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.

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 1.4.

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 1.5. [un peu rapide]

1. On commence par une remarque : si $p_1, \dots, p_k$ 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
   - $a = a_1 a_2$, $b = b_1 b_2$;
   - $a_1 | b_1$ 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 $d' = a_1 b_2$ 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 $a_2 b_1 = m$.
4. D'après le théorème chinois, on a des isomorphismes

$$\begin{aligned} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} &\simeq (\mathbb{Z}/a_1 \times \mathbb{Z}/a_2\mathbb{Z}) \times (\mathbb{Z}/b_1\mathbb{Z} \times \mathbb{Z}/b_2\mathbb{Z}) \\ &\simeq (\mathbb{Z}/a_1 \times \mathbb{Z}/b_2\mathbb{Z}) \times (\mathbb{Z}/b_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z}) \\ &\simeq \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}. \end{aligned}$$

Exercice 1.6.

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 $F_{p+q} = F_p F_{q-1} + F_{p+1} F_q$. 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 $\varphi(x+y) = \varphi(x) + \varphi(y)$.

(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 1.7.

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 $a_{k+1} = c_k$, $b_{k+1} = d_k$,

3. Cette formule évidente est la formule de la comatrice en dimension 2. C'est aussi le théorème de Cayley-Hamilton en dimension 2.

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

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{k+1} = \begin{pmatrix} F_{k-1} & F_k \\ F_k & F_{k+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} F_k & F_{k-1}+F_k \\ F_{k+1} & F_k + F_{k+1} \end{pmatrix} = \begin{pmatrix} F_k & F_{k+1} \\ F_{k+1} & F_{k+2} \end{pmatrix}.$$

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 1.8.

4. Plus généralement, pour une matrice 2×2 inversible on a $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} = \dfrac{1}{ad-bc} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$.

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 1.7.

   c) (*cf.* exerc. 1.7) 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 1.7, 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 $\begin{pmatrix} 0 & 1 \\ 1 & q_m \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_{m-1} \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} = \begin{pmatrix} \alpha & \ell \\ \ell & p \end{pmatrix}$, et par unicité, on trouve $q_j = q_{m+1-j}$.

   Posons alors $m = 2k$ et $\begin{pmatrix} 0 & 1 \\ 1 & q_{k+1} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_{k+2} \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_m \end{pmatrix} = \begin{pmatrix} u & a \\ v & b \end{pmatrix} = A$. On a $\begin{pmatrix} \alpha & \ell \\ \ell & p \end{pmatrix} = {}^tAA$, donc $p = a^2 + b^2$.

   Remarquons de plus que l'on a $\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \ell \\ p \end{pmatrix}$. Comme la matrice $\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix}$ est inversible, $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix}$ d'après l'exercice 1.7. 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 1.9.

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 $n = 2^k m$ 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 $4\times128+1 = 513$ et 5 divise $3\times128+1 = 385$. Enfin, $2\times128+1 = 257 = F_3$ est un nombre de Fermat donc premier à F_5. Le premier nombre à tester est donc $5\times128+1$.

e) On a $2^4 \equiv -5^4 \ [641]$, donc $F_5 = 2^{28}2^4 + 1 \equiv 1 - 5^4 2^{28} \ [641]$.

f) On a $52^7 = 640 \equiv -1 \ [641]$, donc $5^4 2^{28} = (52^7)^4 \equiv 1 \ [641]$ et 641 divise F_5.

Exercice 1.10.

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 $X^n - 1 = Q^2 P$ 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 1.11.

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 $c \in \left\{1, \ldots, \frac{p-1}{2}\right\}$. L'application qui à $c \in \left\{1, \ldots, \frac{p-1}{2}\right\}$ associe la classe dans $\mathbb{F}_p$ de c^2 est donc une bijection de $\left\{1, \ldots, \frac{p-1}{2}\right\}$ 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) $\iff$ (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 1.12.

1. a) On a $1^p = 1$, $(ab)^p = a^p b^p$ et, puisque $p \mid \binom{p}{k}$ 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 1.13.

