y_j)}\frac{\prod_{j=1}^{n-1}(y_n-y_j)}{\prod_{i=1}^{n-1}(x_i+y_n)}D(x_1,\dots,x_{n-1},y_1,\dots y_{n-1}).$$

Enfin, à l'aide d'une récurrence immédiate, on trouve

$$D(x_1,\dots x_n,y_1\dots,y_n)=\frac{\prod_{1\leqslant i<j\leqslant n}(x_j-x_i)(y_j-y_i)}{\prod_{i,j=1}^{n}(x_i+y_j)}.$$

Exercice 7.6. Considérons la matrice $A=(a_{i,j})$ où $a_{i,i}=0$ et $a_{i,j}=1$ pour $i\neq j$. On a $\det A=\sum_{\sigma\in\mathfrak{S}_n}\varepsilon(\sigma)\prod_{i=1}^{n}a_{\sigma(i),i}$. Or pour $\sigma\in\mathfrak{S}_n$ on a $\prod_{i=1}^{n}a_{\sigma(i),i}=1$ si σ est un dérangement et $\prod_{i=1}^{n}a_{\sigma(i),i}=0$ si σ n'est un dérangement. Le nombre cherché est donc $\det A$. Or $\dfrac{1}{n}(A+I_n)$ est un projecteur de rang 1 ; donc $A+I_n$ se diagonalise avec les valeurs propres n de multiplicité 1 et 0 de multiplicité $n-1$ et A se diagonalise avec les valeurs propres $n-1$ de multiplicité 1 et (-1) de multiplicité $n-1$. Donc $\det A=(-1)^{n-1}(n-1)$.

Exercice 7.7. Si $I \subset \{1,\dots m\}$ et $J \subset \{1,\dots,n\}$ ont même nombre d'éléments, on note $\Delta_{I,J} : \mathcal{M}_{m,n}(\mathbb{K}) \to \mathbb{K}$ l'application qui à une matrice A associe le déterminant de sa matrice extraite d'ordre $I \times J$. C'est une application polynomiale en les coefficients de A donc continue.

On a $\{A \in \mathcal{M}_{m,n}(\mathbb{K});\ \text{rg } A \geqslant r\} = \bigcup_{I,J} \Delta_{I,J}^{-1}(\mathbb{K}^*)$ la réunion étant prise sur $I \subset \{1,\dots m\}$ et $J \subset \{1,\dots,n\}$ à r éléments. C'est un ouvert.

Démontrons que, pour $r \leqslant \min(m,n)$, l'adhérence de l'ensemble S_r des matrices de rang r est l'ensemble des T_r matrices de rang $\leqslant r$. Par ce qui précède T_r est fermé ; il contient S_r donc $\overline{S_r}$.

Réciproquement, si $\text{rg}A = s < r$, il existe des matrices inversibles P, Q telles que $A = P \begin{pmatrix} I_s & 0 \\ 0 & 0 \end{pmatrix} Q$.

Alors A est limite de la suite $B_k = P \begin{pmatrix} I_s & 0 & 0 \\ 0 & \frac{1}{k} I_{r-s} & 0 \\ 0 & 0 & 0 \end{pmatrix} Q$, donc $A \in \overline{S_r}$.

Exercice 7.8. Démontrons par récurrence sur n que

$$\Delta_n(a_1,\dots,a_n) = \begin{vmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ 1 & a_3 & a_3^2 & \dots & a_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant i < j \leqslant n} (a_j - a_i).$$

C'est clair pour $n = 2$.

Supposons le résultat vrai pour $n-1$. Commençons par remarquer que si $C_1,\dots,C_n$ sont des vecteurs-colonne et si on pose $C'_1 = C_1$ et $C'_{i+1} = C_{i+1} - a_1 C_i$ (pour $i = 1,\dots,n-1$), la matrice A de colonnes $C_1,\dots,C_n$ et A' de colonnes $C'_1,\dots,C'_n$ ont même déterminant. En effet, on passe de la matrice A à la matrice A' par $n-1$ opérations sur les colonnes - *i.e.* en multipliant à droite par la matrice $\begin{pmatrix} 1 & -a_1 & 0 & \dots & 0 \\ 0 & 1 & -a_1 & \dots & 0 \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$. Donc

$$\Delta_n(a_1,\dots,a_n) = \begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & a_2 - a_1 & a_2^2 - a_1 a_2 & \dots & a_2^{n-1} - a_1 a_2^{n-2} \\ 1 & a_3 - a_1 & a_3^2 - a_1 a_3 & \dots & a_3^{n-1} - a_1 a_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n - a_1 & a_n^2 - a_1 a_n & \dots & a_n^{n-1} - a_1 a_n^{n-2} \end{vmatrix}.$$

Développant par rapport à la première ligne puis mettant $a_i - a_1$ en facteur dans la $(i-1)$-ème ligne,

il vient

$$\begin{aligned}\Delta_n(a_1,\dots,a_n) &= \begin{vmatrix} a_2-a_1 & a_2^2-a_1a_2 & \dots & a_2^{n-1}-a_1a_2^{n-2} \\ a_3-a_1 & a_3^2-a_1a_3 & \dots & a_3^{n-1}-a_1a_3^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_n-a_1 & a_n^2-a_1a_n & \dots & a_n^{n-1}-a_1a_n^{n-2} \end{vmatrix} \\ &= \prod_{j=2}^{n}(a_j-a_1)\begin{vmatrix} 1 & a_2 & \dots & a_2^{n-2} \\ 1 & a_3 & \dots & a_3^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \dots & a_n^{n-2} \end{vmatrix} \\ &= \prod_{j=2}^{n}(a_j-a_1)\Delta_{n-1}(a_2,\dots,a_n)\end{aligned}$$

et on conclut grâce à l'hypothèse de récurrence.

Exercice 7.9.

1. La multiplication (à gauche ou à droite) par une matrice inversible ne change pas le rang. On a donc $\mathrm{rg}A = \mathrm{rg}A'$. Notons A_J et A'_J les matrices formées par les colonnes $C_j;\ j \in J$ et $C'_j;\ j \in J$ respectivement. On a $A'_J = UA_J$, donc $\mathrm{rg}A_J = \mathrm{rg}A'_J$.
2. Notons $(e_1,\dots,e_n)$ la base canonique de K^n. Par définition d'une matrice échelonnée réduite, $C'_{j(k)} = e_k$ et pour $j < j(k)$ on a $C'_j \in \mathrm{Vect}(e_s;\ s<k)$ un pivot. On en déduit que $j(k) = \inf\{j;\ \mathrm{rg}(C'_1,\dots,C'_j) = k\}$, d'où le résultat (d'après 1).
3. Pour $j > r$, on a $a'_{i,j} = 0$, donc $C'_j = \sum_{k=1}^{r} a'_{k,j}e_k = \sum_{k=1}^{r} a'_{k,j}C'_{j(k)}$. On a donc $C_j = U^{-1}C'_j = \sum_{k=1}^{r} a'_{k,j}U^{-1}C_{j(k)} = \sum_{k=1}^{r} a'_{k,j}C_{j(k)}$.
4. Les $j(k)$ sont déterminés par la question 2. On a $\mathrm{rg}\{C_{j(k)};\ 1\leqslant k\leqslant r\} = \mathrm{rg}\{C'_{j(k)};\ 1\leqslant k\leqslant r\} = r$, donc le système $(C_{j(k)})_{1\leqslant k\leqslant r}$ est libre. La question 3 détermine donc les $a'_{i,j}$.

Exercice 7.10.

1. Le déterminant d'un commutateur $ABA^{-1}B^{-1}$ est égal à 1 puisque det est un homomorphisme et K^* est commutatif ($\det(ABA^{-1}B^{-1}) = \det A \det B \det A^{-1} \det B^{-1} = 1$). Donc le groupe des commutateurs, qui est engendré par ces éléments est contenu dans $SL(n,K)$ pour tout n et tout K.

   Supposons d'abord $n=2$ et $K \neq \mathbb{F}_2$. Alors il existe $a \in K^*$, $a \neq 1$. On a

   $$\begin{aligned}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}^{-1}\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a^{-1} & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -\mu \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & (a-1)\mu \\ 0 & 1 \end{pmatrix}.\end{aligned}$$

   Donc toute matrice $I_2 + \lambda E_{1,2}$ est un commutateur. De même (ou en utilisant la transposée), toute matrice $I_2 + \lambda E_{2,1}$ est un commutateur. Par 1. tout élément de $SL(2,K)$ est un produit de commutateurs.

   Si $n \geqslant 3$, pour tout i,j (avec $i \neq j$), il existe k distinct de i et j. On a alors

   $$I_n + \lambda E_{i,j} = (I_n + \lambda E_{k,j})(I_n - E_{i,j})(I_n - \lambda E_{k,j})(I_n + E_{i,j})$$

   comme le montre un calcul où on utilise les formules $E_{i,j}E_{k,\ell} = 0$ si $j \neq k$ et $E_{i,j}E_{j,\ell} = E_{i,\ell}$. Cela prouve que toute transvection est un commutateur, donc tout élément de $SL(n,K)$ est produit de commutateurs.

2. Soit $A \in SL(n,\mathbb{K})$. Écrivons $A = T_1(\lambda_1)\dots T_N(\lambda_N)$ comme un produit de transvections. Alors $A_t = T_1(t\lambda_1)\dots T_N(t\lambda_N)$ est un chemin continue tracé dans $SL(n,\mathbb{K})$ qui joint I_n à A, donc A est dans la composante connexe (par arcs) de I_n dans $SL(n,\mathbb{K})$.
L'application $(A,\lambda) \mapsto AD_n(\lambda)$ est un homéomorphisme de $SL(n,\mathbb{K}) \times \mathbb{K}^*$ sur $GL(n,\mathbb{K})$ - l'homéomorphisme inverse est $B \mapsto \Big(BD_n((\det B)^{-1}), \det B\Big)$. Donc $GL(n,\mathbb{C})$, homéomorphe à un produit de connexes est connexe et $GL(n,\mathbb{R})$ a deux composantes connexes : les matrices de déterminant strictement positif et les matrices de déterminant strictement négatif : ce sont des ouverts connexes et disjoints de $GL(n,\mathbb{R})$.

Exercice 7.11.

Exercice 7.12.

1. est clair.
2. • Il est clair que Φ est linéaire
   • Démontrons que Φ est injective : supposons que $\Phi(D) = 0$. Soit $s : \{1,\dots,p\} \to \{1,\dots,n\}$ une application.
   ∗ Si s est strictement croissante, $D(e_{s(1)}, e_{s(2)}, \dots, e_{s(p)}) = 0$ puisque $\Phi(D) = 0$.
   ∗ Si est injective, il existe une unique permutation $\sigma \in \mathfrak{S}_p$ telle que $s \circ \sigma$ soit strictement croissante. On a $D(e_{s(1)}, e_{s(2)}, \dots, e_{s(p)}) = \varepsilon(\sigma) D(e_{s\circ\sigma(1)}, e_{s\circ\sigma(2)}, \dots, e_{s\circ\sigma(p)}) = 0$.
   ∗ Enfin si s n'est pas injective, $D(e_{s(1)}, e_{s(2)}, \dots, e_{s(p)}) = 0$ puisque D est alternée.
   Enfin, soit $x_1, \dots, x_p \in E^n$. Écrivons $x_j = \sum_{i=1}^{n} a_{i,j} e_i$. Comme D est multilinéaire, il vient
   $$D(x_1,\dots,x_p) = \sum_{s\in\{1,\dots,n\}^{\{1,\dots,p\}}} x_{s(1),1}\dots x_{s(p),p} D(e_{s(1)},\dots,e_{s(p)}) = 0.$$
   • Démontrons que Φ est surjective : soit $s \in J_p$; notons $f_s : E \to K^p$ l'application linéaire définie par $f_s(\sum_{i=1}^{n} t_i e_i) = (t_{s(1)}, t_{s(2)}, \dots, t_{s(p)})$ et posons $D_s(x_1,\dots,x_p) = \det_B(f_s(x_1),\dots,f_s(x_p))$ où B est la base canonique de K^p.
   ∗ On a $D_s(e_{s(1)}, e_{s(2)}, \dots, e_{s(p)}) = \det_B(B) = 1$.
   ∗ Soit $s' \in J_p$; si $s \neq s'$, il existe $j \in \{1,\dots,p\}$ tel que $s'(i) \notin s\{1,\dots,p\}$, donc $f_s(e_{s'(i)}) = 0$. On en déduit que $D_s((e_{s'(1)}, e_{s'(2)}, \dots, e'_{s(p)}) = 0$.
   Donc $\Phi(D_s)(s') = \delta_{s,s'}$: l'image de $(\Phi(D_s)_{s\in J_p}$ est la base canonique de K^{J_p}.
3. L'ensemble J_p possède $\binom{n}{p}$ éléments pour $p \leqslant n$ et est vide pour $p > n$, d'où le résultat.

11.8 Réduction des endomorphismes

Exercice 8.1. Ce sont les matrices diagonales par blocs.

Exercice 8.2.

1. est clair.
2. On a $J^n = I_n$ et, d'après la question 1, pour tout polynôme P de degré $\leqslant n-1$, on a $P(J) \neq 0$. On en déduit que le polynôme minimal de J est $X^n - 1$. D'après le théorème de Cayley-Hamilton, le polynôme minimal divise le polynôme caractéristique. Comme ces deux polynômes ont même degré, il vient $\chi_J = X^n - 1$ (ou $\chi_J = (-1)^n(X^n - 1)$ suivant les conventions).

3. Le polynôme X^n-1 étant scindé à racines simples (sur $\mathbb{C}$) on en déduit que J est diagonalisable. Ses valeurs propres sont les racines n-ièmes de 1. Soit λ une racine n-ièeme de 1. En résolvant un système facile, on trouve qu'un vecteur propre associé à la valeur propre λ est $C_\lambda = \begin{pmatrix} 1 \\ \lambda \\ \lambda^2 \\ \vdots \\ \lambda^{n-1} \end{pmatrix}$.
Posons $\omega = e^{2i\pi/n}$. La matrice formée par ces vecteurs colonnes est $P = (p_{i,j})$ ou $p_{i,j} = \omega^{(i-1)(j-1)}$. On trouve donc $P^{-1}JP = D$ où $D = \mathrm{diag}(\omega^{i-1})$.
Remarquons que les vecteurs C_λ sont deux à deux orthogonaux (on aurait pu le savoir d'avance puisque J est unitaire, donc normale donc ses espaces propres sont orthogonaux 2 à 2) et de même norme $\sqrt{n}$. On en déduit que la matrice $n^{-1/2}P$ est unitaire, donc $P^{-1} = \dfrac{1}{n}P^*$.
Enfin $A = \displaystyle\sum_{k=0}^{n-1} a_k J^k = P\sum_{k=0}^{n-1} a_k D^k P^{-1} = P\mathrm{diag}\Big(\sum_{k=0}^{n-1} a_k\omega^{(i-1)k}\Big)P^{-1}$.

