

*Solutions Exercices MP/MP**

Table des matières

1 Algèbre Générale	2
2 Séries numériques et familles sommables	38
3 Probabilités sur un univers dénombrable	38
4 Calcul matriciel	38
5 Réduction des endomorphismes	39
6 Espaces vectoriels normés	42
7 Fonction d'une variable réelle	82
8 Suites et séries de fonctions	93
9 Séries entières	93
10 Intégration	93
11 Espaces préhilbertiens	93
12 Espaces euclidiens	93
13 Calcul différentiel	93
14 Équation différentielles linéaires	93

1 Algèbre Générale

Solution 1.1. Soit $(x, y) \in G^2$. On a d'abord

$$\begin{aligned}x \cdot y &= (x \cdot y)^{p+1} (x \cdot y)^{-p} \\&= x^{p+1} \cdot y^{p+1} \cdot y^{-p} \cdot x^{-p} \\&= x^{p+1} \cdot y \cdot x^{-p}\end{aligned}\tag{1.1}$$

On cherche maintenant à montrer que x^{p+1} et y commutent. On a

$$\begin{aligned}y^{p+2} \cdot x^{p+2} &= (y \cdot x)^{p+2} \\&= (y \cdot x)^{p+1} \cdot y \cdot x \\&= y^{p+1} \cdot x^{p+1} \cdot y \cdot x\end{aligned}$$

Donc on a $y \cdot x^{p+1} = x^{p+1} \cdot y$. En reportant dans (1.1), on a $x \cdot y = y \cdot x$ et donc G est abélien.

Remarque 1.1.

- Pour (Σ_3, \cdot) , on a f_0, f_1 et f_6 des morphismes mais Σ_3 n'est pas commutatif.
- Si f_2 est un morphisme, alors on a $(x \cdot y)^2 = x \cdot y \cdot x \cdot y = x^2 \cdot y^2$ d'où $y \cdot x = x \cdot y$.

Solution 1.2. A est non vide car $\omega(e_G) = 1$ et $e_G \in A$. Soit $x \in A$ tel que $\omega(x) = 2p + 1$. Soit $k \in \mathbb{Z}$, on a

$$\begin{aligned}x^{2k} = e_G &\Leftrightarrow 2p + 1 \mid 2k \\&\Leftrightarrow 2p + 1 \mid k\end{aligned}$$

d'après le théorème de Gauss.

Ainsi, $\omega(x^2) = 2p + 1$ et $x^2 \in A$, donc

$$\begin{aligned}\varphi : A &\rightarrow A \\x &\mapsto x^2\end{aligned}$$

est bien définie. Soit $x \in A$, il existe $p \in \mathbb{N}$ tel que $x^{2p+1} = e_G$ donc $x^{2p+2} = x$ d'où $(x^{p+1})^2 = x$. Il suffit donc de vérifier que x^{p+1} pour montrer que l'application est surjective. Comme A est fini, elle sera bijective.

On a $gr\{x^{p+1}\} \subset gr\{x\}$ et $(x^{p+1})^2 = x$ donc $gr\{x\} = gr\{x^{p+1}\}$ donc $\omega(x) = \omega(x^{p+1}) = 2p+1$ et donc $x^{p+1} \in A$.

Solution 1.3. On note $m = \theta(\sigma)$. On suppose que σ se décompose en produit de cycle de longueur l_1, \dots, l_m avec $l_1 + \dots + l_m = n$. Comme

$$(a_1, \dots, a_l) = [a_1, a_2] \circ [a_2, a_3] \circ \dots \circ [a_{l-1}, a_l]$$

Donc σ se décompose en $\sum_{i=1}^m (l_i - 1) = n - m$ transpositions. Montrons par récurrence sur k , $\mathcal{H}(k)$:
 "Un produit de k transpositions possède au moins $n - k$ orbites".

Pour $k = 0$, $\sigma = id$ possède n orbites.

Pour $k = 1$, soit τ une transposition, on a $\theta(\tau) = n - 2 + 1 = n - 1$.

Soit $k \in \mathbb{N}$, supposons \mathcal{H}_k , soit $\sigma \in \Sigma_n$ qui se décompose en produit de $k+1$ transpositions.

$$\sigma = \underbrace{\tau_1 \circ \dots \circ \tau_k}_{\sigma'} \circ \tau_{k+1}$$

D'après \mathcal{H}_k , on a $\theta(\sigma') \geq n - k$. Notons $\tau_{k+1} = [a, b]$.