Voir exercice 1.11.

Remarquons que $\dfrac{p+1}{4} \in \mathbb{N}$. Puisque $x^{\frac{p-1}{2}} = 1$, on a $\left(x^{\frac{p+1}{4}}\right)^2 = x^{\frac{p-1}{2}+1} = x$.

1. 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 $0 \leqslant k \leqslant \ell$.
2. 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 $b = \pm 1$.
3. 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 le$b_1 = -1$, alors b est une racine de -1 ; sinon, on continue : on pose $b_2 = b_1^2$. Au bout d'u plus $n-1$ 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 1.14.

1. Prendre pour $a-2$ un nombre strictement positif qui est multiple de tous les nombres premiers $\leqslant n+1$. Alors, pour $0 \leqslant j \leqslant n-1$, $2+j$ a un diviseur premier qui divise aussi $a-2$, donc $a+j$ n'est pas premier.

   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 $b^2 p_1^{\varepsilon_1} \dots p_k^{\varepsilon_k} \leqslant x$.

   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) our $x = 4^{k+1}$, 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.

   d) 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 1.15.

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 $v_p\binom{2n}{n} \leqslant E\big(\frac{\ln 2n}{\ln p}\big)$.
   • Si $n < p \leqslant 2n$, alors $v_p(n!) = 0$ et $v_p((2n)!) = 1$.
   • Si $p \leqslant n < \frac{3p}{2}$, 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 $\ln\binom{2n}{n} \geqslant \sum_{n<p<2n,\ p \text{ premier}} v_p\binom{2n}{n} \ln p \geqslant (\pi(2n) - \pi(n)) \ln n$.

   (ii) On a d'après (c),

$$\begin{aligned} \ln\binom{2n}{n} &= \sum_{p\leqslant 2n/3,\ p \text{ premier}} v_p\binom{2n}{n} \ln p + \sum_{n<p<2n,\ p \text{ premier}} \ln p \\ &\leqslant \pi(2n/3) \ln 2n + (\pi(2n) - \pi(n)) \ln 2n \end{aligned}$$

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 $\binom{2n-1}{k+1} = \frac{2n-1-k}{k+1}\binom{2n-1}{k} \geqslant \binom{2n-1}{k}$; 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 $\binom{2n}{n} \leqslant 2^{2n-1} \leqslant n\binom{2n}{n}$

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 suppose désormais que p est impair.

Un carré est congru à 0 ou 1 modulo 4, donc (i)⇒(iv).

Il résulte de l'exercice 1.11 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 $\dfrac{x \pm i}{p} \notin Z[i]$, 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 $\dfrac{n}{p_j}$ 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 $\dfrac{n}{p_j}$, 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 $a \in \{0, \ldots, d-1\}$ 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 $\sum_{d|n} s_d = n = \sum_{d|n} \varphi(d)$. 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 $(1+p)^{p^{k+1}} = (1+p^{k+1}(1+pb))^p = \sum_{j=0}^{p} \binom{p}{j} p^{j(k+1)}(1+pb)^j$. 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.

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 $k \leqslant n - 1$.

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 $v(x) = (\operatorname{Re} x)^2 + (\operatorname{Im} x)^2 \leqslant \sqrt{3}$. 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 $|\beta - \alpha| \leqslant |\beta|$, on a $|u-1| \leqslant |u|$, donc $\operatorname{Re} u \leqslant 1/2$; de même $|\beta + \alpha| \leqslant |\beta|$ 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 $x = m\alpha + n\beta$.

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 $\begin{pmatrix}a + bx\\ c + dx\end{pmatrix} = \tau\begin{pmatrix}1\\ x\end{pmatrix}$. 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 $\dfrac{a-d}{b}$.

c) Ces inégalités proviennent des inégalités $|x|\geqslant 1$ et $|\mathrm{Re}\, x|\leqslant 1$.