Exercice 8.3.

1. Soit $(E_k)_{0\leqslant k\leqslant n}$ un drapeau et (e_k) une base adaptée. Alors pour tout j,k avec $1\leqslant j\leqslant k\leqslant n$, on a $e_j\in E_j\subset E_k$. On en déduit que $\{e_1,\dots,e_k\}$ est contenu dans E_k, et comme $(e_1,\dots,e_k)$ est libre et $\dim E_k = k$, on en déduit que $(e_1,\dots,e_k)$ est une base de E_k. En particulier, $E_k = \mathrm{Vect}(e_1,\dots,e_k)$, donc le drapeau (E_k) est déterminé par la base (e_k).
Soit (E_k) un drapeau. Pour $k\in\{1,\dots,n\}$ choisissons $e_k\in E_k\setminus E_{k-1}$. Alors, par récurrence $\mathrm{Vect}(e_1,\dots,e_k) = E_k$. En particulier, la famille $(e_1,\dots,e_n)$ est une base de $E = E_n$; elle est adaptée au drapeau.
2. La matrice de u est triangulaire dans la base $(e_1,\dots,e_n)$ si et seulement si pour tout k, on a $u(e_k)\in\mathrm{Vect}(e_1,\dots,e_k) = E_k$. Si $u(E_k)\subset E_k$, alors $u(e_k)\in u(E_k)\subset E_k$. Inversement, si pour tout k on a $u(e_k)\in E_k$, alors pour $j\leqslant k$ on a $u(e_j)\in E_j\subset E_k$, donc l'image de la base $(e_1,\dots,e_k)$ de E_k est contenue dans E_k, ce qui implique que $u(E_k)\subset E_k$.
3. On a $u(e_k) = \lambda_k e_k + \displaystyle\sum_{j<k} a_{j,k}e_j$, donc $u(e_k)-\lambda_k e_k\in E_{k-1}$. De plus le drapeau (E_j) est stable par $u-\lambda_k\mathrm{id}_E$, donc $(u-\lambda_k\mathrm{id}_E)(E_{k-1})\subset E_{k-1}$. Donc l'image par $u-\lambda_k\mathrm{id}_E$ de $E_k = E_{k-1}\oplus Ke_k$ est contenue dans E_{k-1}.
Par récurrence sur k, on en déduit que $(u-\lambda_1\mathrm{id}_E)\circ\ldots\circ(u-\lambda_k\mathrm{id}_E)$ est nul sur E_k. En particulier, pour $k=n$, l'endomorphisme $\chi_u(u) = (u-\lambda_1\mathrm{id}_E)\circ\ldots\circ(u-\lambda_n\mathrm{id}_E)$ est nul sur $E_n = E$; c'est l'endomorphisme nul. Cela établit le théorème de Cayley-Hamilton pour les endomorphismes triangulables.

Exercice 8.4.

1. Soit B une base dans laquelle la matrice M de u est triangulaire supérieure. Notons B_0 la la base orthonormée obtenue à partir de B par orthonormalisation de Gram-Schmidt. La matrice de passage $P = P_{B,B_0}$ est triangulaire supérieure, donc la matrice $P^{-1}MP$ de u dans la base B_0 est triangulaire supérieure.
2. Soit (A_k) une suite de matrices trigonalisables convergeant vers une matrice A. On doit démontrer que A est trigonalisable.
Pour chaque k, la matrice A_k étant trigonalisable dans une base orthonormée, il existe $U_k\in O(n)$ telle que $U_kA_kU_k^{-1} = T_k$ soit triangulaire supérieure. Comme $O(n)$ est compact, il existe une application strictement croissante $\varphi:\mathbb{N}\to\mathbb{N}$ telle que $(U_{\varphi(k)})$ soit convergente vers $U\in O(n)$. La suite extraite $A_{\varphi(k)}$ est convergente, donc, par continuité du produit, la suite $T_{\varphi(k)} = {}^tU_{\varphi(k)}A_{\varphi(k)}U_{\varphi(k)}$ converge vers ${}^tUAU$. Comme chaque $T_{\varphi(k)}$ est triangulaire ${}^tUAU$ l'est aussi, donc A est trigonalisable.

3. Notons $\mathcal{D} \subset M_n(\mathbb{R})$ et $\mathcal{T} \subset M_n(\mathbb{R})$ l'ensemble des matrices diagonalisables et trigonalisables respectivement. Puisque $\mathcal{T}$ est fermé et $\mathcal{D} \subset \mathcal{T}$, il vient $\overline{\mathcal{D}} \subset \mathcal{T}$.
   Soit $A \in \mathcal{T}$ et P une matrice inversible telle que $A = PTP^{-1}$ avec T triangulaire. Notons λ_i les éléments diagonaux de T. Soit D la matrice diagonale $D = \mathrm{diag}(i)$. Pour $\alpha \in \mathbb{R}_+^*$, $T + \alpha D$ a pour coefficients diagonaux $\lambda_i + \alpha i$. Soient $i, j \in \{1, \dots, n\}$ tels que $i \neq j$.
   Si $\lambda_i = \lambda_j$, alors $\lambda_i + \alpha i \neq \lambda_j + \alpha j$; si $\lambda_i \neq \lambda_j$ et $(n-1)\alpha < |\lambda_i - \lambda_j|$, on aura
   $$|(\lambda_i + \alpha i) - (\lambda_j + \alpha j)| \geqslant |\lambda_i - \lambda_j| - |\alpha(j - i)|.$$
   Donc, prenant α assez petit, ([6]) on aura encore $\lambda_i + \alpha i \neq \lambda_j + \alpha j$. Ainsi, toutes les valeurs propres de $T + \alpha D$ sont distinctes donc $T + \alpha D$ est diagonalisable. Prenant une telle suite α_k tendant vers 0, on écrit A comme limite $P(T + \alpha_k D)P^{-1}$ de matrices semblables à des matrices diagonalisables, donc diagonalisables.
4. Soit u un endomorphisme diagonalisable possédant une valeur propre double. Dans une base bien choisie, la matrice de u sera $\mathrm{diag}(d_1, \dots, d_n)$ avec $d_1 = d_2 = d$. Notons alors v l'endomorphisme dont la matrice est $E_{1,2}$ dans cette même base. Les endomorphismes u et v commutent, u est diagonalisable et v est nilpotent. Pour $\varepsilon \neq 0$, la partie nilpotente de $u + \varepsilon v$ dans la décomposition de Dunford est εv, qui n'est pas nul. Donc $u + \varepsilon v$ n'est pas diagonalisable. Cela prouve que $u \notin \mathring{\mathcal{D}}$.
   Supposons maintenant que $\chi_u = (X - d_1) \dots (X - d_n)$ avec $d_1 > d_2 > \dots > d_n$. Choisissons des nombres réels c_i pour $i = 0, \dots, n$, avec $c_0 > d_0$, $d_i > c_i > d_{i+1}$ pour $1 \leqslant i \leqslant n-1$ et $d_n > c_n$. Le signe de $\chi_u(c_i)$ est $(-1)^i$. Comme l'application $v \mapsto \det(c_i \mathrm{id}_E - v)$ est continue, l'ensemble $U_i = \{v \in L(E);\ (-1)^i \det(c_i \mathrm{id}_E - v) > 0\}$ est ouvert ainsi que l'intersection (finie) $U = \bigcap_{i=0}^{n} U_i$.
   Si $v \in U$, son polynôme caractéristique change de signe, donc s'annule d'après le théorème des valeurs intermédiaires entre c_i et c_{i-1} (pour $1 \leqslant i \leqslant n$). Comme χ_v possède n racines réelles distinctes, il est scindé à racines simples. On en déduit que U est formé de matrices diagonalisables à valeurs propres distinctes. En particulier $u \in \mathring{\mathcal{D}}$

Exercice 8.5.

1. Comme son polynôme caractéristique est scindé, la matrice A est trigonalisable : il existe $U \in GL_n(K)$ telle que $U^{-1}AU = T$ est triangulaire et ses coefficients diagonaux sont $\lambda_1, \dots, \lambda_n$. On a alors $Q(A) = UQ(T)U^{-1}$. Or la matrice $Q(T)$ est triangulaire et ses coefficients diagonaux sont les $Q(\lambda_k)$. Il vient $\chi_{Q(A)} = \chi_{Q(T)} = \prod_{k=1}^{n} (Q(\lambda_k) - X)$.
2. Soit $A \in M_n(\mathbb{C})$ la matrice compagnon du polynôme P. Elle est à coefficients entiers. La matrice A^q est à coefficients entiers, donc χ_{A^q} est un polynôme à coefficients entiers. Or d'après le première question $\chi_{A^q} = (-1)^n \prod_{k=1}^{n} (X - \lambda_k^q)$.

Exercice 8.6. Si u est trigonalisable, son polynôme caractéristique est scindé (d'après le théorème 8.7) et c'est un polynôme annulateur (d'après le théorème de Cayley-Hamilton).

Pour établir la réciproque, nous procédons par récurrence sur la dimension de E. C'est clair si $\dim E = 1$.

Notons n la dimension de E et supposons que tout endomorphisme d'un espace de dimension $n-1$ admettant un polynôme annulateur scindé est trigonalisable. Soit $u \in L(E)$ et supposons que u admet un polynôme annulateur scindé $P = \prod_{j=1}^{k} (X - \lambda_j)^{\alpha_j}$ et démontrons que u est trigonalisable. Remarquons qu'alors le polynôme minimal de u, qui divise P, est scindé, et l'on peut supposer que P est le polynôme

6. On peut prendre $0 < \alpha < (n-1)^{-1} \min\{|\lambda_i - \lambda_j|;\ (i,j) \in \{1, \dots, n\}^2,\ \lambda_i \neq \lambda_j\}$.

minimal. L'endomorphisme $u - \lambda_1 \mathrm{id}_E$ n'est pas surjectif (sinon le quotient de P par $X - \lambda_1$ serait annulateur). Soit H un hyperplan de E contenant l'image de $u - \lambda_1 \mathrm{id}_E$. On a $(u - \lambda_1 \mathrm{id}_E)(H) \subset \mathrm{im}\,(u - \lambda_1 \mathrm{id}_E) \subset H$, donc H est stable par $u - \lambda_1 \mathrm{id}_E$, donc par u. Le polynôme P est encore annulateur pour la restriction de u à H. D'après l'hypothèse de récurrence, il existe une base $(e_1, \dots, e_{n-1})$ de H dans la quelle la restriction de u est triangulaire. La matrice de u dans la base $(e_1, \dots, e_{n-1}, e_n)$ est triangulaire pour tout $e_n \in E \setminus H$.

Voici une autre méthode pour établir cette réciproque : d'après le « lemme des noyaux » (théorème 8.13) il suffit de démontrer que la restriction u_j de u à $E_j = \ker(u - \lambda_j \mathrm{id}_E)^{\alpha_j}$ est trigonalisable. Or $u_j = \mathrm{id}_{E_j} + n_j$ où n_j est nilpotent donc trigonalisable d'après l'exercice suivant.

Exercice 8.7.

1. Puisque X^m est annulateur, le polynôme minimal de u divise X^m. Les diviseurs (unitaires) de X^m sont les X^k avec $0 \leqslant k \leqslant m$. Or, on a supposé que pour $k < m$, on a $u^k \neq 0$. Le polynôme minimal de u est donc X^m.
2. La composée de morphismes surjectifs est surjective. Si u était surjectif, u^m le serait aussi...
3. On a $u(\mathrm{im}\ u) \subset u(E) = \mathrm{im}\ u$, donc $\mathrm{im}\ u$ est stable par u.
   Démontrons par récurrence sur la dimension de E qu'il existe une base de E dans laquelle la matrice de u est triangulaire avec des 0 sur la diagonale.
   Si $\dim E = 1$, puisque u n'est pas surjectif, son image est un sous-espace strict de E, donc $\mathrm{im}\ u = \{0\}$, soit $u = 0$, d'où le résultat.
   Notons n la dimension de E et supposons que tout endomorphisme nilpotent d'un espace de dimension $k < n$ est trigonalisable avec des 0 sur la diagonale. Soit $u \in L(E)$ un endomorphisme nilpotent.
   Puisque $\mathrm{im}\ u \subset E$ et $\mathrm{im}\ u \neq E$, la dimension de $\mathrm{im}\ u$ est $< n$ et la restriction de u à $\mathrm{im}\ u$ est nilpotente. D'après l'hypothèse de récurrence, il existe une base $(e_1, \dots, e_k)$ de $\mathrm{im}\ u$ dans la quelle la matrice A de la restriction de u est triangulaire. Complétons $(e_1, \dots, e_k)$ en une base de $(e_1, \dots, e_n)$ de E. La matrice de u dans la base $(e_1, \dots, e_n)$ est de la forme $\begin{pmatrix} A & B \\ 0 & 0 \end{pmatrix}$ (puisque $\mathrm{im}\ u = \mathrm{Vect}(e_1, \dots, e_k)$, d'où le résultat.
   Cela prouve aussi que $\chi_u = X^{\dim E}$.
4. Si $x \in N_k$, alors $u^k(x) = 0$, donc $u^{k+1}(x) = u(u^k(x)) = 0$ et donc $x \in N_{k+1}$. Si $x \in I_{k+1}$, il existe $y \in E$ tel que $x = u^{k+1}(y) = u^k(u(y))$, donc $x \in I_k$.
5. Soient $k \in \{0, \dots, m-1\}$. On a $u(I_k) = I_{k+1}$, donc u induit par restriction une application linéaire surjective $v_k : I_k \to I_{k+1}$. Le noyau de v_k est $\{x \in I_k;\ u(x) = 0\} = \ker u \cap I_k$.
   Par le théorème du rang $\dim I_k = \dim I_{k+1} + \dim \ker v_k$, or la suite $\ker v_k = I_k \cap \ker u$ est décroissante. Enfin, $\dim N_k = \dim E - \dim I_k$ et $\dim N_{k+1} = \dim E - \dim I_{k+1}$, donc $\dim N_{k+1} - \dim N_k = \dim I_k - \dim I_{k+1} = \dim \ker v_k$.