Si a et b appartiennent à la même orbite. On note (a_1, \dots, a_r) le cycle correspondant avec $a_r = a$ et $a_s = b$ où $s \in \{1, \dots, r-1\}$. On a

$$\begin{cases} (a_1, \dots, a_{r-1}, a_r) \circ [a, b](a_i) = a_{i+1} & \text{où } i \notin \{r, s\} \\ (a_1, \dots, a_{r-1}, a_r) \circ [a, b](a_r) = a_{s+1} \\ (a_1, \dots, a_{r-1}, a_r) \circ [a, b](a_s) = a_1 \end{cases}$$

On n'a pas perdu d'orbites, donc $\theta(\sigma) \geq n - k - 1$.

Si a et b n'appartiennent pas à la même orbite, notons (a_1, \dots, a_r) et (b_1, \dots, b_s) ces orbites avec $a = a_r$ et $b = b_s$. On a

$$\begin{cases} \underbrace{(a_1, \dots, a_{r-1}, a_r) \circ (b_1, \dots, b_s) \circ [a_r, b_s]}_{\sigma''}(a_i) = a_{i+1} & \text{où } i \in \{1, \dots, r-1\} \\ (a_1, \dots, a_{r-1}, a_r) \circ (b_1, \dots, b_s) \circ [a_r, b_s](b_j) = b_{j+1} & \text{où } j \in \{1, \dots, s-1\} \\ (a_1, \dots, a_{r-1}, a_r) \circ (b_1, \dots, b_s) \circ [a_r, b_s](a_r) = b_1 \\ (a_1, \dots, a_{r-1}, a_r) \circ (b_1, \dots, b_s) \circ [a_r, b_s](b_s) = a_1 \end{cases}$$

Donc

$$\sigma'' = (a_1, \dots, a_r, b_1, \dots, b_s)$$

On a perdu une orbite et donc $\theta(\sigma) \geq n - k - 1$. D'où le résultat par récurrence sur k .

Solution 1.4. On note par \bar{k} les éléments de $\mathbb{Z}/n\mathbb{Z}$ et par \tilde{l} les éléments de $\mathbb{Z}/m\mathbb{Z}$.

Soit f un morphisme. On pose $f(\bar{1}) = \tilde{x}$ où $x \in \{0, \dots, m-1\}$. On a donc $nf(\bar{1}) = f(\bar{0}) = \tilde{0}$.

On a donc $\tilde{nx} = \tilde{0}$ donc $m \mid nx$. On écrit $m = m_1(m \wedge n)$ et $n = n_1(m \wedge n)$. D'après le théorème de Gauss, on a donc $m_1 \mid x$. Donc $x = km_1$ avec $k \in \{0, \dots, (n \wedge m) - 1\}$.

Réciproquement, soit $k \in \{0, \dots, (n \wedge m) - 1\}$. On définit

$$\begin{aligned} f_k : \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/m\mathbb{Z} \\ \bar{l} &\mapsto \widetilde{lk m_1} \end{aligned}$$

Si $\bar{l} = \bar{l}'$, alors $n \mid l - l'$ et donc $nm_1 \mid (l - l')km_1$ puis $n_1(n \wedge m)m_1 \mid (l - l')km_1$ donc $m \mid (l - l')km_1$ d'où $\widetilde{lk m_1} = \widetilde{l'k m_1}$ donc f est bien définie et c'est évidemment un morphisme.

Soit $k, k' \in \{0, \dots, n \wedge m - 1\}$ avec $k \neq k'$. Si $\widetilde{km_1} = \widetilde{k'm_1}$ alors $m \mid (k - k')m_1$ et donc $n \wedge m \mid k - k'$ et $|k - k'| < n \wedge m$ donc $k = k'$ ce qui est absurde. Ainsi, les f_k sont distincts, on a donc $n \wedge m$ morphismes.

Remarque 1.2. Exemple pour l'exercice précédent : morphisme de $\mathbb{Z}/4\mathbb{Z}$ dans $\mathbb{Z}/6\mathbb{Z}$. On a $f(\bar{1}) = \tilde{x}$ d'où $4x = \tilde{0}$ donc $3 \mid x$ d'où $x \in \{0, 3\}$. On a donc le morphisme trivial $f_0 : \bar{l} \mapsto \tilde{0}$ et $f_1 : \bar{l} \mapsto \tilde{3l}$.

Solution 1.5. On considère $H = \{x \in G \mid x^2 = e_G\}$. Si $x \notin H$, alors $x^{-1} \neq x$ et donc $P = \prod_{x \in H} x$. H est le noyau du morphisme $x \mapsto x^2$ (morphisme car G est abélien) donc H est un sous-groupe. Soit K un sous-groupe de H et $a \in H \setminus K$. Montrons que $K \cup aK$ est un sous-groupe de H .