5. On a $-4bc\geqslant 4b^2$ et $(a-d)^2\leqslant b^2$, donc $19=-4bc-(a-d)^2\geqslant 4b^2-b^2=3b^2$.
6. Puisque b est impair et $3b^2\leqslant 19$, il vient $b=1$.
7. 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 K 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 $(a_ib_j)_{1\leqslant i\leqslant p;\ 1\leqslant j\leqslant q}$ 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 $x=\displaystyle\sum_{j=1}^{n}\mu_jb_j$ et, pour chaque j, il existe $(\lambda_{1,j},\dots,\lambda_{p,j})\in K^p$ tels que $\mu_j=\displaystyle\sum_{i=1}^{p}\lambda_{i,j}a_i$. on a alors $x=\displaystyle\sum_{j=1}^{q}\sum_{i=1}^{p}\lambda_{i,j}a_ib_j$ donc le système $(a_ib_j)_{1\leqslant i\leqslant p;\ 1\leqslant j\leqslant q}$ est générateur.

Soient $(\lambda_{i,j}) \in K^{pq}$ tels que $\sum_{j=1}^{q}\sum_{i=1}^{p}\lambda_{i,j}a_ib_j = 0$; 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 $(a_ib_j)_{1\leqslant i\leqslant p;\ 1\leqslant j\leqslant q}$ 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 $P = \sum_{k=0}^{n} a_kX^k$. On démontre immédiatement par récurrence sur $n \in \mathbb{N}$ qu'il existe un sous corps K_1 de L contenant $a_0, \ldots, a_n$ 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 $0 = q^nP(p/q) = \sum_{k=0}^{n} a_kp^kq^{n-k}$. Comme p et q divisent cette somme, il vient $p|q^na_0$ et $q|p^na_n$, 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 $F = \dfrac{2}{X^3} + \dfrac{4}{X^2} + \dfrac{7}{X} - \dfrac{7}{X-1} + \dfrac{3}{(X-1)^2}$. Donc une primitive de $t \mapsto F(t)$ est $t \mapsto -\dfrac{1}{t^2} - \dfrac{4}{t} - \dfrac{3}{t-1} + 7\ln\left|\dfrac{t}{t-1}\right| + c$ 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 $x \mapsto \dfrac{1}{6\sqrt{2}}\ln\left|\dfrac{x-\sqrt{2}}{x+\sqrt{2}}\right| + \dfrac{1}{3}\mathrm{Arctan}\, x + c$.

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 $\displaystyle\prod_{k=0}^{d-1}(X - e^{\frac{2ik\pi}{d}}) = X^d - 1$.
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 $\lambda_1, \dots, \lambda_k$ 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 $\dfrac{(AB)'}{AB} = \dfrac{A'}{A} + \dfrac{B'}{B}$. Décomposons P en facteurs irréductibles : $P = a\prod_{i=1}^{k} P_i^{m_i}$. On a $\dfrac{P'}{P} = \sum_{i=1}^{k} \dfrac{m_i P_i'}{P_i}$.
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 $\sum_{i=1}^{k} \dfrac{m_i(z-\lambda_i)}{|z-\lambda_i|^2} = 0$, donc z est barycentre des λ_i affectés des coefficients strictement positifs $\dfrac{m_i}{|z-\lambda_i|^2}$.
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 $c = \dfrac{\alpha+\beta+\gamma}{3}$. 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 $\left(\frac{x}{|a| + |b|}\right)^2 + \left(\frac{y}{|a| - |b|}\right)^2 = \frac{1}{4}$; ses foyers ont donc comme coordonnées $y = 0$ et $x = \pm\frac{\sqrt{(|a| + |b|)^2 - (|a| - |b|)^2}}{2} = \pm\sqrt{|ab|}$.

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 $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ (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 $(x, \frac{pq}{x})$, 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, $y_A + y_B + y_C - q = \frac{pq}{x_A} + \frac{pq}{x_B} + \frac{pq}{x_C} - \frac{pq}{p} = \frac{pq\sigma_3}{\sigma_4} = 2q$.] 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 $Q_1 = \prod\limits_{j=1}^{n-1} X - x_j$.