Exercice 8.8.

1. Posons $F = \mathrm{Vect}(x_0, \dots, x_{k-1})$. On a $u(F) = \mathrm{Vect}(x_1, \dots, x_k)$ et puisque $x_k \in F$, on a $u(F) \subset F$. On en déduit (à l'aide d'une récurrence) que, pour tout $\ell \in \mathbb{N}$, on a $u^\ell(F) \subset F$. Donc $x_\ell = u^\ell(x_0) \in F$.
2. La matrice d'un endomorphisme u dans une base $(e_1, \dots, e_n)$ est une matrice compagnon si et seulement si, pour $j = 1 \dots, n-1$, on a $u(e_j) = e_{j+1}$. Dans ce cas, on a $(u^j(e_1))_{0 \leqslant j \leqslant n-1}$ est une base de E, donc u est cyclique. De plus, si $P = \sum_{k=0}^{n-1} \lambda_k X^k$ est un polynôme non nul de degré $< n$, on a $P(u)(x_0) = \sum_{k=0}^{n-1} \lambda_k e_{k+1} \neq 0$, donc $P(u) \neq 0$. Le polynôme minimal est de degré au moins n, et divise χ_u : c'est χ_u (au signe près).

Supposons inversement que u et cyclique et soit x_0 un vecteur cyclique ; pour $j \in \mathbb{N}$, posons $x_j = u^j(x_0)$; soit k le plus petit entier tel que $(x_0, \dots, x_k)$ soit lié. Par définition de k, $(x_0, \dots, x_{k-1})$ est libre et $x_k \in \mathrm{Vect}(x_0, \dots, x_{k-1})$. D'après la question 1, on a $x_\ell \in \mathrm{Vect}(x_0, \dots, x_{k-1})$ pour tout $\ell \in \mathbb{N}$, donc $\mathrm{Vect}(x_0, \dots, x_{k-1}) = E$ puisque la famille $(x_\ell)_{\ell \in \mathbb{N}}$ est génératrice (x_0 étant cyclique). En d'autres termes, $(x_0, \dots, x_{k-1})$ est une base de E. Dans cette base la matrice de u est une matrice compagnon.

Exercice 8.9.

1. D'après le critère d'Eisenstein avec $p = 2$, pour tout $n \in \mathbb{N}^*$, le polynôme $X^n - 2$ convient.
2. Si $P \in \mathbb{Q}[X]$ est un polynôme irréductible de degré n, le corps $K = \mathbb{Q}[X]/(P)$ est de dimension n sur $\mathbb{Q}$. Pour $x \in K$, l'application $m_x : y \mapsto xy$ de K dans K est $\mathbb{Q}$-linéaire. L'application $x \mapsto m_x$ est un homomorphisme d'anneaux et une application linéaire de K dans $L_{\mathbb{Q}}(K)$ qui est isomorphe à $M_n(\mathbb{Q})$ *via* le choix d'une base $(e_1, \dots, e_n)$ du $\mathbb{Q}$-espace vectoriel K.
3. Soit F un sous-espace de dimension $n^2 - n + 1$ de $M_n(K)$; puisque $\dim F + \dim K > \dim M_n(\mathbb{Q})$, on en déduit que F et K ne sont pas en somme directe. Donc il existe $x \in F \cap K$ non nul. Comme K est un corps, x est inversible dans K, et donc dans $M_n(\mathbb{Q})$ (on a $m_x.m_{x^{-1}} = \mathrm{id}_K$).

Exercice 8.10.

1. est clair.
2. Soit P le polynôme unitaire tel que $J_x = PK[X]$. Remarquons que, d'après le théorème de Cayley-Hamilton, on a $\chi_u(u)(x) = 0$, donc P divise χ_u. Notons n la dimension de E. Alors l'équivalence entre les assertions suivantes :
   (i) x est cyclique ;
   (ii) $(x, u(x), \dots, u^{n-1}(x))$ est une base de E ;
   (iii) $(x, u(x), \dots, u^{n-1}(x))$ est libre ;
   (iv) pour tout polynôme non nul Q de degré $< n$, on a $Q(u)(x) \neq 0$;
   (v) $\partial P \geqslant n$;
   (vi) $P = \chi_u$.
3. Puisque Q_j n'est pas un multiple de ϖ_u, $Q_j(u) \neq 0$ et il existe donc $x \in E$ tel que $Q_j(u)(x) \neq 0$. Écrivons $\varpi_u = P_j^{\alpha_j} R_j$ et posons $x_j = R_j(u)(x)$. On a $P_j^{\alpha_j}(u)(x_j) = P_j^{\alpha_j}(u) \circ R_j(u)(x) = \varpi_u(u)(x) = 0$ et $P_j^{\alpha_j - 1}(u)(x_j) = P_j^{\alpha_j - 1}(u) \circ R_j(u)(x) = Q_j(u)(x) \neq 0$.
   On en déduit que $P_j^{\alpha_j} \in J_{x_j}$ et $P_j^{\alpha_j - 1} \notin J_{x_j}$. Écrivons $J_{x_j} = AK[X]$ où A est un polynôme unitaire. Alors A divise $P_j^{\alpha_j}$ mais ne divise pas $P_j^{\alpha_j - 1}$, donc $A = P_j^{\alpha_j}$.
4. Écrivons $J_y = AK[X]$ où A est un polynôme unitaire. On a $\varpi_u \in J_y$, donc A divise ϖ_u, donc $A = \prod_{j=1}^{k} P_j^{\beta_j}$ avec $0 \leqslant \beta_j \leqslant \alpha_j$.
   Soit $j, \ell \in \{1, \dots, k\}$; comme $P_j^{\alpha_j}$ ne divise pas Q_j, on a $Q_j(x_j) \neq 0$. Pour $\ell \in \{1, \dots, k\}$ distinct de j, comme $P_\ell^{\alpha_\ell}$ divise Q_j, on a $Q_j(u)(x_\ell) = 0$. Il vient $Q_j(u)(y) = Q_j(u)(x_j) \neq 0$, donc A ne divise pas Q_j : on en déduit que $\beta_j = \alpha_j$. Donc $A = \varpi_u$.
5. On a démontré qu'il existe $y \in E$ tel que J_y soit engendré par ϖ_u ; si $\varpi_u = \chi_u$, y est cyclique d'après 2.
   Si u est cyclique, alors il existe y tel que J_y soit engendré par χ_u ; or $\varpi_u \in J_y$, donc $\chi_u | \varpi_u$. Ils sont égaux (au signe près) d'après le théorème de Cayley-Hamilton.

Exercice 8.11.

1. a) L'application $\varphi : P \mapsto P(u)(x)$ étant linéaire, $\mathcal{J} = \varphi^{-1}(F)$ est un sous-espace vectoriel. Soient $P \in \mathcal{J}$ et $Q \in K[X]$; comme F est stable par $Q(u)$, on a $(QP)(u)(x) = Q(u)\big(P(u)(x)\big) \in F$, donc $QP \in \mathcal{J}$. Cela prouve que $\mathcal{J}$ est un idéal.

   b) On a $\varpi_u(u)(x) = 0 \in F$ donc $\varpi_u \in \mathcal{J}$, donc $P_F | \varpi_u$.

   c) • Soit $y \in F$. Comme x est cyclique, il existe $Q \in K[X]$ tel que $y = Q(u)(x)$; alors, par définition de $\mathcal{J}$, on a $Q \in \mathcal{J}$, donc il existe $P \in K[X]$ tel que $Q = P_F P$. Alors $y = P_F(u)\big(P(u)(x)\big)$, donc $y \in \operatorname{im} P_F(u)$.
   • Soit $y \in \operatorname{im} P_F(u)$. Alors il existe $z \in E$ tel que $y = P_F(u)(z)$ et l'on a $Q_F(u)(y) = (Q_F P_F)(u)(z) = 0$ puisque $Q_F P_F = \varpi_u$ est annulateur pour u.
   • Soit $y \in \ker Q_F(u)$. Comme x est cyclique, il existe $Q \in K[X]$ tel que $y = Q(u)(x)$; alors, $0 = Q_F(u)(y) = (Q_F Q)(u)(x)$. Or, comme x est cyclique, pour $P \in K[X]$ on a $P(u)(x) = 0 \iff \varpi_u | P$ (*cf.* exerc. 8.10, question 2). On en déduit que $\varpi_u | Q_F Q$ et puisque $\varpi_u = P_F Q_F$, il vient $P_F | Q$, donc $Q \in \mathcal{J}$, soit enfin $y \in F$.

   d) Notons u_F la restriction de u à F. Posons $y = P_F(u)(x)$. Pour tout $z \in F$, il existe $P \in K[X]$ tel que $P(u)(x) = z$ (car x est cyclique) et, puisque $z \in F$, $P \in \mathcal{J}$, donc il existe $Q \in K[X]$ tel que $P = QP_F$, soit $z = Q(u)\big(P_F(u)(x)\big) = Q(u_F)(y)$, donc y est cyclique pour u_F. Enfin, Q_F est un polynôme annulateur pour u_F et si $Q \in K[X]$ est de degré $< \partial Q_F$, alors $\partial(P_F Q) < \partial \varpi_u$, donc $Q(u)P_F(u)(x) \neq 0$, soit $Q(u_F)(y) \neq 0$. On en déduit que Q_F est le polynôme minimal de u_F, qui est son polynôme caractéristique puisque u_F est cyclique. Donc $\dim F = \partial Q_F$.

2. Si u est cyclique, les sous-espaces de E invariants par u sont les $\ker Q(u)$ où Q est un diviseur du polynôme minimal de u (d'après 1.c). Or le polynôme minimal de u a un nombre fini de diviseurs unitaires (si on écrit $\varpi_u = \prod_{j=1}^{k} P_j^{\alpha_j}$, avec P_j irreductibles unitaires et distincts, les diviseurs unitaires de ϖ_u sont les $\prod_{j=1}^{k} P_j^{\beta_j}$ avec $0 \leqslant \beta_j \leqslant \alpha_j$; il y en a $\prod_{j=1}^{k} \alpha_j + 1$). Donc E possède un nombre fini de sous-espaces invariants.

   On suppose que E possède un nombre fini de sous-espaces invariants $F_1, \dots, F_N$. Pour $x \in E$, notons $E_x = \{P(u)(x);\ P \in K[X]\}$; c'est un sous-espace invariant et il existe $j(x) \in \{1, \dots, N\}$ tel que $E_x = F_{j(x)}$. Posons $J = \{j(x);\ x \in E\}$; comme $x \in E_x = F_{j(x)}$, il vient $\bigcup_{j \in J} F_j = E$.

   D'après l'exercice 4.4, l'un des F_j est égal à E, donc u est cyclique.

3. Si le polynôme caractéristique χ_u de u est irréductible, il est égal au polynôme minimal, donc u est cyclique et les seuls sous-espaces invariants sont les $\ker Q(u)$ avec Q diviseur de χ_u, soit E et $\{0\}$ puisque χ_u est irréductible.

   Si E ne possède pas de sous-espaces invariants par u autres que $\{0\}$ et E, alors pour tout $x \in E$ non nul, l'espace $\{P(u)(x);\ P \in K[X]\}$ est invariant et non nul, donc x est cyclique. Si P, Q sont des polynômes tels que $PQ = \chi_u$ avec Q non scalaire, puisque P n'est pas un multiple de $\chi_u = \varpi_u$ l'endomorphisme $P(u)$ n'est pas nul, donc $\operatorname{im} P(u) \neq \{0\}$. Comme c'est un sous-espace invariant par u, il vient $\operatorname{im} P(u) = E$. Or $Q(u) \circ P(u) = 0$, donc $Q(u)$ est nul sur $\operatorname{im} P(u) = E$; il vient $Q(u) = 0$, donc Q est annulateur pour u ; c'est un multiple de χ_u. On en déduit que P est scalaire. Donc χ_u est irréductible.

Exercice 8.12. Pour $t = 1$, cette matrice est égale à $I_2 + N$ avec N nilpotente. Comme N et I_2 commutent, c'est sa décomposition de Dunford. Pour $t \neq 1$, cette matrice a deux valeurs propres distinctes : elle est diagonalisable. Sa décomposition de Dunford est donc $A = A + 0$... On en déduit que la décomposition de Dunford n'est pas continue, *i.e.* que l'application $A \mapsto (D, N)$ n'est pas continue.

Exercice 8.13. Pour une matrice $M = (m_{i,j}) \in M_n(\mathbb{C})$, notons $\overline{M}$ la matrice $(\overline{m_{i,j}})$. Comme A est réelle, on a $\overline{A} = A = \overline{D} + \overline{N}$. Comme l'application $M \mapsto \overline{M}$ est un homomorphisme d'anneaux, les

matrices $\overline{D}$ et $\overline{N}$ commutent, $\overline{N}$ est nilpotente ; enfin, si on écrit $D = P^{-1}\Delta P$ avec Δ diagonale, on a $\overline{D} = \overline{P}^{-1}\overline{\Delta P}$, donc $\overline{D}$ est diagonalisable. Par unicité de la décomposition de Dunford, il vient $D = \overline{D}$ et $N = \overline{N}$, donc D et N sont réelles.

Exercice 8.14. Notons D le PGCD de P et ϖ_u, et écrivons $\varpi_u = QD$ et $P = RD$ (avec $Q, R \in K[X]$). Si $D \neq 1$, Q n'est pas multiple de ϖ_u, donc $Q(u) \neq 0$. Or, on a $0 = \varpi_u(u) = D(u)Q(u)$, donc le noyau de $D(u)$ contient l'image de $Q(u)$, donc $D(u)$ n'est pas injectif. L'endomorphisme $P(u) = R(u)D(u)$ s'annule sur le noyau de $D(u)$ donc n'est pas injectif.

Si ϖ_u et P sont premiers entre eux, écrivons une relation de Bézout $1 = PQ + \varpi_u R$. On a $\mathrm{id}_E = P(u)Q(u) + \varpi_u(u)R(u)$, et puisque $\varpi_u(u) = 0$, l'endomorphisme $P(u)$ est inversible d'inverse $Q(u)$.

Exercice 8.15.