On a $e_G \in K \cup aK$. Soit $x \in K \cup aK \subset H$, on a $x^{-1} = x \in K \cup aK$. Soit $(x_1, x_2) \in (K \cup aK)^2$, si $(x_1, x_2) \in K^2$, c'est ok. Si $(x_1, x_2) \in (aK)^2$, on note $x_1 = a \cdot k_1$ et $x_2 = a \cdot k_2$ avec $(k_1, k_2) \in K^2$. On a $x_1 \cdot x_2 = a^2 \cdot k_1 \cdot k_2 = k_1 \cdot k_2 \in K$. Si $x_1 \in K$ et $x_2 \in aK$, alors $x_1 \cdot x_2 = a \cdot k_1 \cdot k_2 \in aK$. Donc $K \cup aK$ est un sous-groupe de H .

Soit $x \in K \cap aK$, il existe $(k_1, k_2) \in K^2$ tel que $k_1 = a \cdot k_2$ et $a \in K$ ce qui est impossible. Donc $K \cap aK = \emptyset$.

On construit alors par récurrence K_n : on pose $K_0 = \{e_G\}$ et à l'étape n , si $K_n = H$ on arrête, sinon il existe $a_{n+1} \in H \setminus K_n$ et on pose $K_{n+1} = K_n \cup a_{n+1}K$. Alors $|K_{n+1}| = 2|K_n|$. Comme H est fini, il existe $n_0 \in \mathbb{N}$ tel que $H = K_{n_0}$. On a alors $|H| = 2^{n_0}$.

Ainsi, si $n_0 = 0$, on a $H = \{e_G\}$ et $P = e_G$. Si $n_0 = 1$, on a $H = \{e_G, a_1\}$ et $P = a_1 \neq e_G$. Si $n_0 \geq 2$, comme chaque a_k apparaît un nombre pair de fois dans le produit, on a $P = e_G$.

Solution 1.6. Soit $x_0 \in \mathbb{R}$. $(\overline{kx_0})_{0 \leq k \leq n}$ ne sont pas deux à deux distincts. Donc il existe $l \neq l' \in \{0, \dots, n\}^2$ tel que $\overline{lx_0} = \overline{l'x_0}$ d'où $0 < |l - l'| \leq n$. Donc il existe $j \in \{1, \dots, n\}$ avec $jx_0 \in G$. Ainsi, $n!x_0 \in G$ (itéré de jx_0). Ce raisonnement est vrai pour $x = \frac{x_0}{n!}$ donc $x_0 \in G$. Ainsi, $G = \mathbb{R}$.

Solution 1.7. Soit f un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même. Soit $k \in \{0, \dots, n-1\}$, on a $f(\overline{k}) = kf(\overline{1})$. Par isomorphisme, $\omega(f(\overline{1})) = \omega(\overline{1}) = n$. Notons alors $\overline{x} = f(\overline{1})$ avec $x \in \{0, \dots, n-1\}$.

Si $x \wedge n = 1$, il existe $(u, v) \in \mathbb{Z}^2$ tel que $ux + vn = 1$, donc $u\overline{x} = \overline{1} \in \text{gr}\{\overline{x}\}$. Ainsi, $\mathbb{Z}/n\mathbb{Z} = \text{gr}\{\overline{x}\}$ (car les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont des itérés de $\overline{1}$) donc $\omega(\overline{x}) = n$.

Réciproquement, si $\omega(\overline{x}) = n$, $\overline{1} \in \text{gr}\{\overline{x}\}$ donc il existe $u \in \mathbb{Z}$ tel que $u\overline{x} = \overline{1} = \overline{ux}$. Donc $n \mid ux - 1$, c'est-à-dire qu'il existe $v \in \mathbb{Z}$ tel que $ux - 1 = vn$, d'où $ux + vn = 1$. D'après Bézout, on a $x \wedge n = 1$. Finalement, on a $\omega(\overline{x}) = n$ si et seulement si $x \wedge n = 1$.

Ainsi, les isomorphismes sont nécessairement de la forme

$$\begin{aligned} f_x : \mathbb{Z}/n\mathbb{Z} &\rightarrow \mathbb{Z}/n\mathbb{Z} \\ \overline{k} &\mapsto \overline{kx} \end{aligned}$$

où $x \in \{0, \dots, n-1\}$ et $x \wedge n = 1$.

Réciproquement, si $x \in \{0, \dots, n-1\}$ est tel que $x \wedge n = 1$, f_x est évidemment un morphisme. Si $\overline{k} \in \ker(f_x)$, on a $f_x(\overline{k}) = \overline{0}$ si et seulement si $\overline{kx} = \overline{0}$ si et seulement si $n \mid kx$ et comme $n \wedge x = 1$, d'après le théorème de Gauss, on a $n \mid k$ donc $\overline{k} = \overline{0}$ donc $\ker(f_x) = \{\overline{0}\}$. Donc f_x est injective, donc bijective car $|\mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}/n\mathbb{Z}| = n$.