   Si on écrit $Q_1 = \sum\limits_{j=0}^{n} b_j X_j$ (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) Démontrons cette propriété par récurrence sur r. C'est vrai 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 en déduit 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 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 $\mathrm{Res}(a_0 + a_1 X, X - b) = \begin{vmatrix} a_0 & -b \\ a_1 & 1 \end{vmatrix} = a_0 + a_1 b$.

Écrivons $A = \sum_{k=0}^{n} a_k X^k = a_0 + XA_1$, où $A_1 = \sum_{k=1}^{n} a_k X^{k-1}$.

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 $A = A(b) + \sum_{k=0}^{m-1} \alpha_k X^k (X-b)$. 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 $E_m \times E_{n_1} \times E_{n_2}$:

$$\hat{\mathcal{B}} = ((1,0), (X,0), \dots, (X^{n_1-1}, 0), (0,1), (0,X), \dots, (0, X^{m+n_2-1}))$$

$$\tilde{\mathcal{B}} = ((1,0,0), (X,0,0), \dots, (X^{m-1}, 0, 0), (0,1,0), \dots, (0, X^{n_1-1}, 0), (0,0,1), \dots, (0,0,X^{n_2-1}))$$

   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. Soit $P \in \mathbb{Z}[X]$ non scalaire. Si P est irréductible sur $\mathbb{Z}$, on a $c(P) = 1$ (puisque P est divisible par $c(P)$). Supposons donc que $c(P) = 1$ et que P n'est pas irréductible sur $\mathbb{Q}$ et donnons-nous une décomposition $P = AB$ avec $A, B \in \mathbb{Q}[X]$ non scalaires. 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 $bB = c(bB)B_1$. On a alors $c(aA)c(bB) = c(abAB) = c(abP) = ab$, donc $abA_1B_1 = c(aA)c(bB)A_1B_1 = aAbB = abP$, ce qui donne $P = A_1B_1$, donc P n'est pas irréductible sur $\mathbb{Z}$.

Exercice 3.17. Supposons que $P = AB$ avec $A, B \in \mathbb{Z}[X]$. Comme P est unitaire, on peut supposer (quitte à les remplacer par leur opposé) que A et B sont unitaires. Notons n, a, b les degrés respectifs de P, A et B. Notons $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ la réduction modulo p. C'est un morphisme d'anneaux. On a $p(P) = X^n = \pi(A)\pi(B)$. Or le seul polynôme unitaire de degré a divisant X^n est X^a, donc $\pi(A) = X^a$ et de même $\pi(B) = X^b$. En d'autres termes tous les coefficients sauf le coefficient dominant de A et B sont divisibles par p. Si A et B était non constants, p divise $A(0)$ et $B(0)$, donc p^2 divise $P(0)$, ce qui est contraire à l'hypothèse.

NB Cette démonstration marche aussi si au lieu de supposer que P est unitaire, on suppose juste que le contenu de P est 1 (*cf.* exerc. 3.16).

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) $\dfrac{c-a}{c-b}$ n'est pas un carré.

L'application $c \mapsto \dfrac{c-a}{c-b}$ 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), $\dfrac{p}{1-pt} = \sum_{n=1}^{+\infty} \dfrac{nN_n t^{n-1}}{1-t^n}$.
   Multipliant par t, on trouve $\sum_{k=1}^{+\infty} p^k t^k = \sum_{n=1}^{+\infty}\sum_{k=1}^{+\infty} nN_n t^{kn}$. Donc, prenant le terme d'ordre ℓ dans cette série entière $p^\ell t^\ell = \sum_{n|\ell} nN_n$.

   c) résulte immédiatement de 1.b) et 2.b).

   d) On a donc $nN = p^n + \sum_{d|n;d\neq n} \mu(\frac{n}{d}) p^d \geqslant p^n - \sum_{d|n;\ d\neq n} p^d \geqslant p^n - \sum_{1\leqslant d\leqslant n/2} p^d \geqslant p^n - (n/2)p^{n/2}$.
   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. 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 4.2. 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 4.3.

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 $j \in \{1, \ldots, n\}$ on ait $y + \lambda x \in F_j$, *i.e.* $y + \lambda x \notin \bigcup_{j=1}^{n} F_j$.