1. L'endomorphisme v est cyclique. On a donc $\chi_v = \varpi_v$. Or ϖ_v divise $\varpi_u = P^k$. C'est donc une puissance P^j de P (avec $j \leqslant k$). Raisonnons par récurrence sur la dimension de E. Si $\dim(E) \leqslant \partial P$, on a $E = F$ et $\chi_u = P$. Formons une base $(e_1, \dots, e_\ell)$ de F et complétons-la en une base $(e_1, \dots, e_n)$ de E. Dans cette base, la matrice de u est de la forme $\begin{pmatrix} A & C \\ 0 & D \end{pmatrix}$. Le polynôme minimal de D divise celui de u : c'est une puissance de P. D'après l'hypothèse de récurrence, χ_D est une puissance de P, ainsi que $\chi_u = \chi_A\chi_D$.
2. Écrivons $\varpi_u = \prod_{j=1}^{m} P_j^{\alpha_j}$ la décomposition du polynôme minimal de u en facteurs irréductibles ; posons $F_j = \ker P_j^{\alpha_j}(u)$, et notons v_j la restriction de u à F_j. Comme $E = \bigoplus F_j$, on a $\chi_u = \prod_{j=1}^{m} \chi_{v_j}$. Or, d'après la question précédente, pour tout j, il existe $\beta_j \geqslant \alpha_j$ tel que $\chi_{v_j} = P_j^{\beta_j}$.
3. Puisque χ_u et ϖ_u ont les mêmes diviseurs irréductibles on a (i) $\iff$ (ii). L'équivalence (ii) $\iff$ (iii) résulte de l'exercice 8.14.

Exercice 8.16. Notons $A \in M_n(K) \subset M_n(L)$ la matrice de u dans une base de E. Soit $\lambda \in L$ une racine de P. Puisque P divise χ_u, on a $\chi_u(\lambda) = 0$, donc λ est une valeur propre de A. En d'autres termes, il existe un vecteur colonne non nul $X \in L^n$ tel que $AX = \lambda X$, donc $P(A)X = 0$. En particulier, $\det P(u) = \det P(A) = 0$. D'après l'exercice 8.14, on en déduit que P et ϖ_u ne sont pas premiers entre eux, et puisque P est irréductible, il divise ϖ_u.

Exercice 8.17.

1. Écrivons $\varpi = PQ$. Alors $Q(u) \neq 0$ car ϖ ne divise pas Q. Comme $P(u) \circ Q(u) = \varpi(u) = 0$, $P(u)$ est nul sur l'image de $Q(u)$. Soit x un vecteur non nul dans cette image. On a donc $P(u)(x) = 0$. Notons k le degré de P. Remarquons que l'ensemble $J_x = \{T \in K[X];\ T(u)(x) = 0\}$ est un idéal dans $K[X]$; il est donc de la forme $D\,K[X]$. Alors D divise P (puisque $P \in J_x$) et puisque $x \neq 0$, on a $1 \notin J_x$, donc $J_x = P\,K[X]$. L'application $T \mapsto T(u)x$ est alors un isomorphisme de $K[X]/J_x$ sur un sous-espace F_x de E invariant par u. On a $\dim F_x = \dim K[X]/J_x = k$.
2. Cela résulte immédiatement de la question précédente puisque tout polynôme irréductible sur $\mathbb{R}$ est de degré 1 ou 2. *Une autre solution de cette question est donnée dans le lemme 9.33.*

Exercice 8.18.

1. Numérotons les sommets du triangle de 1 à 3. Deux points sont joignables par un (unique) chemin de longueur 1 si et seulement s'ils sont distincts. En d'autres termes, le nombre $a_{i,j}$ de chemins de

longueur 1 joignant i à j est donné par la matrice $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$. Le nombre $a_{i,j}^{(n)}$ de chemins de longueur n joignant les s i et j est alors donné par la matrice A^n. Pour calculer A^n, on écrit $A = 3P - I_3$ où $P = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ est un projecteur de rang 1. Écrivons $A = 2P - (I_3 - P)$; on a $A^n = 2^n P + (-1)^n (I_3 - P) = \frac{2^n - (-1)^n}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} + (-1)^n I_3$. Donc $a_{i,j}^{(n)} = \frac{2^n - (-1)^n}{3}$ si $i \neq j$ et $a_{i,i}^{(n)} = \frac{2^n - (-1)^n}{3} + (-1)^n = \frac{2^n + 2(-1)^n}{3}$.

2. Dans un hexagone régulier, il y a 2 triangles équilatéraux. Numérotons les sommets de l'hexagone en donnant les numéros de 1 à 3 aux sommets d'un des deux triangles, puis le numéro $3 + i$ au sommet opposé à i, de sorte que la matrice d'adjacence est ici $M = \begin{pmatrix} 0_3 & A \\ A & 0_3 \end{pmatrix}$ où A est la matrice rencontrée pour le triangle $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$. On trouve $M^n = \begin{pmatrix} A^n & 0_3 \\ 0_3 & A^n \end{pmatrix}$ si n est pair et $M^n = \begin{pmatrix} 0_3 & A^n \\ A^n & 0_3 \end{pmatrix}$ si n est impair. Il n'y a donc pas de chemin de longueur paire joignant un sommet au sommet opposé ; pour n impair, il y a $a_{i,i}^{(n)} = \frac{2^n - 2}{3}$ chemins joignant un sommet au sommet opposé.

3. Numérotons les sommets du pentagone de 1 à 5. Deux points sont joignables par un (unique) chemin de longueur 1 si et seulement s'ils sont distants de 1 modulo 5. En d'autres termes, le nombre $a_{i,j}$ de chemins de longueur 1 joignant i à j est donné par la matrice $A = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$. Le nombre $a_{i,j}^{(n)}$ de chemins de longueur n joignant les s i et j est alors donné par la matrice A^n. Pour calculer A^n, on diagonalise A. Notons que c'est une matrice circulante (*cf.* exercice **??**). On a donc, en posant $\omega = e^{2i\pi/5}$, $a = 2\cos(2\pi/5) = \frac{-1+\sqrt{5}}{2}$ et $b = 2\cos(4\pi/5) = \frac{-1-\sqrt{5}}{2}$,

$$A = \frac{1}{5}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}\begin{pmatrix} 2 & & & & \\ & a & & & \\ & & b & & \\ & & & b & \\ & & & & a \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \end{pmatrix}.$$

Il vient

$$A^n = \frac{1}{5}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}\begin{pmatrix} 2^n & & & & \\ & a^n & & & \\ & & b^n & & \\ & & & b^n & \\ & & & & a^n \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \end{pmatrix}.$$

On trouve donc qu'il y a
$a_{1,1}^{(n)} = \frac{1}{5}(2^n + 2a^n + 2b^n)$ chemins de longueur n joignant un sommet à lui même,
$a_{1,2}^{(n)} = \frac{1}{5}(2^n + a^{n+1} + b^{n+1})$ chemins de longueur n joignant un sommet à un sommet adjacent et

$a_{1,3}^{(n)} = \dfrac{1}{5}(2^n + ba^n + ab^n) = \dfrac{1}{5}(2^n - a^{n-1} - b^{n-1})$ chemins de longueur n joignant un sommet à un autre sommet non adjacent.

4. Numérotons les sommets du tétraèdre de 1 à 4. Deux points sont joignables par un (unique) chemin de longueur 1 si et seulement s'ils sont distincts. En d'autres termes, le nombre $a_{i,j}$ de chemins de longueur 1 joignant i à j est donné par la matrice $A = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$. Or $A = 3P - (I_4 - P)$ où P est l'idempotent $P = \dfrac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}$ de sorte que $A^n = 3^n P + (-1)^n(I_n - P)$.
   On a donc $a_{i,i}^{(n)} = \dfrac{3^n + (-1)^n.3}{4}$ et $a_{i,j}^{(n)} = \dfrac{3^n - (-1)^n}{4}$ pour $i \neq j$.
5. Dans un cube, il y a deux tétraèdres réguliers. Numérotons les sommets du cube en donnant les numéros de 1 à 4 aux sommets d'un des deux tétraèdres, puis le numéro $4 + i$ au sommet opposé à i, de sorte que la matrice d'adjacence est ici $M = \begin{pmatrix} 0_4 & A \\ A & 0_4 \end{pmatrix}$ où A est la matrice $\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ rencontrée pour le tétraèdre. On trouve $M^n = \begin{pmatrix} A^n & 0_4 \\ 0_4 & A^n \end{pmatrix}$ si n est pair et $M^n = \begin{pmatrix} 0_4 & A^n \\ A^n & 0_4 \end{pmatrix}$ si n est impair.
   Il n'y a pas de chemin de longueur paire joignant un sommet au sommet opposé. Si n est impair $\dfrac{3^n - 3}{4}$ chemins de longueur n joignent un sommet au sommet opposé.

Exercice 8.19.

1. On a $X_{k+1} = MX_k$ où $M = \begin{pmatrix} 0 & \frac{1}{4} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{4} \\ \frac{1}{2} & \frac{1}{4} & \frac{1}{2} \end{pmatrix}$.
2. Par récurrence, il vient $X_k = M^k X_0$.
   On peut diagonaliser la matrice M : Comme $LM = L$ où $L = (1\ 1\ 1)$, 1 est valeur propre. Un calcul démontre qu'un vecteur propre associé est $u = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}$. On peut aussi remarquer que $v = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$ vérifie $Mv = \frac{1}{4}v$. La somme des valeurs propres étant $\mathrm{Tr}(M) = 1$, $-\frac{1}{4}$ doit être valeur propre. On trouve un vecteur propre associé $w = \begin{pmatrix} 2 \\ -1 \\ -1 \end{pmatrix}$. On a donc $M = PDP^{-1}$ où $P = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & -1 \\ 2 & -1 & -1 \end{pmatrix}$ donc $P^{-1} = \dfrac{1}{10}\begin{pmatrix} 2 & 2 & 2 \\ 0 & 5 & -5 \\ 4 & -1 & -1 \end{pmatrix}$ et $D = \mathrm{diag}(1, \frac{1}{4}, -\frac{1}{4})$. On peut ainsi écrire $M = P_1 + \frac{1}{4}P_2 - \frac{1}{4}P_3$ où $P_1 = \dfrac{1}{5}\begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix}$, $P_2 = \dfrac{1}{2}\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 1 \end{pmatrix}$ et $P_3 = \dfrac{1}{10}\begin{pmatrix} 8 & -2 & -2 \\ -4 & 1 & 1 \\ -4 & 1 & 1 \end{pmatrix}$ vérifient $P_i^2 = P_i$ et $P_iP_j = 0$ pour $i \neq j$.
   Il vient $M^k = PD^kP^{-1} = P\mathrm{diag}(1, 4^{-k}, (-4)^{-k})P^{-1} = P_1 + 4^{-k}P_2 + (-4)^{-k}P_3$.

3. Les coefficients $m_{i,j}^k$ de M^k indiquent la probabilité qu'il fasse beau ($i=1$), qu'il fasse de l'orage ($i=2$) ou qu'il y ait une pluie fine ($i=3$) au temps k sachant qu'il fait beau ($j=1$) qu'il y a de l'orage ($j=2$) ou une pluie fine ($j=3$) au temps 0 (indice de colonne). S'il fait beau aujourd'hui, la probabilité qu'il fasse beau dans une semaine est donc $m_{1,1}^7 = \frac{1}{5} - 4^{-7}\frac{4}{5}$.
4. À long terme, il y a une probabilité de 20% d'avoir un beau jour, 40% d'avoir de l'orage et 40% d'avoir de la pluie fine.

Exercice 8.20. L'ensemble $F = \{P(u);\ P \in \mathbb{K}[X]\}$ est un sous-espace vectoriel de dimension finie de $L(E)$; il est fermé. Comme $\exp u$ est limite de la suite $P_n(u) = \sum_{k=0}^{n} \frac{u^k}{k!} \in F$, on a $\exp u \in F$.

Exercice 8.21.

1. Supposons que $u^{k+1} = 0$, et notons Q le polynôme $Q = \sum_{j=0}^{k-1} \frac{X^j}{(j+1)!}$. On a $\exp(u) = \mathrm{id}_E + v$, où $v = \sum_{j=1}^{k} \frac{1}{j!} u^j = u \circ Q(u)$, et puisque u et $Q(u)$ commutent, on a $v^{k+1} = u^{k+1} \circ Q(u)^{k+1} = 0$, donc $\exp u$ est unipotent.
2. Pour $t \in \mathbb{R}$, posons $f(t) = e^t - 1$ et, pour $t \in]-1, +\infty[$, posons $g(t) = \ln(1+t)$. Ces fonctions sont nulles en 0 et admettent, en 0 les développements limités $f(t) = E_k(t) + o(t^k)$ et $g(t) = L_k(t) + o(t^k)$. Par le théorème de composition des développements limités, on a $g \circ f(t) = L_k \circ E_k(t) + o(t^k)$ et $f \circ g(t) = E_k \circ L_k(t) + o(t^k)$. Or f et g sont réciproques l'une de l'autre, donc $L_k \circ E_k(t) = t + o(t^k)$ et $E_k \circ L_k(t) = t + o(t^k)$.
   Puisque $L_k \circ E_k(t) - t = o(t^k)$, tous les termes jusqu'au degré k du polynôme $L_k \circ E_k - X$ sont nuls, *i.e.* il existe un polynôme R_k tel que $L_k \circ E_k - X = X^{k+1} R_k$; de même, il existe un polynôme S_k tel que $E_k \circ L_k - X = X^{k+1} S_k$. On a donc $E_k(L_k(u)) = E_k \circ L_k(u) = u + u^{k+1} R_k(u) = u$ et $L_k(E_k(u)) = u$.
3. Notons $\mathcal{N}$ l'ensemble des matrices carrées d'ordre n nilpotentes et $\mathcal{U}$ l'ensemble des matrices carrées d'ordre n unipotentes. Si $u \in \mathcal{N}$, alors $u^n = 0$. Les applications $\exp : \mathcal{N} \to \mathcal{U}$ et $(id_E + u) \mapsto L_{n-1}(u)$ de $\mathcal{U}$ dans $\mathcal{N}$ sont polynomiales donc continues et, par la question 2 ce sont des bijections réciproques l'une de l'autre.
4. Soit $A \in GL_n(\mathbb{C})$. Écrivons $A = N + D$ sa décomposition de Dunford. Remarquons que, puisque N et A commutent, $A^{-1}N$ est une matrice nilpotente, donc $A^{-1}D = I_n - (A^{-1}N)$ est inversible (d'inverse $I_n + (A^{-1}N) + (A^{-1}N)^2 + ...$). On en déduit que D est inversible. On peut alors écrire $A = D(I_n + N_1)$, avec $N_1 = A^{-1}N$, où N_1 et D commutent, D est diagonalisable et N_1 est nilpotente.
   Posons $N_2 = L_{n-1}(N_1)$; on a $\exp N_2 = I_n + N_1$.
   Écrivons $D = P^{-1}\Delta P$ où $P \in GL_n(\mathbb{C})$ et $\Delta = \mathrm{diag}(\lambda_i)$ est diagonale. Soit $f : \mathbb{C}^* \to \mathbb{C}$ une détermination du logarithme complexe, et Q le polynôme d'interpolation de Lagrange satisfaisant $Q(\lambda) = f(\lambda)$ pour toute valeur propre de Δ. On a donc $Q(\Delta) = \mathrm{diag}(Q(\lambda_i)) = \mathrm{diag}(f(\lambda_i))$ et $\exp(Q(\Delta)) = \mathrm{diag}(\exp(Q(\lambda_i))) = \Delta$.
   Puisque $Q(D) = P^{-1}Q(\Delta)P$, il vient $\exp(Q(D)) = P^{-1}\exp(Q(\Delta))P = D$.
   Puisque D et N_1 commutent, $Q(D)$ et $N_2 = L_{n-1}(N_1)$ commutent, donc

$$\exp(Q(D) + N_2) = \exp(Q(D))\exp(N_2) = D(I_n + N_1) = A.$$

11.9 Formes quadratiques

Exercice 9.1.