Solution 1.8. Si $y \in \text{Im}\varphi$, y possède $|\ker \varphi|$ antécédents. En effet, il existe $x_0 \in G$ tel que $y = \varphi(x_0)$. Pour tout $x \in G$, on a $\varphi(x) = y$ si et seulement si $\varphi(x) = \varphi(x_0)$ si et seulement si $\varphi(x_0^{-1} \cdot x) = e_G$

si et seulement si $x_0^{-1} \cdot x \in \ker \varphi$ si et seulement si $x \in x_0 \ker \varphi$. Comme

$$\begin{aligned} g : \ker \varphi &\rightarrow x_0 \ker \varphi \\ x &\mapsto x \cdot x_0 \end{aligned}$$

est bijective, on a $|\ker \varphi| = |x_0 \ker \varphi|$. Ainsi, on a $|G| = |\operatorname{Im} \varphi| \times |\ker \varphi|$.

Dans tous les cas, on a $\ker \varphi \subset \ker \varphi^2$ et $\operatorname{Im} \varphi^2 \subset \operatorname{Im} \varphi$. On a ensuite

$$\begin{aligned} \operatorname{Im} \varphi^2 = \operatorname{Im} \varphi &\iff |\operatorname{Im} \varphi^2| = |\operatorname{Im} \varphi| \\ &\iff |\ker \varphi^2| |\operatorname{Im} \varphi^2| = |\ker \varphi^2| |\operatorname{Im} \varphi| = |G| = |\ker \varphi| |\operatorname{Im} \varphi| \\ &\iff |\ker \varphi^2| = |\ker \varphi| \\ &\iff \ker \varphi^2 = \ker \varphi \end{aligned}$$

Solution 1.9. On considère

$$\begin{aligned} f : G &\rightarrow G \\ x &\mapsto x^m \end{aligned}$$

l'exercice revient à montrer que f est bijective. D'après le théorème de Bézout, il existe $(a, b) \in \mathbb{Z}^2$ tel que $am + bn = 1$. Soit $y \in G$, on a

$$y^1 = y = y^{am+bn} = y^{am} \cdot \underbrace{y^{bn}}_{=e_G} = y^{am} = (y^a)^m$$

Donc f est surjective et comme G est fini, f est bijective.

Solution 1.10.

1. On a $e_G \in S_g$, si $(x, y) \in S_g^2$ alors $x \cdot y \cdot g = x \cdot g \cdot y = g \cdot x \cdot y$ donc $x \cdot y \in S_g$ et si $x \in S_g$ alors $x \cdot g = g \cdot x$ implique $g \cdot x^{-1} = x^{-1} \cdot g$ en multipliant par l'inverse de x à gauche et à droite donc $x^{-1} \in S_g$.
2. Soit $(h, h') \in G^2$. On a $h \cdot g \cdot h^{-1} = h' \cdot g \cdot h'^{-1}$ si et seulement si $g \cdot h^{-1} \cdot h' = h^{-1} \cdot h \cdot g$ si et seulement si $h^{-1} \cdot h \in S_g$ si et seulement si $h' \in hS_g$. Or $|hS_g| = |S_g|$ car

$$\begin{aligned} I_h : S_g &\rightarrow hS_g \\ x &\mapsto h \cdot x \end{aligned}$$

est bijective de réciproque $I_{h^{-1}}$. Soit la relation d'équivalence \mathcal{R}_0 sur G définie par $h\mathcal{R}_0h'$ si et seulement si $h \cdot g \cdot h^{-1} = h' \cdot g \cdot h'^{-1}$. Chaque classe à $|S_g|$ éléments et il y a $|C(g)|$ classes dans G d'où $|G| = |S_g| |C(g)|$.

3. On a $Z(G) = \cap_{g \in G} S_g$ donc $Z(G)$ est un sous-groupe et pour tout $g \in G$, $Z(G) \subset S_g$.

4. Pour $x \in G$, on note $\bar{x} = \{h \cdot x \cdot h^{-1} \mid h \in G\} = C(x)$.

On a $|\bar{x}| = 1$ si et seulement si pour tout $h \in G$, $h \cdot x \cdot h^{-1} = x$ si et seulement si $x \in Z(G)$.