Exercice 4.4. 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 4.5.

- 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 4.6.

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 $\dim E = \dim F + \dim G = \dim F + \operatorname{codim} F$.
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 $\operatorname{codim} F_1 = \dim G_1 \leqslant \dim G = \operatorname{codim} F$.
4. Si $\ker f$ admet un supplémentaire F de dimension finie, alors la restriction de f est un isomorphisme de F sur $\operatorname{im} f$ (prop. 4.18), donc $\operatorname{rg} f = \operatorname{codim} F$.
   Supposons inversement que $\operatorname{rg} f$ est fini et soit $(e_1, \dots, e_k)$ une base de $\operatorname{im} f$. 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 $\operatorname{Vect}\{x_1, \dots, x_k\}$ 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 $z = g(y_1) + g(y_3) \in g(F_1) + g(\operatorname{im} f)$.

11.6 Matrices et bases

Exercice 6.1. La matrice $B = \begin{pmatrix} I_r & 0 \\ -A_3 A_1^{-1} & I_{n-r} \end{pmatrix}$ est inversible. Donc $BA = \begin{pmatrix} A_1 & A_2 \\ 0 & A_4 - A_3 A_1^{-1} A_2 \end{pmatrix}$ 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 $\mathrm{rg}\{f_1, \ldots, f_n\} = \dim E - \dim\{f_1, \ldots, f_n\}^o = \dim E - \dim \ker \varphi = \mathrm{rg}\varphi$. La famille $(f_1, \ldots, f_n)$ 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 $\iff \operatorname{rg} f = \dim F \iff {}^t f$ est injective ;
- f est injective $\iff \operatorname{rg} f = \dim E \iff {}^t f$ est surjective.

2. Par définition $\ker {}^t f = \{\ell \in F^*;\ \ell \circ f = 0\} = \{\ell \in F^*;\ \operatorname{im} f \subset \ker \ell\} = (\operatorname{im} f)^\perp$.
Si $g \in \operatorname{im} {}^t f$, 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 : $\operatorname{rg}{}^t f = \operatorname{rg} f = \dim E - \dim \ker f = \dim(\ker f)^\perp$.

Exercice 6.6.

1. La bilinéarité est claire et la symétrie est la propriété de trace $\operatorname{Tr}(AB) = \operatorname{Tr}(BA)$. Notons $(E_{i,j})$ la base canonique de $\mathcal{M}_n(K)$. Pour $A = (a_{i,j})$, on a $\operatorname{Tr}(AE_{i,j}) = a_{j,i}$. Si $\operatorname{Tr}(AB) = 0$ 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 $A \mapsto \operatorname{Tr}(A.)$ est bijective, donc il existe $A \in \mathcal{M}_n(K)$ tel que $F = \{B \in \mathcal{M}_n(K);\ \operatorname{Tr}(AB) = 0\}$.
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 $\operatorname{Tr}(PAQJ) = 0$. Or $\operatorname{Tr}(PAQJ) = \operatorname{Tr}(AQJP)$. 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 $\operatorname{Tr}({}^t MM) = \sum_{i,j} m_{i,j}^2 \geqslant 0$. 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 $b(S, A) = \operatorname{Tr}(SA) = \operatorname{Tr}({}^t(SA)) = \operatorname{Tr}({}^t A {}^t S) = \operatorname{Tr}(-AS) = -\operatorname{Tr}(SA)$. 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 $\operatorname{Vect}\{f_1, f_2, f_3, f_4\} = (\{f_1, f_2, f_3, f_4\}^o)^\perp = E^*$. 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 $P_2 = \dfrac{(X-a)(X-b)^2}{(a-b)^2}\cdot$ 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 $(X-b)^2 S$ 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 $P : t \mapsto \det(M + iN)$ 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 $\mathrm{rg}A = s < r$, 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

$$\Delta_n(a_1, \ldots, a_n) = \begin{vmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} \\ 1 & a_3 & a_3^2 & \ldots & a_3^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{vmatrix} = \prod_{1 \leqslant i < j \leqslant n} (a_j - a_i).$$

C'est clair pour $n = 2$.