1. Le vecteur e_i est orthogonal à tous les e_j pour $j \neq i$ car la base $(e_1, \ldots, e_n)$ est orthogonale et à e_i car il est isotrope. Il s'ensuit que $e_i^\perp = E$, donc $e_i \in \ker q$.
2. Notons φ la forme polaire de q. Soit $x = \sum_{i=1}^{n} \lambda_i e_i$ un élément de E. On a $\varphi(x, e_i) = \lambda_i q(e_i)$. On a donc $x \in \ker q$ si et seulement si on a $\lambda_i q(e_i) = 0$ pour tout i, *i.e.* si $\lambda_i = 0$ pour tout $i \notin J$, *i.e.* si et seulement si $x \in \mathrm{Vect}\{e_i;\ i \in J\}$.

Exercice 9.2. L'application qui à une forme quadratique associe sa matrice (dans la base canonique) est un isomorphisme entre l'espace des formes quadratiques sur K^n et celui des matrices symétriques à coefficients dans K. La dimension de ces deux espaces est $\dfrac{n(n+1)}{2}$.

Exercice 9.3.

1. Si q est une forme quadratique sur $\mathbb{R}^n$, l'application $x \mapsto q(x)$ est continue donc bornée sur le compact S, ce qui donne un sens à l'application N. Si $q(x) = 0$ pour tout $x \in S$, alors pour tout $y \in \mathbb{R}^n$ non nul, on aura $q(y) = \|y\|^2 q(\|y\|^{-1} y) = 0$ par homogénéité, donc $q = 0$.
   Pour $\lambda \in \mathbb{R}$, on a $N(\lambda q) = \sup\{|\lambda||q(x)|;\ x \in S\} = |\lambda| N(q)$.
   Si q_1 et q_2 sont deux formes quadratiques sur $\mathbb{R}^n$, pour tout $x \in S$ on a $|(q_1 + q_2)(x)| \leqslant |q_1(x)| + |q_2(x)| \leqslant N(q_1) + N(q_2)$; prenant le sup sur $x \in S$, il vient $N(q_1 + q_2) \leqslant N(q_1) + N(q_2)$.
2. L'application Δ qui à une forme quadratique associe le déterminant de sa matrice est polynomiale donc continue. L'ensemble des formes quadratiques non dégénérées est $\Delta^{-1}(\mathbb{R}^*)$. Il est ouvert.
   Soit q une forme quadratique et notons A sa matrice dans la base canonique de $\mathbb{R}^n$. Pour $k \in \mathbb{N}$, si $\dfrac{1}{k+1}$ n'est pas une valeur propre de A, la forme quadratique q_k de matrice $A - \lambda I_n$ est non dégénérée. Comme A possède un nombre fini de valeurs propres, q_k est non dégénérée pour k assez grand, donc q est limite d'une suite de formes quadratiques non dégénérées.
3. Soit q une forme quadratique de signature $(p, n-p)$. Il existe des sous-espaces E et F de $\mathbb{R}^n$ tels que $\dim E = p$, $\dim F = n - p$ et les restrictions de q à E et à F sont non dégénérées positive et négative respectivement. Posons $\alpha = \inf\{|q(x)|;\ x \in E \cup F;\ \|x\| = 1\}$. Avec les notations de l'exercice précédent, si $N(q - q') < \alpha$, restrictions de q' à E et à F sont non dégénérées positive et négative respectivement, donc la signature de q' est $(p, n-p)$.
4. Soit $q \in Q^*$ et notons $(p, n-p)$ sa signature.
   Notons T_p l'ensemble des formes quadratiques de signature $(p, n-p)$. Le complémentaire de T_p dans Q^* est la réunion des T_k pour $k \neq p$; il est ouvert. Donc T_p est ouvert et fermé dans Q^*. Si C est la composante connexe de q dans Q^*, l'ensemble $C \cap T_p$ est ouvert et fermé dans C, non vide car il contient q, donc $C \cap T_p = C$, autrement dit C est contenu dans T_p.
   Si $q' \in T_p$, il existe des bases $B = (e_1, \ldots, e_p, e_{p+1}, \ldots, e_n)$ et $B' = (e'_1, \ldots, e'_p, e'_{p+1}, \ldots, e'_n)$ orthogonales pour q et q' respectivement, telles que $q(e_i) = 1 = q'(e'_i)$ pour $1 \leqslant i \leqslant p$ et $q(e_i) = -1 = q'(e'_i)$ pour $p+1 \leqslant i \leqslant n$. Notons alors $f \in GL(\mathbb{R}^n)$ l'automorphisme tel que $f(e'_i) = e_i$. On a $q \circ f = q'$. Quitte à remplacer e'_1 par $-e'_1$, on peut de plus supposer que $\det f > 0$. Inversement, si q' s'écrit $q \circ f$ avec $f \in GL(\mathbb{R}^n)$, la matrice de q' dans la base $f^{-1}(B)$ est celle de q dans la base B, donc $q' \in T_p$.
   On en déduit que $T_p = \{q \circ f;\ f \in GL(\mathbb{R}^n)_+\}$ où on a noté $GL(\mathbb{R}^n)_+$ l'ensemble des automorphismes de $\mathbb{R}^n$ de déterminant > 0. Comme $GL(\mathbb{R}^n)_+$ est connexe par arcs, et $f \mapsto q \circ f$ est continue (si A et P sont les matrices de q et f dans la base canonique, celle de $q \circ f$ est ${}^tPAP$), on en déduit que T_p est connexe (par arcs). C'est la composante connexe de q.

Exercice 9.4.

1. Soit H un hyperplan de E. Notons (r', s') la signature de la restriction de q à H. Soit F un sous-espace de H de dimension r' tel que la restriction de q à F soit définie positive et soit G un sous-espace de dimension r de E contenant F tel que la restriction de q à G soit définie positive. On a $F = H \cap G$, donc $r - 1 \leqslant r' \leqslant r$.
   De même, $s - 1 \leqslant s' \leqslant s$.

2. a) Soit $k \in \{0, \dots, n-1\}$. Puisque q est non dégénérée, on a $\dim E_k^\perp = n - k$. On en déduit que $E_k^\perp \cap E_{k+1}$ n'est pas nul. Soit e_{k+1} un vecteur non nul de $E_k^\perp \cap E_{k+1}$. Puisque la restriction de q à E_k est non dégénérée, il vient $E_k^\perp \cap E_k = \{0\}$, donc $e_{k+1} \notin E_k$. On en déduit que $E_{k+1} = E_k \oplus \mathbb{R}e_{k+1}$. Par récurrence sur k, $(e_1, \dots, e_k)$ est une base de E_k.
   Enfin, pour $j \neq k$, par exemple $j < k$, on a $e_j \in E_j \subset E_{k-1}$ et $e_k \in E_{k-1}^\perp$, donc la base $(e_1, \dots, e_n)$ de E est orthogonale.

   b) Le signe de $\det A_k$ ne dépend pas de la base de E_k (dans une autre base, on a $A'_k = {}^tPA_kP$ où P est une matrice de passage donc $\det A'_k = (\det P)^2 \det A_k$).
   Fixons une base $(e_1, \dots, e_n)$ orthogonale pour q donnée par la question précédente. Alors $(e_1, \dots, e_n)$ est une base de E_k. Dans cette base, on a $\det A_{k+1} = q(e_{k+1}) \det A_k$, donc $\det A_{k+1}$ et $\det A_k$ sont de signe opposé si et seulement si $q(e_{k+1})$ est négatif. Le nombre de changements de signe est donc le nombre de e_k avec $q(e_k) < 0$.

Exercice 9.5. Rappelons qu'une équation du type $q(x) = 1$ est celle d'un ellipsoïde si q est définie positive, un hyperboloïde à une nappe si la signature de q est $(2, 1)$ et un hyperboloïde à deux nappes si la signature de q est $(1, 2)$.

Pour trouver la signature de q peut utiliser la réduction de Gauss. On écrit donc $xy + yz + zx = (x + z)(y + z) - z^2 = X^2 - Y^2 - Z^2$ où $X = \dfrac{x + y + 2z}{2}$, $Y = \dfrac{x - y}{2}$ et $z = Z$. Ces formes linéaires sont des coordonnées dans la base $(e_1 + e_2, e_1 - e_2, e_3 - e_1 - e_2)$. Dans cette nouvelle base, l'équation est $X^2 - Y^2 - Z^2 + 1 = 0$. La quadrique est un hyperboloïde à une nappe.

Si on cherche à étudier les propriétés métriques de notre quadrique, on doit la réduire dans une base orthonormée. Cela revient à diagonaliser la matrice $\begin{pmatrix} 0 & 1/2 & 1/2 \\ 1/2 & 0 & 1/2 \\ 1/2 & 1/2 & 0 \end{pmatrix}$ de b dans une base orthonormée de $\mathbb{R}^3$. Ses valeurs propres sont 1 et $-1/2$ (avec multiplicité 2) et une base orthoormée de vecteurs propres est $e_1 = 1/\sqrt{3}(1, 1, 1)$, $e_2 = 1/\sqrt{2}(1, -1, 0)$ et $e_3 = 1/\sqrt{6}(1, 1, -2)$. Dans cette base orthonormée l'équation de notre quadrique est $2X^2 - Y^2 - Z^2 + 2 = 0$. On en déduit que c'est un hyperboloïde (à une nappe évidemment) de révolution (autour de l'axe des X).

Remarquons que l'on pouvait prévoir que cette quadrique est un hyperboloïde de révolution : elle contient $\{(t, -1/t, 0);\ t \in \mathbb{R}^*\}$ donc elle n'est pas bornée : ce n'est pas un ellipsoïde. Elle est invariante par les permutations des axes, par exemple $(x, y, z) \mapsto (y, z, x)$ qui est d'ordre 3. Elle a donc deux valeurs propres confondues (par la remarque concluant notre discussion sur les quadriques). Reste à vérifier qu'elle est non dégénérée et calculer sa signature pour savoir combien elle a de nappes.

Exercice 9.6. Posons $q(M) = Tr(M^2)$. L'application $b : (M, N) \mapsto Tr(MN)$ est une forme bilinéaire. Elle est symétrique d'après la propriété de la trace. C'est donc la forme polaire de q. Si $M = (a_{i,j})$ est dans le noyau de q, alors $0 = b(M, {}^tM) = \sum_{i,j} a_{i,j}^2$, donc $M = 0$. Notons $(k, n^2 - k)$ sa signature. La restriction de q au sous-espaces $\mathcal{S}$ (*resp.* $\mathcal{A}$) des matrices symétriques (*resp.* antisymétriques) est définie positive. Il vient $k \geqslant \dfrac{n(n+1)}{2}$ (*resp.* $n^2 - k \geqslant \dfrac{n(n-1)}{2}$. Donc la signature de q est $\Big(\dfrac{n(n+1)}{2}, \dfrac{n(n-1)}{2}\Big)$.

Notons que $\mathcal{S}$ et $\mathcal{A}$ sont orthogonaux pour q : si $M \in \mathcal{S}$ et $N \in \mathcal{A}$, il vient $Tr(MN) = Tr({}^t(MN)) = -Tr(NM) = -Tr(MN)$ donc $Tr(MN = 0)$.

Exercice 9.7. Notons (r,s) la signature de q. Démontrons que cette dimension maximale est $n - \max(r,s)$.

Quitte à changer q en $-q$ on peut supposer que $r \geqslant s$. Dans une base $(e_1,\dots,e_n)$ bien choisie, q s'écrit $q(\sum_{i=1}^{n} x_i e_i) = \sum_{k=1}^{r} x_k^2 - \sum_{k=r+1}^{r+s} x_k^2$. Les vecteurs $e_i - e_{i+r}$ pour $i = 1,\dots,s$ et les vecteurs e_ℓ avec $\ell > r+s$ sont deux à deux orthogonaux et isotropes donc engendrent un espace totalement isotrope de dimension $n-r$.

Par ailleurs, tout sous-espace de dimension $p > n-r$ a une intersection non nulle avec $\mathrm{Vect}(e_1,\dots,e_r)$ donc contient des vecteurs non isotropes.

Exercice 9.8. Commençons par la question 2. Notons φ la forme polaire de q et définissons les applications linéaires $f : F \to G^*$ qui à $x \in F$ associe la forme linéaire $y \mapsto \varphi(x,y)$ sur G et $g : G \to F^*$ qui à $y \in G$ associe la forme linéaire $x \mapsto \varphi(x,y)$ sur F. Soit $(u_1,\dots,u_n)$ une base de F et $(v_1,\dots,v_p)$ une base de G. Notons $A \in M_{n,k}(K)$ la matrice $(a_{k,\ell})$ où pour $1 \leqslant k \leqslant n$ et $1 \leqslant \ell \leqslant p$ on pose $a_{k\ell} = \varphi(u_k, v_\ell)$. La matrice de f dans les bases $(u_1,\dots,u_n)$ et $(v_1^*,\dots,v_p^*)$ est ${}^tA$; la matrice de g dans les bases $(v_1,\dots,v_p)$ et $(u_1^*,\dots,u_n^*)$ est A, donc f et g ont le même rang. Or $\ker f = \{x \in F;\ \forall y \in G,\ \varphi(x,y) = 0\} = F \cap G^\perp$ et $\ker g = G \cap F^\perp$. Il vient

$$\dim F - \dim(F \cap G^\perp) = \mathrm{rg} f = \mathrm{rg} g = \dim G - \dim(F^\perp \cap G).$$

Prenant $G = E$, on retrouve la question 1, puisque $E^\perp = \ker q$.