Soit \mathcal{A} une partie de G telle que $(\bar{x})_{x \in \mathcal{A}}$ forme une partition de $G \setminus Z(G)$. On a

$$|G| = p^\alpha = |Z(G)| + \sum_{x \in \mathcal{A}} |C(x)|$$

Si $x \in \mathcal{A}$, $x \notin Z(G)$ donc $|S_x| < |G|$ (car $x \in Z(G)$ si et seulement si $S_x = G$) et donc

$$|C(x)| = \frac{|G|}{|S_x|}$$

d'après 2. Donc $|C(x)| = p^\beta$ avec $\beta \in \{1, \dots, \alpha\}$ car $|C(x)| \neq 1$. Donc

$$p \mid \sum_{x \in \mathcal{A}} |C(x)|$$

d'où

$$p \mid |Z(G)|$$

donc $|Z(G)| \neq 1$.

5. On a

$$p^2 = |Z(G)| + \sum_{x \in \mathcal{A}} |C(x)|$$

D'après la question 4, on a $|Z(G)| \neq 1$ et $|Z(G)| \mid |G|$.

Si $Z(G) \neq G$, alors $|Z(G)| = p$. Pour $x \in \mathcal{A}$, $Z(G) \subset S_x \neq G$ donc $|S_x| = p$ (car $|S_x| \mid |G|$) et donc $Z(G) = S_x$. Or $x \in S_x$ et $x \notin Z(G)$ ce qui n'est pas possible, donc $|Z(G)| = p^2$ et $Z(G) = G$. Donc G est abélien.

S'il existe un élément d'ordre p^2 . G est cyclique et est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$. Sinon, pour tout $x \in G \setminus \{e_G\}$, on a $\omega(x) = p$. Soit $x_1 \in G \setminus \{e_G\}$ et $x_2 \in G \setminus \text{gr}\{x_1\}$. Soit

$$\begin{aligned} f: \left(\mathbb{Z}/p\mathbb{Z}\right)^2 &\rightarrow G \\ (\bar{k}, \bar{l}) &\mapsto x_1^k \cdot x_2^l \end{aligned}$$

f est bien définie car si $\bar{k} = \bar{k}'$ et $\bar{l} = \bar{l}'$, on a $p \mid k - k'$ et $p \mid l - l'$ donc $x_1^k \cdot x_2^l = x_1^{k'} \cdot x_2^{l'}$.

Comme G est abélien, f est un morphisme.

Montrons que f est injective. Soit $(\bar{k}, \bar{l}) \in \ker(f)$ avec $(k, l) \in \{0, \dots, p-1\}^2$, on a $x_1^k \cdot x_2^l = e_G$ donc $x_2^l = x_1^{-k}$. Si $l \in \{1, \dots, p-1\}$ or p est premier donc $l \wedge p = 1$ donc il existe $(u, v) \in \mathbb{Z}^2$ tel que $lu + pv = 1$. Alors on a

$$x_2 = x_2^{lu+pv} = x_2^{lu} \cdot x_2^{pv} = x_2^{lu} = x_1^{-k} \in \text{gr}\{x_1\}$$

ce qui n'est pas possible. Donc $\bar{l} = \bar{0}$ et de même $\bar{k} = \bar{0}$ donc f est injective et ainsi $|\mathbb{Z}/p^2\mathbb{Z}| = |G|$ donc f est un isomorphisme.

Remarque 1.3. Les groupes de cardinal p^3 ne sont pas nécessairement abélien, par exemple le groupe des isométries du carré \mathcal{D}_4 de cardinal 8.

Solution 1.11. Soit f un morphisme de $(\mathbb{Z}, +)$ dans (\mathbb{Q}_+^*, \times) . Pour tout $n \in \mathbb{Z}$, $f(n) = f(1)^n$ donc il existe $r_0 \in \mathbb{Q}_+^*$ tel que $f(1) = r_0$ donc $f: n \mapsto r_0^n$.

Soit f un morphisme de $(\mathbb{Q}, +)$ dans (\mathbb{Q}_+^*, \times) . Pour tout $a \in \mathbb{N}^*$, $f(1) = f(\frac{1}{a})^a$. Pour tout p premier, on a $\nu_p(f(1)) = a\nu_p(f(\frac{1}{a}))$ donc pour tout $a \in \mathbb{N}^*$, $a \mid \nu_p(f(1))$ donc $\nu_p(f(1)) = 0$ pour tout p premier, donc $f(1) = 1$. Ainsi, pour tout $n \in \mathbb{Z}$, $f(n) = f(1)^n = 1$ et $f(b \times \frac{a}{b}) = f(a) = 1 = f(\frac{a}{b})^b$ donc $f(\frac{a}{b}) = 1$. Donc $f: r \mapsto 1$.