Supposons le résultat vrai pour $n-1$. Commençons par remarquer que si $C_1, \ldots, C_n$ sont des vecteurs-colonne et si on pose $C'_1 = C_1$ et $C'_{i+1} = C_{i+1} - a_1 C_i$ (pour $i = 1, \ldots, n-1$), la matrice A de colonnes $C_1, \ldots, C_n$ et A' de colonnes $C'_1, \ldots, C'_n$ 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 $\begin{pmatrix} 1 & -a_1 & 0 & \ldots & 0 \\ 0 & 1 & -a_1 & \ldots & 0 \\ 0 & 0 & 1 & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$. Donc

$$\Delta_n(a_1, \ldots, a_n) = \begin{vmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & a_2 - a_1 & a_2^2 - a_1 a_2 & \ldots & a_2^{n-1} - a_1 a_2^{n-2} \\ 1 & a_3 - a_1 & a_3^2 - a_1 a_3 & \ldots & a_3^{n-1} - a_1 a_3^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n - a_1 & a_n^2 - a_1 a_n & \ldots & a_n^{n-1} - a_1 a_n^{n-2} \end{vmatrix}.$$

Développant par rapport à la première ligne puis mettant $a_i - a_1$ en facteur dans la $(i-1)$-ème ligne, il vient

$$\begin{aligned} \Delta_n(a_1, \ldots, a_n) &= \begin{vmatrix} a_2 - a_1 & a_2^2 - a_1 a_2 & \ldots & a_2^{n-1} - a_1 a_2^{n-2} \\ a_3 - a_1 & a_3^2 - a_1 a_3 & \ldots & a_3^{n-1} - a_1 a_3^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ a_n - a_1 & a_n^2 - a_1 a_n & \ldots & a_n^{n-1} - a_1 a_n^{n-2} \end{vmatrix} \\ &= \prod_{j=2}^{n} (a_j - a_1) \begin{vmatrix} 1 & a_2 & \ldots & a_2^{n-2} \\ 1 & a_3 & \ldots & a_3^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & a_n & \ldots & a_n^{n-2} \end{vmatrix} \\ &= \prod_{j=2}^{n} (a_j - a_1) \Delta_{n-1}(a_2, \ldots, a_n) \end{aligned}$$

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 $(e_1, \ldots, e_n)$ 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 $j(k) = \inf\{j;\ \mathrm{rg}(C'_1, \ldots, C'_j) = k\}$, 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 $A = T_1(\lambda_1) \ldots T_N(\lambda_N)$ comme un produit de transvections. Alors $A_t = T_1(t\lambda_1) \ldots T_N(t\lambda_N)$ 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.

1. est clair.
2. • Il est clair que Φ est linéaire
   • Démontrons que Φ est injective : supposons que $\Phi(D) = 0$. Soit $s : \{1, \ldots, p\} \to \{1, \ldots, n\}$ 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 $D = \operatorname{diag}(\omega^{i-1})$.

Remarquons que le 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 $P^{-1} = \frac{1}{n}P^*$.

Enfin $A = \sum_{k=0}^{n-1} a_k J^k = P \sum_{k=0}^{n-1} a_k D^k P^{-1} = P \operatorname{diag}\Big(\sum_{k=0}^{n-1} a_k \omega^{(i-1)k}\Big) P^{-1}$.

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 $u(e_k)=\lambda_k e_k+\sum_{j<k}a_{j,k}e_j$, 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 $(u-\lambda_1\mathrm{id}_E)\circ\dots\circ(u-\lambda_k\mathrm{id}_E)$ est nul sur E_k. En particulier, pour $k=n$, l'endomorphisme $\chi_u(u)=(u-\lambda_1\mathrm{id}_E)\circ\dots\circ(u-\lambda_n\mathrm{id}_E)$ 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 convergent 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 $P(T+\alpha_kD)P^{-1}$ 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

6. On peut prendre $0<\alpha<(n-1)^{-1}\min\{|\lambda_i-\lambda_j|;\ (i,j)\in\{1,\dots,n\}^2,\ \lambda_i\neq\lambda_j\}$.