Exercice 9.9.

1. En effet $F + Kx$ est totalement isotrope et contient F : il est donc égal à F (en particulier, on a $\ker q \subset F$).
2. Puisque F est totalement isotrope, on a $F \subset F^\perp$, donc $F \cap G \subset F^\perp \cap G$. Si $x \in F^\perp \cap G$, il est isotrope (car $x \in G$), donc $x \in F$ d'après la question 1.
3. Échangeant les rôles de F et G, il vient $G^\perp \cap F = F \cap G = F^\perp \cap G$. Or, d'après l'exercice 9.8, on a $\dim F - \dim(G^\perp \cap F) = \dim G - \dim(F^\perp \cap G)$.

Exercice 9.10.

1. On a ou bien $F = \sigma(F) = E$ et on pose $\tau = \sigma$; ou bien $F = \sigma(F) = \{0\}$ et on pose $\tau = \mathrm{id}_E$.
2. a) Puisque x et y sont orthogonaux, on a $q(x+y) = q(x) + q(y)$. Il vient $q(x + \sigma(y)) = q(\sigma((x+y)) = q(x) + q(y) = q(x) + q(\sigma(y))$, donc $\sigma(y) \in x^\perp$.
   b) La restriction q_1 de q à E_1 est non dégénérée, puisque $E_1^\perp = (x^\perp)^\perp = Kx$ et $Kx \cap E_1 = 0$ (x étant non isotrope). Notons $\sigma_1 : F_1 \to E_1$ la restriction de σ. Par l'hypothèse de récurrence, il existe $\tau_1 \in O(q_1)$ qui prolonge σ_1). L'application $\tau : \lambda x + y \mapsto \lambda x + \tau_1(y)$ convient (pour $\lambda \in K$ et $y \in E_1$).
3. a) On a $q(x+y) + q(x-y) = 2q(x) + 2q(y) = 4q(x) \neq 0$ puisque $q(y) = q(\sigma(x)) = q(x)$.
   b) Notons φ la forme polaire de q. On a $\varphi(x+y, x-y) = q(x) - q(y) = 0$; si $x+y$ n'est pas isotrope, on peut prendre $G = K(x+y)$; si $x-y$ n'est pas isotrope, on peut prendre $G = (x-y)^\perp$.
   c) La symétrie τ_1 définie par $\tau_1(u+v) = u - v$ pour $u \in G$ et $v \in G^\perp$ convient.
   d) Notons $\sigma_1 : F \to E$ l'application $u \mapsto \tau_1^{-1}(\sigma(u))$. On a $\sigma_1(x) = x$. Par la question 2, L'application σ_1 se prolonge en un élément $\tau_2 \in O(q)$. On pose alors $\tau = \tau_1 \circ \tau_2$.
4. a) On peut prolonger ℓ en une forme linéaire $\ell_1 \in E^*$; or l'application $x \mapsto \varphi(x,.)$ est bijective de E sur E^* puisque q est non dégénérée.

b) Soit x_0 tel qu'on ait $\varphi(x_0, y) = \ell(z)$ pour tout $z \in F$; soit $y \in F$ tel que $\ell(y) \neq 0$. Pour $\lambda \in K$, on a $q(x_0 + \lambda y) = q(x_0) + 2\lambda\ell(y)$ (puisque y est isotrope). On peut choisir λ tel que $x = x_0 + \lambda y$ soit isotrope. Pour $z \in F$, on a $\varphi(y, z) = 0$ (car F est totalement isotrope), donc $\varphi(x, z) = \varphi(x_0, z) = \ell(z)$.

c) Notons $\sigma' : \sigma(F) \to F$ l'application réciproque de σ. Pour $y \in \sigma(F)$, on a $q(y) = q(\sigma(\sigma'(y))) = q(\sigma'(y)) = 0$, donc $\sigma(F)$ est totalement isotrope. Appliquant la question précédente à $\ell \circ \sigma'$, on trouve un élément isotrope $x' \in E$ tel qu'on ait $\varphi(x', \sigma(y)) = \ell(y)$ pour tout $y \in F$.
Pour $\lambda \in K$ et $y \in F$, posons $\overline{\sigma}(y + \lambda x) = \sigma(y) + \lambda x'$. Remarquons que puisque ℓ n'est pas nulle, on a $x \notin F$ et $x' \notin \sigma(F)$, donc $\overline{\sigma}$ est bien définie et injective. Pour tout $y \in F$ et $\lambda \in K$, puisque x, x', y et $\sigma(y)$ sont isotropes, on a $q(\overline{\sigma}(y+\lambda x)) = 2\lambda\varphi(\sigma(y), x') = 2\lambda\ell(y) = q(y+\lambda x)$.

d) L'espace $F \oplus Kx$ n'étant pas isotrope, l'application $\overline{\sigma}$ se prolonge (d'après la question 3) en un élément de $O(q)$.

Exercice 9.11. Soient $S, T \in M_+(n, \mathbb{R})$. Pour $\lambda \in \mathbb{R}_+$, notons $E_\lambda(S)$ et $E_\lambda(T)$ les espaces propres de S et T de valeur propre λ. Notons $\lambda_1, \ldots, \lambda_p$ les valeurs propres de T. Supposons que $S^2 = T$. Remarquons que si λ est une valeur propre de S alors $\lambda \geqslant 0$ et λ^2 est une valeur propre de T et $E_\lambda(S) \subset E_{\lambda^2}(T)$. Donc les valeurs propres de S sont les $\sqrt{\lambda_j}$. Comme S est diagonalisable, on a $\bigoplus_{j=1}^{k} E_{\sqrt{\lambda_j}}(S) = \mathbb{R}^n$; puisque la somme des espaces propres de T est directe, on en déduit que $E_{\sqrt{\lambda_j}}(S) = E_{\lambda_j}(T)$. En d'autres termes S est l'unique opérateur tel que $S(x) = \sum_{j=1}^{k} \sqrt{\lambda_j} x_j$ si on écrit $x = \sum_{j=1}^{k} x_j$ dans la décomposition $\mathbb{R}^n = \bigoplus_{j=1}^{k} E_{\lambda_j}(T)$. L'application $T \mapsto T^2$ est donc bijective de $M_+(n, \mathbb{R})$ dans $M_+(n, \mathbb{R})$.

Exercice 9.12. Voir décomposition d'Iwasawa, analyse p. **??**. On peut aussi en donner directement une démonstration utilisant la décomposition de Cholesky, démontrée dans l'exercice **??**.

La matrice A^*A est définie positive (pour tout $X \in \mathbb{K}^n$ non nul, on a $X^*A^*AX = (AX)^*AX \in \mathbb{R}_+^*$). D'après la décomposition de Cholesky, (exerc. **??**), il existe une matrice triangulaire supérieure T dont les coefficients diagonaux sont (réels et) strictement positifs telle que $T^*T = A^*A$. Posons $Q = AT^{-1}$ Alors

$$Q^*Q = (AT^{-1})^*(AT) = (T^{-1})^*A^*AT^{-1} = (T^{-1})^*T^*TT^{-1} = I_n$$

Donc Q est unitaire et $A = QT$.

Si $Q_1T_1 = Q_2T_2$, alors $T_1^*T_1 = T_1^*Q_1^*Q_1T_1 = T_2^*Q_2^*Q_2T_2 = T_2^*T_2$, donc $T_1 = T_2$ par l'unicité dans la décomposition de Choelsky. Enfin $Q_1 = (Q_1T_1)T_1^{-1} = Q_2$.

Exercice 9.13.

1. Posons $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. On a

$$ {}^tMM - M{}^tM = \begin{pmatrix} c^2 - b^2 & ab + cd - ac - bd \\ ab + cd - ac - bd & b^2 - c^2 \end{pmatrix} = (b - c) \begin{pmatrix} -b - c & a - d \\ a - d & b + c \end{pmatrix}, $$

de sorte que ${}^tMM = M{}^tM$ si et seulement si $b = c$ ou si $a = d$ et $b = -c$.

2. Le calcul par blocs de ${}^tMM$ et $M{}^tM$ donne en bloc en haut à gauche l'égalité ${}^tAA = A{}^tA + B{}^tB$. Prenant la trace, puisque $Tr({}^tAA) = Tr(A{}^tA)$, il vient $Tr(B{}^tB) = 0$; or, si $B = (b_{i,j})$, on a $0 = Tr(B{}^tB) = \sum_{i,j} b_{i,j}^2$, donc $B = 0$.

Enfin ${}^tMM = \begin{pmatrix} {}^tAA & 0 \\ 0 & {}^tCC \end{pmatrix}$ et $M{}^tM = \begin{pmatrix} A{}^tA & 0 \\ 0 & C{}^tC \end{pmatrix}$, donc A et C sont normales.

3. On raisonne par récurrence sur la dimension n de E.
   - Si $n = 1$, alors M est diagonale.
   - Supposons $n \geqslant 2$ et le résultat connu pour toutes les matrices normales de taille $< n$. Si M a une valeur propre réelle λ, on note $e_1 \in \mathbb{R}^n$ un vecteur colonne propre associé de norme 1 ; complétons le en une base orthonormée $(e_1, \dots, e_n)$. Posons dans ce cas $F = \mathbb{R}e_1$. Sinon, d'après le lemme 9.33, il existe un sous-espace F de $\mathbb{R}^n$ de dimension 2 stable par l'application $X \mapsto MX$. Prenons une base orthonormée $(e_1, \dots, e_n)$ de $\mathbb{R}^n$ telle que e_1, e_2 soit une base de F. Dans tous les cas F est stable. Notons $d = 1$ ou 2 sa dimension.
     Comme F est stable, on a $M = UM'U^{-1}$ où U est la matrice de passage de la base canonique à la base $(e_1, \dots, e_n)$: c'est une matrice de passage entre bases orthonormées donc U est orthogonale et où M' est de la forme $\begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$ où A est une matrice $d \times d$. Alors, comme U est orthogonale, la matrice M' est normale. On en déduit que $B = 0$ et A et C sont normales d'après la question 2. Si $d = 2$, comme A n'a pas de valeurs propres réelles, c'est une matrice de similitude directe d'après la question 1. D'après l'hypothèse de récurrence, il existe $U_1 \in O_{n-d}$ telle $U_1^{-1}CU_1$ soit de la forme voulue. Alors
     $$\begin{pmatrix} I_d & 0 \\ 0 & U_1^{-1} \end{pmatrix} U^{-1}MU \begin{pmatrix} I_d & 0 \\ 0 & U_1 \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & U_1^{-1}CU_1 \end{pmatrix}$$
     a la forme voulue.
4. On a démontré que, pour tout endomorphisme normal u, il existe une base orthonormée de E dans laquelle la matrice de u est de la forme $M = \begin{pmatrix} D & 0 \\ 0 & D_1 \end{pmatrix}$ où $D = \mathrm{diag}(\lambda_i)$ est diagonale et $D_1 = \mathrm{diag}(S_i)$ est diagonale par blocs 2×2, les $S_i = \begin{pmatrix} a_i & -b_i \\ b_i & a_i \end{pmatrix}$ étant des matrices de similitudes directes.
   Si u est orthogonale (*resp.* antisymétrique) il en va de même pour D et D_1, donc les λ_i sont égaux à ± 1 (*resp.* nuls) et $a_i^2 + b_i^2 = 1$ (*resp.* $a_i = 0$).

11.10 Géométrie affine en dimension finie

Exercice 10.1. Soit $A \in E$. Pour $M \in E$, on a $\overrightarrow{Af(M)} = \overrightarrow{Af(A)} + \vec{f}(\overrightarrow{AM})$, donc $f(M) = M \iff \overrightarrow{Af(A)} = (\mathrm{id}_{\vec{E}} - \vec{f})(\overrightarrow{AM})$. L'application $\mathrm{id}_{\vec{E}} - \vec{f}$ étant bijective, l'existence et unicité en découlent.

Exercice 10.2. Soit f est une telle application, et soient A, B deux points distincts de E. Alors $A' = f(A)$ et $B' = f(B)$ sont distincts (car f est injective) et les droites (AB) et $(A'B')$ étant parallèles, il existe $\lambda \in K^*$ tel que $\overrightarrow{A'B'} = \lambda\overrightarrow{AB}$. Soit alors h l'homothétie translation de rapport λ et telle que $h(A) = h(A')$. L'application $g = h^{-1} \circ f$ envoie toute droite en une droite parallèle et de plus on a $g(A) = A$ et $g(B) = B$. En particulier, si D est une droite passant par A (*resp.* B), alors $g(D)$ est la droite parallèle à D et passant par A (*resp.* B), donc $g(D) = D$. Si $M \in E \setminus (AB)$, alors $g(M) \in g((AM)) = (AM)$ et $g(M) \in g((BM)) = (BM)$, donc $g(M) \in (AM) \cap (BM) = \{M\}$. Comme $\dim E \geqslant 2$, il existe $C \in E \setminus (AB)$. Par ce qui précède $g(C) = C$, et, appliquant ce qui précède à A, C, on trouve que $g(M) = M$ pour tout $M \notin (AC)$. Cela prouve que g fixe tout point de (AB) (distinct de A), donc que $g = \mathrm{id}_E$, soit $f = h$.

Exercice 10.3. On a $F \cap G \neq \emptyset \iff \exists M \in E;\ \overrightarrow{AM} \in \overrightarrow{F}$ et $\overrightarrow{MB} \in \overrightarrow{G} \iff \overrightarrow{AB} \in \overrightarrow{F} + \overrightarrow{G}$.

Exercice 10.4. Rappelons que deux droites qui se coupent sont coplanaires. Soient $d_1, d_2 \in \mathcal{D}$ deux droites distinctes. Notons A leur point d'intersection et P le plan qui contient d_1 et d_2. On suppose

qu'au moins une droite $d_3 \in \mathcal{D}$ ne passe pas par A. Elle coupe d_1 en un point B et d_2 en un point C. Ces deux points sont distincts de A, donc distincts, donc $d_3 = (BC) \subset P$. Soit $d \in \mathcal{D}$. Par ce qui précède, si $A \notin d$ alors $d \subset P$. Si $A \in d$, comme d coupe d_3 en un point M distinct de A, on a $d = (AM)$, donc $d \subset P$.