Solution 1.12. On a $xy = y^2x$, $x^2y = xy^2x = y^4x^2$, $x^3y = x^2y^2x = xy^4x^2 = y^8x^3$, $x^5y = y^{32}x^5$ donc $y^{31} = e_G$ et $\omega(y) = 31$. Tout élément de G peut s'écrire $y^\lambda x^\mu$ avec $(\lambda, \mu) \in \{0, \dots, 30\} \times \{0, \times 4\}$. Soit

$$\begin{aligned} f: \{0, \dots, 30\} \times \{0, \times 4\} &\rightarrow G \\ (\lambda, \mu) &\mapsto y^\lambda x^\mu \end{aligned}$$

est surjective par construction. Soit $((\lambda, \mu), (\lambda', \mu')) \in (\{0, \dots, 30\} \times \{0, \times 4\})^2$ tel que $y^\lambda x^\mu = y^{\lambda'} x^{\mu'}$ donc $y^{\lambda-\lambda'} = x^{p'-p}$ d'où $y^{5(\lambda-\lambda')} = x^{5(\mu'-\mu)} = e_G$. Or $\omega(y) = 31$ donc $31 \mid 5(\lambda - \lambda')$ et d'après le théorème de Gauss, $31 \mid \lambda - \lambda'$. Or $(\lambda, \lambda') \in \{0, \dots, 30\}^2$ donc $\lambda = \lambda'$ et de même $\mu = \mu'$ donc f est injective donc bijective et $|G| = 155$. Soit G' un autre tel groupe engendré par x' et y' , on forme

$$\begin{aligned} g: G &\rightarrow G \\ y^p x^\mu &\mapsto y'^\lambda x'^\mu \end{aligned}$$

et on vérifie que g est un isomorphisme.

Solution 1.13.

1. Soit $i \in \{1, \dots, r\}$, il existe nécessairement $y_i \in G$ tel que $\nu_{p_i}(\omega(y_i)) = p_i^{\alpha_i}$ (où ν_p est la valuation p -adique), sinon on ne pourrait pas avoir ce terme dans le ppcm. Donc $p_i^{\alpha_i} \mid \omega(y_i)$.

2. Il existe $n \in \mathbb{N}$ tel que $\omega(y_i) = p_i^{\alpha_i} n$. Posons $x_i = y_i^n \in G$. Alors pour $k \in \mathbb{N}$,

$$x_i^k = e_G \iff y_i^{nk} = e_G \iff \omega(y_i) \mid nk \iff p_i^{\alpha_i} \mid k$$

Donc $\omega(x_i) = p_i^{\alpha_i}$.

3. On pose $x = \prod_{i=1}^r x_i$. Soit $k \in \mathbb{N}$, alors

$$x^k = e_G \iff \prod_{i=1}^r x_i^k = e_G$$

Pour $i \in \{1, \dots, r\}$, on met le tout à la puissance $M_i = \prod_{\substack{j=1 \\ j \neq i}}^r p_j^{\alpha_j}$. On a alors, pour tout $i \in \{1, \dots, r\}$,

$$x_i^{kM_i} = e_G \iff p_i^{\alpha_i} \mid kM_i \iff p_i^{\alpha_i} \mid k$$

la dernière équivalence venant du théorème de Gauss. Donc pour tout $i \in \{1, \dots, r\}$, $p_i^{\alpha_i} \mid k$, ce qui équivaut donc à $N \mid k$ et donc $\omega(x) = N$.

Solution 1.14. Sur un corps commutatif, un polynôme de degré n admet au plus n racines. Montrons qu'il existe $x_1 \in \mathbb{K}^*$ tel que $\omega(x_1) = |\mathbb{K}^*|$. Par définition de N , pour tout $x \in \mathbb{K}^*$, $\omega(x) \mid N$. D'où $x^N = 1_{\mathbb{K}}$. Donc x est racine de $X^N - 1$. Ainsi, $|\mathbb{K}^*| \leq N$. Par ailleurs, $N \mid |\mathbb{K}^*|$ car pour tout $x \in \mathbb{K}^*$, $x^{|\mathbb{K}^*|} = 1_{\mathbb{K}^*}$. Donc $|\mathbb{K}^*| = N$ et donc $\mathbb{K}^* = \text{gr}\{x_1\}$.

On a $|\mathbb{Z}/13\mathbb{Z}^*| = 12$ donc pour tout $\bar{x} \in (\mathbb{Z}/13\mathbb{Z})^*$, $\omega(\bar{x}) \in \{1, 2, 3, 4, 6, 12\}$. On a $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{8}$, $\bar{2}^4 = \bar{16} = \bar{3}$, $\bar{2}^6 = \bar{12}$ donc $\omega(\bar{2}) = 12$ et

$$\mathbb{Z}/13\mathbb{Z}^* = \text{gr}\{\bar{2}\} = \left\{ \bar{2}^k \mid k \in \{0, \dots, 11\} \right\}$$

Solution 1.15.