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 posons $u + \varepsilon v$ 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 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 ui 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 $u(\text{im } u) \subset u(E) = \text{im } u$, donc 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 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 im $u \subset E$ et im $u \neq E$, la dimension de im u est $< n$ et la restriction de u à im u est nilpotente. D'après l'hypothèse de récurrence, il existe une base $(e_1, \dots, e_k)$ de 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 im $u = \text{Vect}(e_1, \dots, e_k)$, 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 $F = \text{Vect}(x_0, \dots, x_{k-1})$. On a $u(F) = \text{Vect}(x_1, \dots, x_k)$ 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 $x_k \in \text{Vect}(x_0, \dots, x_{k-1})$. D'après la question 1, on a $x_\ell \in \text{Vect}(x_0, \dots, x_{k-1})$ pour tout $\ell \in \mathbb{N}$, donc $\text{Vect}(x_0, \dots, x_{k-1}) = E$ 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. 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_j, $Q_j(u) \neq 0$ 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 $P_j^{\alpha}(u)(x_j) = P_j^{\alpha_j}(u) \circ R_j(u)(x) = \varpi_u(u)(x) = 0$ 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 8.10.

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. 8.9, 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 4.3, 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 8.11. 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 8.12. 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 8.13. 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 8.14.

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 8.13.

Exercice 8.15. 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 8.13, on en déduit que P et ϖ_u ne sont pas premiers entre eux, et puisque P est irréductible, il divise ϖ_u.

Exercice 8.16.

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 9.31.*

Exercice 8.17. 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 8.18.

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.
   Par ailleurs, si $q' \in T_p$, il existe des bases $B = (e_1, \dots, e_p, e_{p+1}, \dots, e_n)$ et $B' = (e'_1, \dots, e'_p, e'_{p+1}, \dots, e'_n)$ 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 (dans une autre base, on a $A'_k = {}^tPA_kP$ où P est une matrice de passage donc $\det A'_k = (\det P)^2 \det A_k$).
      On peut donc choisir la base $(e_1, \dots, e_k)$ de la question précédente. 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).

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 $\lambda_1,\dots,\lambda_p$ 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'Iwazawa, analyse p. **??**

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 $a=d$ 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 9.31, 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 M' est normale, donc $B = 0$ 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. Notons que
     $$\begin{pmatrix} U_1^{-1} & 0 \\ 0 & U_2^{-1} \end{pmatrix} U^{-1}MU \begin{pmatrix} I_d & 0 \\ 0 & U_1 \end{pmatrix} = \begin{pmatrix} A & 0 \\ 0 & U_1^{-1}CU_1 \end{pmatrix}$$
     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 modules 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 $\big((A, \sin 2\hat{A}), (B, \sin 2\hat{B}) + (C, \sin 2\hat{C})\big)$ centre O du cercle circonscrit du triangle ABC.
3. a) Dans le triangle $AA'B$, rectangle en A', on a $A'B = |\cotan \hat{B}| AA'$. De même $A'C = |\cotan \hat{C}| AA'$. 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. 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 $\overrightarrow{Mf(M)}=\displaystyle\sum_{j=1}^{m}\overrightarrow{M_{j-1}M_j}\in\sum_{j=1}^{m}\overrightarrow{H}_j^{\perp}$. On en déduit que $\displaystyle\sum_{j=1}^{m}\overrightarrow{M_{j-1}M_j}\in\sum_{j=1}^{m}\overrightarrow{H}_j^{\perp}$ 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 10.9. 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 10.10. Écrivons $f = T_{\vec{v}} \circ g$ la décomposition canonique de f et soit A un point fixe de g. Pour $M \in M$, 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 10.11.

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 $k\pi/2$ dont l'axe relie 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 $\pm\pi/2$).
   c) Les demi tours dont l'axe relie 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 $(a, b)(c, d)$.
   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.
   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 $\pm 2\pi/3$).

   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.