Exercice 10.5. Le gradient de $\psi : M \mapsto \|AM\|^2$ est $2\overrightarrow{AM}$ (*i.e.* $d\psi_M(\vec{v}) = 2\langle\overrightarrow{AM}|\vec{v}\rangle$). Donc M est un point critique pour φ si et seulement si $\sum \lambda_i \overrightarrow{A_iM} = 0$.

- Supposons que $\sum \lambda_i \neq 0$, alors le seul point critique est le barycentre G des (A_i, λ_i). Dans ce cas, on a

$$\begin{aligned}\varphi(M) &= \sum_{i=1}^{n} \lambda_i \|(\overrightarrow{A_iG} + \overrightarrow{GM})\|^2 \\ &= \sum_{i=1}^{n} \lambda_i (\|\overrightarrow{A_iG}\|^2 + \|GM\|^2) + \Big\langle \sum \lambda_i \overrightarrow{A_iG} | \overrightarrow{GM} \Big\rangle \\ &= \varphi(G) + \Big(\sum \lambda_i\Big)\|GM\|^2.\end{aligned}$$

  Donc G est un maximum si $\sum \lambda_i < 0$ et un minimum si $\sum \lambda_i > 0$.
- Si $\sum \lambda_i = 0$, le gradient de φ est constant égal à $\vec{v} = 2\sum \lambda_i \overrightarrow{A_iA}$ (ce vecteur ne dépend pas de $A \in E$) et φ est affine : on a

$$\begin{aligned}\varphi(M) &= \sum_{i=1}^{n} \lambda_i (\|\overrightarrow{A_iA}\|^2 + \|AM\|^2) + 2\Big\langle \sum \lambda_i \overrightarrow{A_iA} | \overrightarrow{AM} \Big\rangle \\ &= \varphi(A) + \big\langle \vec{v} | \overrightarrow{AM} \big\rangle.\end{aligned}$$

Exercice 10.6. L'ensemble $T = \{(x,t) \in C \times \mathbb{R};\ f(x) \leqslant t\}$ est une partie convexe de $E \times \mathbb{R}$, donc $T \cap (E \times]-\infty, a[)$ et $T \cap (E \times]-\infty, a])$ sont convexes, ainsi que leur image par la projection $p : (x,t) \mapsto x$.

Exercice 10.7.

1. C'est essentiellement la définition puisque le centre de gravité est l'isobarycentre de A, B et C. Notons cependant que l'on a $G = \frac{1}{3}A + \frac{2}{3}\Big(\frac{B+C}{2}\Big)$, de sorte que G est bien situé sur la médiane : droite joignant A au milieu de B et C - et de même pour les deux autres médianes.
2. a) Soit $(0, \vec{i}, \vec{j})$ un repère orthonormé. Les affixes de A, B, C ont même module si et seulement si $OA = OB = OC$, c'est à dire si et seulement si O est le centre du cercle circonscrit à ABC.

   b) L'existence de z, s, t résultent de ce que les affixes de A, B, C sont de même module et distincts. D'après la propriété de l'angle au centre, $s = 2\hat{B}$ et $t = 2\hat{C}$ modulo 2π.

   c) On a $z_A(\sin 2\hat{A}) + z_B(\sin 2\hat{B}) + z_C(\sin 2\hat{C}) = z\Big(\sin(2\pi - s - t) + (\sin t)e^{is} + (\sin s)e^{-it}\Big) = 0$; donc le barycentre de $\big((A, \sin 2\hat{A}), (B, \sin 2\hat{B}) + (C, \sin 2\hat{C})\big)$ est le centre O du cercle circonscrit du triangle ABC.
3. a) Dans le triangle $AA'B$, rectangle en A', on a $A'B = |\operatorname{cotan}\hat{B}|AA'$. De même $A'C = |\operatorname{cotan}\hat{C}|AA'$. Lorsque les angles $\hat{B}$ et $\hat{C}$ sont aigus, on en déduit que $\tan\hat{B}\,\overrightarrow{A'B} + \tan\hat{C}\,\overrightarrow{A'C} = \vec{0}$. Cette même égalité reste vraie lorsque un des angles $\hat{B}$ ou $\hat{C}$ est obtus : dans ce cas, $\overrightarrow{A'B}$ et $\overrightarrow{A'C}$ ont même sens mais $\tan\hat{B}$ et $\tan\hat{C}$ sont de signes opposés.

b) On a $\tan\hat{A}\,\overrightarrow{HA}+\tan\hat{B}\,\overrightarrow{HB}+\tan\hat{C}\,\overrightarrow{HC}=\tan\hat{A}\,\overrightarrow{HA}+(\tan\hat{B}+\tan\hat{C})\overrightarrow{HA'}$. On en déduit que le vecteur $\tan\hat{A}\,\overrightarrow{HA}+\tan\hat{B}\,\overrightarrow{HB}+\tan\hat{C}\,\overrightarrow{HC}$ est colinéaire à $\overrightarrow{AA'}$; de même, il est colinéaire à $\overrightarrow{BB'}$ et $\overrightarrow{CC'}$. Il est donc nul. Notons que, si le triangle ABC est rectangle disons en A, alors l'orthocentre est A et $\tan\hat{A}=\infty$. Le résultat reste cohérent...

4. a) La bissectrice intérieure de deux demi droites non opposées dirigées par des vecteurs unitaires $\vec{u}$ et $\vec{v}$ est dirigée par $\vec{u}+\vec{v}$.

   b) On a $BC\,\overrightarrow{IA}+CA\,\overrightarrow{IB}+AB\,\overrightarrow{IC}=(BC+CA+AB)\,\overrightarrow{IA}+CA.AB\left(\dfrac{\overrightarrow{AB}}{AB}+\dfrac{\overrightarrow{AC}}{AC}\right)$. Ce vecteur est colinéaire à $\overrightarrow{IA}$ - et de même à $\overrightarrow{IB}$ (et à $\overrightarrow{IC}$) donc il est nul.

   c) On a $\dfrac{\sin\hat{A}}{BC}=\dfrac{\sin\hat{B}}{CA}=\dfrac{\sin\hat{C}}{AB}$ d'où le résultat.

Exercice 10.8.

1. Si d divise a et a' et $d\geqslant 2$, alors $M+\dfrac{1}{d}\vec{u}\in\,]M,M+\vec{u}[\,\cap\mathbb{Z}^2$, donc M et $M+\vec{u}$ ne sont pas visibles l'un de l'autre.

   Supposons a et a' premiers entre eux et écrivons une relation de Bézout $sa+s'a'=1$. Soit $\lambda\in\mathbb{R}$; si $A+\lambda\vec{u}\in\mathbb{Z}^2$, il vient $\lambda a\in\mathbb{Z}$ et $\lambda a'\in\mathbb{Z}$ donc $\lambda=(\lambda a)s+(\lambda a')s'\in\mathbb{Z}$. Donc, pour $\lambda\in\,]0,1[$, on a $M+\lambda\vec{u}\notin\mathbb{Z}^2$, soit $]M,M+\vec{u}[\,\cap\mathbb{Z}^2=\emptyset$.

2. a) Comme a et a' sont premiers entre eux, il existe $s,s'\in\mathbb{Z}$ tels que $as+a's'=1$. Posons alors $P=\begin{pmatrix}a & -s'\\ a' & s\end{pmatrix}$. On a bien $\det P=1$ et $\begin{pmatrix}a\\ a'\end{pmatrix}=P\begin{pmatrix}1\\ 0\end{pmatrix}$.

   b) L'application f linéaire de $\mathbb{R}^2$ dans $\mathbb{R}^2$ de matrice P, envoie $\mathbb{Z}^2$ sur $\mathbb{Z}^2$ (puisque P et P^{-1} sont à coefficients entiers). De plus, comme elle préserve les barycentres, elle envoie l'intérieur de $\mathcal{P}(O,\vec{i},\vec{w})$ sur l'intérieur de $\mathcal{P}(O,\vec{u},\vec{v})$. Elle induit donc une bijection de l'ensemble de points de $\mathbb{Z}^2$ situés dans ces intérieurs.

   c) Remarquons d'abord que puisque $f(]O,O+\vec{w}[\,\cap\mathbb{Z}^2)=\,]O,O+\vec{v}[\,\cap\mathbb{Z}^2=\emptyset$ les points O et $O+\vec{w}$ sont visibles l'un de l'autre. Pour $k\in\mathbb{Z}$ compris strictement entre 0 et c', la droite $y=k$ rencontre l'intérieur du parallélogramme $\mathcal{P}(0,\vec{i},\vec{w})$ en un intervalle de la forme $](k,t_k),(k,t_k+1)[$ (avec $t_k=\dfrac{kc}{c'}$). Comme les points O et $O+\vec{w}$ sont visibles l'un de l'autre, t_k n'est pas entier, donc la droite $y=k$ rencontre l'intérieur du parallélogramme $\mathcal{P}(0,\vec{i},\vec{w})$ en un et un seul point entier $(k,E\left(\dfrac{kc}{c'}\right)+1)$. On a donc exactement $|c'|-1$ points entiers situés à l'intérieur de $\mathcal{P}(0,\vec{i},\vec{w})$.

   Or $\begin{pmatrix}a & b\\ a' & b'\end{pmatrix}=P\begin{pmatrix}1 & c\\ 0 & c'\end{pmatrix}$ donc $\det(\vec{u},\vec{v})=(\det P)(\det(\vec{i},\vec{w}))=c'$.

3. Ce sont les points M tels que le parallélogramme $\mathcal{P}(O,\overrightarrow{OA},\overrightarrow{OM})$ ne possède pas de points entiers dans son intérieur. Ce sont aussi les points M, situés en dehors de la droite (OA) dont la distance à la droite (OA) soit minimale. L'aire du paralléogramme $\mathcal{P}(O,\overrightarrow{OA},\overrightarrow{OM})$ étant le produit de la longueur OA par la distance de M à la droite (OA), on peut aussi dire que M est un point entier dans une des deux droites parallèles à (OA) et à distance $\dfrac{1}{OA}$ de cette droite...

Exercice 10.9. Posons $\dim E=n$ et $\dim\overrightarrow{F}=k$.

1. Soit $(A_1,\dots,A_{k+1})$ un repère affine de F ; complétons le en un repère affine $(A_1,\dots,A_{n+1})$ de E. En faisant la construction décrite dans la preuve du théorème 10.21 à partir de ce repère, on trouve $\sigma_j=\mathrm{id}_E$ pour $j\leqslant k+1$, et σ_j est produit d'au plus $j-k-1$ réflexions pour $j>k+1$. On en déduit que $f=\sigma_{n+1}^{-1}$ est produit de $n-k$ réflexions au plus.

Supposons que $f = \tau_m \circ \ldots \circ \tau_1$ où τ_j est la réflexion par rapport à un hyperplan H_j et démontrons que $m \geqslant n-k$. Alors $\vec{f} = \vec{\tau}_m \circ \ldots \circ \vec{\tau}_1$ est l'identité sur $\overrightarrow{H}_1 \cap \ldots \cap \overrightarrow{H}_m$, donc $\overrightarrow{H}_1 \cap \ldots \cap \overrightarrow{H}_m \subset \overrightarrow{F}$. Donc $\dim F = k \geqslant n-m$.

2. Une translation est la composée de deux réflexions : soit $\vec{v} \in \overrightarrow{E}$ et soit τ la réflexion par rapport à un hyperplan orthogonal à $\vec{v}$. Posons $\tau' = T_{\vec{v}} \circ \tau$. On vérifie sans peine que τ' est la réflexion hyperplane par rapport à $T_{\vec{v}/2}(H)$. Donc $T_{\vec{v}} = \tau' \circ \tau$.

   Maintenant, si f est une isométrie, il existe une isométrie g possédant des points fixes et une translation T telles que $f = T \circ g$ (on peut utiliser la décomposition canonique (10.22), ou prendre $T = T_{\overrightarrow{Af(A)}}$ pour un point $A \in E$ quelconque. Alors $g = T^{-1} \circ f$ fixe A). La dimension de l'espace des points fixes de g est égale à k, donc par la première question, g est produit de $n-k$ réflexions et f est produit de $n-k+2$ réflexions.

   Supposons que $f = \tau_m \circ \ldots \circ \tau_1$ où τ_j est la réflexion par rapport à un hyperplan H_j. Remarquons que pour tout j et tout $M \in E$, on a $\overrightarrow{M\tau_j(M)} \in \overrightarrow{H}_j^{\perp}$. Soit $M \in E$; posons $M_0 = M$, $M_1 = \tau_1(M)$, et $M_j = \tau_j(M_{j-1})$, de sorte que $M_m = f(M)$. On a donc $\overrightarrow{Mf(M)} = \sum_{j=1}^{m} \overrightarrow{M_{j-1}M_j} \in \sum_{j=1}^{m} \overrightarrow{H}_j^{\perp}$. On en déduit que $\sum_{j=1}^{m} \overrightarrow{M_{j-1}M_j} \in \sum_{j=1}^{m} \overrightarrow{H}_j^{\perp}$ contient le sous-espace engendré par les $\overrightarrow{Mf(M)}$ pour $M \in E$

   Écrivons $f = T_{\vec{v}} \circ g$ la décomposition canonique de f. On a $\{\overrightarrow{Mg(M)};\ M \in E\} = \mathrm{im}(\vec{f} - \mathrm{id}_{\vec{E}})$, donc $\{\overrightarrow{Mf(M)};\ M \in E\} = \{\vec{w}+\vec{v};\ \vec{v} \in \mathrm{im}(\vec{f}-\mathrm{id}_{\vec{E}})\}$. Le sous-espace engendré est $\mathbb{R}\vec{v} \oplus \mathrm{im}(\vec{f}-\mathrm{id}_{\vec{E}})$ qui est de dimension $n-k+1$.

   On en déduit que $m \geqslant n-k+1$. De plus g est produit de $n-k$ réflexions, donc $\det \vec{f} = \det \vec{g} = (-1)^{n-k}$; il vient $(-1)^m = (-1)^{n-k}$ donc $m-(n-k)$ est pair. Donc $m \geqslant n-k+2$.