1. Soit $(x, y) \in G^2$, on a $(x \cdot y)^2 = (x \cdot y) \cdot (x \cdot y) = e_G$ donc $x \cdot y = y^{-1} \cdot x^{-1}$ et comme $x^2 = e_G$, $x^{-1} = x$ d'où $xy = yx$ et G est abélien.

2. Soit (x_1, \dots, x_n) une famille génératrice minimale de G : pour tout $x \in G$, il existe $(\varepsilon_i) \in \{0, 1\}^n$ tel que $x = \prod_{i=1}^n x_i^{\varepsilon_i}$ (car G est abélien). Soit

$$\begin{aligned} f : (\mathbb{Z}/2\mathbb{Z})^n &\rightarrow G \\ (\bar{\varepsilon}_1, \dots, \bar{\varepsilon}_n) &\mapsto \prod_{i=1}^n x_i^{\varepsilon_i} \end{aligned}$$

Si pour tout $i \in \{1, \dots, n\}$ on a $\overline{\varepsilon_i} = \overline{\varepsilon'_i}$, alors $x^{\varepsilon_i} = x^{\varepsilon'_i}$ car $x_i^2 = e_G$ et $2 \mid \varepsilon_i - \varepsilon'_i$. Donc f est bien définie.

f est clairement un morphisme (car G est abélien). D'après la première question, f est surjective. Montrons que f est injective. Soit $(\overline{\varepsilon_1}, \dots, \overline{\varepsilon_n})$ tel que $\prod_{i=1}^n x_i^{\varepsilon_i} = e_G$. Soit $i \in \{1, \dots, n\}$, supposons ε_i impair, on a alors $x_i = \varepsilon_i = x_i$. D'où $x_i = \prod_{j=1}^n x_j^{-\varepsilon_j} = \prod_{j=1}^n x_j^{\varepsilon_j}$ car $x^2 = e_G$. Donc $x_i \in \text{gr}(x_j, j \in \{1, \dots, n\}, j \neq i)$, ce qui contredit le caractère minimal de (x_1, \dots, x_n) . Ainsi, f est injective donc est un isomorphisme.

Remarque 1.4. En notant $+$ la loi sur G , on peut définir

$$\begin{aligned} f : \mathbb{Z}/2\mathbb{Z} \times G &\rightarrow G \\ (\varepsilon, x) &\mapsto x^\varepsilon \end{aligned}$$

. Alors $(G, +, \cdot)$ est un $\mathbb{Z}/2\mathbb{Z}$ -espace vectoriel, de dimension finie n car G est fini, et le choix d'une base réalise un isomorphisme de $(\mathbb{Z}/2\mathbb{Z})^n, +$ dans $(G, +)$.

Remarque 1.5. Par isomorphisme, on a

$$\prod_{x \in G} x = f\left(\sum_{(\overline{\varepsilon_1}, \dots, \overline{\varepsilon_n}) \in (\mathbb{Z}/2\mathbb{Z})^n} (\overline{\varepsilon_1}, \dots, \overline{\varepsilon_n})\right)$$

Pour $n = 1$, on a $\overline{0} + \overline{1} = \overline{1}$, pour $n = 2$, on a $(\overline{0}, \overline{0}) + (\overline{0}, \overline{1}) + (\overline{1}, \overline{0}) + (\overline{1}, \overline{1}) = (\overline{0}, \overline{0})$. Pour $n > 2$, $\overline{1}$ apparaît 2^{n+1} fois sur chaque coordonnée (donc un nombre pair de fois), donc la somme fait $(\overline{0}, \dots, \overline{0})$.

Solution 1.16.

1. Si G est abélien, on a $D(G) = \{e_G\}$.
2. Soit $\sigma \in \mathcal{A}_n$, σ se décompose en un produit d'un nombre pair de transpositions. Soient $[a, b]$ et $[c, d]$ deux transpositions.
 - Si $\{a, b\} = \{c, d\}$, alors $[a, b] \circ [c, d] = \text{id}$.
 - Si $a \in \{c, d\}$, supposons par exemple $a = c$ et $b \neq d$. On a alors $[a, b] \circ [c, d] = [a, b] \circ [a, d] = [b, a, d]$.
 - Si $\{a, b\} \cap \{c, d\} = \emptyset$, on a

$$[a, b] \circ [c, d] = [a, b] \circ \underbrace{[b, c] \circ [b, c]}_{=\text{id}} \circ [c, d] = [a, b, c] \circ [b, c, d]$$

Donc les 3-cycles engendrent \mathcal{A}_n .