Exercice 10.10. On a $f \circ T_{\vec{v}} = T_{\vec{f}(\vec{v})} \circ f$, donc on a l'équivalence :

(i) $\vec{f}(\vec{v}) = \vec{v}$;

(ii) $f \circ T_{\vec{v}} = T_{\vec{v}} \circ f$;

(iii) $T_{\vec{v}} \circ f(A) = T_{\vec{f}(\vec{v})} \circ f(A)$;

(iv) $f(A) + \vec{v} = f(A) + \vec{f}(\vec{v})$.

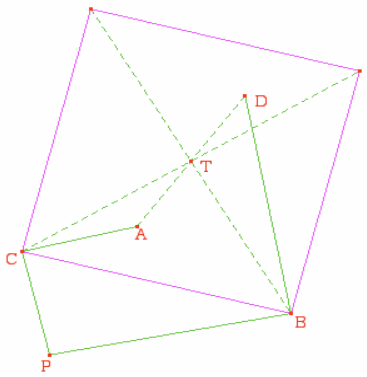
En effet, il est clair que (i)⇒(ii) ⟺ (iii)⇒(iv) ⟺ (i).

Pour $\vec{v} \in \ker(\mathrm{id}_{\vec{E}} - \vec{f})$, l'application $T_{\vec{f}(\vec{v})} \circ f$ possède un point fixe si et seulement s'il existe $\vec{z} \in \overrightarrow{E}$ el que $f(A) + \vec{v} + \vec{f}(\overrightarrow{z}) = A + \overrightarrow{z}$ soit $\overrightarrow{Af(A)} = -\vec{v} + (\mathrm{id}_{\vec{E}} - \vec{f})(z)$. Un tel $\vec{v}$ et un tel $\vec{z}$ existent si et seulement si $\overrightarrow{Af(A)} \in \ker(\mathrm{id}_{\vec{E}} - \vec{f}) + \mathrm{im}(\mathrm{id}_{\vec{E}} - \vec{f})$. Si $\vec{v}$ existe il est unique si et seulement si $\ker(\mathrm{id}_{\vec{E}} - \vec{f}) \cap \mathrm{im}(\mathrm{id}_{\vec{E}} - \vec{f}) = \{0\}$.

Exercice 10.11. Écrivons $f = T_{\vec{v}} \circ g$ la décomposition canonique de f et soit A un point fixe de g. Pour $M \in E$, on a $\overrightarrow{Mf(M)} = \overrightarrow{Mg(M)} + \vec{v} = (\vec{f} - \mathrm{id}_{\vec{E}})(\overrightarrow{AM}) + \vec{v}$. Comme $\mathrm{im}(\vec{f} - \mathrm{id}_{\vec{E}})$ et $\ker(\vec{f} - \mathrm{id}_{\vec{E}})$ sont orthogonaux, $Mf(M)$ est minimal si et seulement si $(\vec{f} - \mathrm{id}_{\vec{E}})(\overrightarrow{AM}) = 0$ c'est à dire si $\overrightarrow{AM} \in \ker(\vec{f} - \mathrm{id}_{\vec{E}})$, soit si M est un point fixe de g.

Exercice 10.12. Dans le plan affine euclidien orienté (de l'île du pendu) notons C le chêne, B la vieille barque, P le point de départ de Paul, A le premier piquet et D le second. D'après les

indications du parchemin nous pouvons écrire $A = r_1(P), D = r_2(P)$ où r_1 est la rotation de centre C, d'angle $\frac{\pi}{2}$, et r_2 est la rotation de centre B, d'angle $-\frac{\pi}{2}$. Cela implique $P = r_1^{-1}(A), D = r_2 r_1^{-1}(A) = r(A)$ où $r = r_2 r_1^{-1}$ est une rotation d'angle π en tant que composée de rotations. Par conséquent r est une symétrie centrale de centre T (milieu de tous les segments $[AD]$ possibles, donc lieu du trésor), qui ne dépend que des points C et B, et non pas du point de départ P.



Dans un certain sens Paul a eu de la chance, se retrouvant dans un problème de point fixe. Pour trouver plus rapidement le trésor le mieux pour lui c'est de commencer directement en C, car pour ce cas particulier T sera le centre du carré de côté $[CB]$, situé « à gauche » de ce segment.

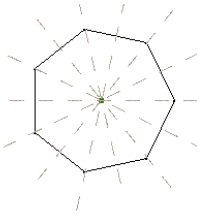
Si l'on souhaite utiliser les nombres complexes, on note a, b, c, d, p, t les affixes respectifs de A, B, C, D, P, T décrits ci-dessus. On a $a - c = i(p - c)$ et $d - b = -i(p - b)$ de sorte que $t = \dfrac{a+d}{2} = \dfrac{c(1-i) + b(1+i)}{2}$ ne dépend pas du point de départ p.

Exercice 10.13.

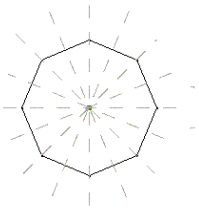
1. Notons D_n^+ le groupe des isométries directes de D_n. Remarquons que $\rho^n = \mathrm{id}_{\mathcal{E}}$, donc $\rho(P_{n-1}) = P_0$; on en déduit immédiatement que $\rho \in D_n^+$. Il en résulte que D_n^+ contient les puissances de ρ, c'est-à-dire le groupe cyclique $\{\rho^k;\ 0 \leqslant k \leqslant n-1\}$.

   Toute application affine qui envoie $\{P_0, P_1, \ldots, P_{n-1}\}$ sur lui-même fixe son centre de gravité O. Donc toute isométrie directe qui fixe $\{P_0, P_1, \ldots, P_{n-1}\}$ est une rotation de centre O. Une telle rotation ρ' est déterminée par l'image d'un point quelconque distinct de O et en particulier par $\rho'(P_0)$. Comme $\rho'(P_0) \in \{P_0, P_1, \ldots, P_{n-1}\}$, on a au plus n éléments dans D_n^+, donc $D_n^+ = \{\rho^k;\ 0 \leqslant k \leqslant n-1\}$.
2. Remarquons que $\sigma(P_0) = P_0$ et que pour $i \in \{1, \ldots, n-1\}$, on a $\sigma(P_i) = P_{n-i}$. On en déduit que $\sigma \in D_n$. Alors, $\rho^k \circ \sigma \in D_n$ pour tout $k \in \{0, ..., n-1\}$. Soit $\alpha \in D_n$. Si α est directe alors $\alpha \in D_n^+$ donc α est de la forme ρ^k ; si α est indirecte, alors $\sigma \circ \alpha \in D_n^+$, donc est de la forme ρ^k ; alors $\alpha = \sigma \circ \rho^k$ (puisque $\sigma^2 = \mathrm{id}$). Ces éléments étant deux à deux distincts D_n a $2n$ éléments.
3. - ρ^k est la rotation de centre O et d'angle $2k\pi/n$.
   - Notons α une rotation de centre O. Puisque $\alpha \circ \sigma$ est une isométrie impaire possédant un point fixe, c'est une symétrie, de sorte que $\alpha \circ \sigma = (\alpha \circ \sigma)^{-1} = \sigma \circ \alpha^{-1}$. Prenant pour α la rotation d'angle π/n, on trouve $\rho^k \circ \sigma = \alpha^k \circ \sigma \circ \alpha^{-k}$. Or la symétrie $\alpha^k \circ \sigma \circ \alpha^{-k}$ qui fixe $\alpha^k(P_0)$ est donc la symétrie orthogonale par rapport à la droite $(O\,\alpha^k(P_0))$. Deux cas sont alors possibles :

   a) Si n est impair, pour tout k, α^k est égal égal à un ρ^ℓ (avec $k = 2\ell$ si k est pair ou $k + n = 2\ell$ si k est impair), donc $\rho^k \circ \sigma$ est la symétrie par rapport à la droite (OP_ℓ).



   b) Si $n = 2m$ est pair, on distinguera selon que $k = 2\ell$ (*i.e.* k est pair) auquel cas $\rho^k \circ \sigma$ est la symétrie par rapport à la droite (OP_ℓ) ; si $k = 2\ell + 1$ est impair, alors $\rho^k \circ \sigma$ est la symétrie par rapport à la droite passant par O et le milieu du coté $[P_\ell, P_{\ell+1}]$ (et aussi par le milieu du coté $[P_{\ell+m}, P_{\ell+m+1}]$).



Exercice 10.14. On numérote les faces du cube de 1 à 6 de façon à ce que la face opposée à la face i soit la face $7 - i$ (comme un dé).

1. Le groupe du cube est contenu dans $SO(3)$; ses éléments, en dehors de l'identité, sont des rotations. Dans le groupe du cube, il y a :

a) L'identité.

b) Les rotations d'angles $k\pi/2$ d'axe reliant les centres de deux faces opposées avec k impair. Ils opèrent par permutation circulaire sur les diagonales ; on trouve ainsi $3 \times 2 = 6$ éléments (3 = nombre de paires de faces opposées $\times$ deux rotations d'angles $\pm\pi/2$). Un tel élément fixe deux faces opposées (par exemple 1 et 6) et est une permutation cyclique sur les quatre autres faces (par exemple un cycle $(2, 3, 5, 4)$).

c) Les demi-tours d'axe reliant les centres de deux faces opposées. Il y en a 3. La décomposition en cycles de leur action sur les diagonales est de la forme $(a, b)(c, d)$. Leur action sur les faces fixe deux faces opposées (par exemple 1 et 6) et envoie les autres dans leur opposé. L'action sur les faces est du type $(2, 5)(3, 4)$.

d) Les demi tours dont l'axe relie les centres de deux arêtes diagonalement opposées. Leur action échange les deux diagonales extrémités de ces arêtes et fixe les deux autres diagonales. Comme il y a 12 arêtes dans un cube, il y a 6 tels éléments. L'ation sur les faces, par exemple si on prend l'axe reliant le milieu de l'arête séparant les faces 2 et 3 au milieu milieu de l'arête séparant les faces 5 et 4, échange se décompose en cycles $(1, 6)(2, 3)(4, 5)$.

e) Les rotations d'angle $2k\pi/3$ d'axe une diagonale. Leur action fixe cette diagonale et permute circulairement les autres. Il y $4 \times 2 = 8$ tels éléments. (4 = nombre de diagonales $\times$ deux rotations d'angles $\pm 2\pi/3$). Si on prend la diagonale du somme commun aux faces $1, 2, 3$, son action sur les faces est comme $(1, 2, 3)(6, 5, 4)$.

On a bien trouvé les 24 éléments.

2. Le groupe du cube opère sur les trois paires de faces opposées ou, autrement dit, sur les trois droites reliant les centres de deux faces opposées. On obtient ainsi un morphisme à valeurs dans $\mathfrak{S}_3$. Le noyau est formé d'éléments fixant ces trois droites. Comme il s'agit de rotations, outre l'identité, il y aura les trois demi-tours autour de ces axes.

Exercice 10.15.

1. Un coloriage c est fixé par g si et seulement si pour tout $z \in Y$ on a $c(g^{-1}.z) = c(z)$. Si c est un coloriage invariant par g, on aura $c(g.y) = c(y)$ pour tout $y \in Y$ (appliquant l'égalité ci dessus à $z = gy$), puis par récurrence sur n, $c(g^n y) = c(y) = c(g^{-n} y)$. En d'autres termes, c doit être constant sur les orbites de g. Inversement, il clair que tout coloriage constant sur les orbites de g est invariant par g.

   Pour choisir un coloriage invariant par g, on doit donc choisir une couleur par orbite : il y a donc $d^{k(g)}$ choix.

2. Comptons à l'aide de l'exercice 10.14, pour chaque élément $g \in G$, le nombre d'orbites dans son action sur les faces du cube.

   a) L'identité a 6 orbites.

   b) Les 6 rotations d'angles $k\pi/2$ dont l'axe relie les centres de deux faces opposées avec k impair donnent des 4 cycles du type $(2, 3, 5, 4)$. Un tel cycle a 3 orbites $\{1\}$, $\{6\}$ et $\{2, 3, 4, 5\}$.

   c) Les 3 demi-tours d'axe reliant les centres de deux faces opposées ont une décomposition en cycles du type $(2, 5)(3, 4)$: ils ont donc 4 orbites (dans cet exemple $\{1\}$, $\{6\}$, $\{2, 5\}$ et $\{3, 4\}$).

   d) Les 6 demi-tours d'axe reliant les centres de deux arêtes diagonalement opposées se décomposent en cycles du type $(1, 6)(2, 3)(4, 5)$ et ont donc 3 orbites.

   e) Les 8 rotations d'angle $2k\pi/3$ d'axe une diagonale donnent une décomposition en cycles comme $(1, 2, 3)(6, 5, 4)$: il y a alors deux orbites.

   Par la formule de Burnside on obtient que le nombre de coloriages du cube est donc

$$\frac{1}{24}\Big(d^6 + 6d^3 + 3d^4 + 6d^3 + 8d^2\Big) = \frac{d^6 + 3d^4 + 12d^3 + 8d^2}{24}.$$

3. Comptons à l'aide de l'exercice 10.13 le nombre d'orbites des éléments $g \in D_n$ du groupe diédras dans son action sur les sommets du polygone.

   a) Soit $m \in \{0, \dots, n-1\}$. Notons k le pgcd de n et m. Alors $g = \rho^m$ est d'ordre n/k. Le sous-groupe qu'il engendre est un groupe de rotations qui agit librement dans le polygone : il a k orbites. Notons que m s'écrit $k\ell$ avec ℓ premier avec n/k : il y a donc $\varphi(n/k)$ tels m (où φ est l'indicatrice d'Euler).

   b) Si $n = 2m$, la moitié des symétries ont deux points fixes (celles dont l'axe passe par les sommets du polygone) donc $m+1$ orbites (2 orbites à un point et $m-1$ orbites à 2 points) ; l'autre moitié n'ont pas de points fixes et ont donc m orbites (à 2 points).

   c) Dans le cas où $n = 2m+1$, toutes les symétries ont un point fixe, et ont donc $m+1$ orbites (m orbites à 2 points et 1 à un point).

   Par la formule de Burnside on obtient que le nombre de coloriages du polygone est

$$\begin{aligned} &\frac{1}{2n}\Big(\Big(\sum_{k|n} \varphi(n/k) d^k\Big) + m(d^m + d^{m+1})\Big) && \text{si } n = 2m \\ &\frac{1}{2n}\Big(\Big(\sum_{k|n} \varphi(n/k) d^k\Big) + n d^{m+1}\Big) && \text{si } n = 2m+1. \end{aligned}$$

Index