3. On a

$$\sigma \circ (a_1, a_2, a_3) \circ \sigma^{-1} = (\sigma(a_1), \sigma(a_2), \sigma(a_3))$$

On peut trouver $\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ telle que a_i soit envoyé sur b_i pour $i \in \{1, 2, 3\}$ et les éléments $\{1, \dots, n\} \setminus \{a_1, a_2, a_3\}$ dans $\{1, \dots, n\} \setminus \{b_1, b_2, b_3\}$. Donc les 3-cycles sont conjugués dans Σ_n .

Si $n \geq 5$ et σ impair, soit $(c_1, c_2) \in \{1, \dots, n\} \setminus \{a_1, a_2, a_3\}$. $\sigma' = \sigma \circ [c_1, c_2]$ est pair et $\sigma'(a_i) = b_i$. Donc les trois cycles sont conjugués dans \mathcal{A}_n pour $n \geq 5$. C'est cependant faux pour $n = 3$ et $n = 4$.

4. Soit $(\sigma, \sigma') \in \Sigma_n^2$. En notant \mathcal{E} la signature d'une permutation (morphisme de (Σ_n, \circ) dans $(\{-1, 1\}, \times)$), on a

$$\mathcal{E}(\sigma \circ \sigma^{-1} \circ \sigma' \circ \sigma'^{-1}) = 1$$

donc $\sigma \circ \sigma^{-1} \circ \sigma' \circ \sigma'^{-1} \in \mathcal{A}_n$. Donc $D(\Sigma_n) \subset \mathcal{A}_n$.

Soit ensuite (a_1, a_2, a_3) un 3-cycle. On a $(a_1, a_3, a_2)^2 = (a_1, a_2, a_3)$ et $(a_1, a_3, a_2)^{-1} = (a_1, a_2, a_3)$. Ainsi, on a

$$\sigma \circ (a_1, a_3, a_2) \circ \sigma^{-1} \circ (a_1, a_2, a_3) = (a_1, a_3, a_2)^2 = (a_1, a_2, a_3)$$

On pose $\sigma = [a_2, a_3]$, et alors (a_1, a_2, a_3) est un commutateur. Ainsi, $(a_1, a_2, a_3) \in D(\Sigma_n)$ et donc $\mathcal{A}_n \subset D(\Sigma_n)$ (d'après la première question).

Finalement, on a $D(\Sigma_n) = \mathcal{A}_n$.

Remarque 1.6. Pour $n \geq 5$, on a $D(\mathcal{A}_n) = \mathcal{A}_n$.

Solution 1.17.

1. Pour $g \in G$, τ_g est bijective de réciproque $\tau_{g^{-1}}$. On a notamment $\tau_{g \cdot g'} = \tau_g \circ \tau_{g'}$ donc τ est un morphisme. Si $g \in G$ est tel que $\tau_g = \text{id}$, pour tout $x \in G$, on a $gx = x$ donc $g = e_G$. Donc τ est un morphisme injectif et G est isomorphe à $\text{Im} \tau = \tau(G)$, sous-groupe de $\Sigma(G)$, lui-même isomorphe à Σ_n .

2. Soit

$$\begin{aligned} f: \Sigma_n &\rightarrow GL_n(\mathbb{C}) \\ \sigma &\mapsto (\delta_{i, \sigma(j)})_{1 \leq i, j \leq n} = P_\sigma \end{aligned}$$

P_σ est la matrice de permutation associée à σ . f est un morphisme, et est injectif, donc G est isomorphe à un sous-groupe de $GL_n(\mathbb{C})$.

Solution 1.18. Soit $(x, y, z, t) \in \mathbb{N}^4$ tel que $x^2 + y^2 + z^2 = 8t + 7$. Dans $\mathbb{Z}/8\mathbb{Z}$, on a $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$, $\overline{2}^2 = \overline{4}$, $\overline{3}^2 = \overline{1}$, $\overline{4}^2 = \overline{0}$, $\overline{5}^2 = \overline{1}$, $\overline{6}^2 = \overline{4}$ et $\overline{7}^2 = \overline{1}$. Donc la somme de 3 de ces classes ne donnent pas $\overline{7}$.

Par récurrence, prouvons la propriété. Soit $(x, y, z, t) \in \mathbb{N}^4$ tel que $x^2 + y^2 + z^2 = (8t + 7)4^{n+1}$. Parmi x, y, z les trois sont pairs ou deux d'entre eux sont impairs. Si x, y impairs et z pair, on écrit $x = 2x' + 1, y = 2y' + 1, z = 2z'$, alors $x^2 + y^2 + z^2 \equiv 2[4]$ mais $(8t + 7)4^{n+1} \equiv 0[4]$: contradiction. Nécessairement, x, y et z sont pairs. En divisant par 4, on se ramène donc à l'hypothèse de récurrence.

Solution 1.19. On raisonne sur $\mathbb{Z}/7\mathbb{Z}$. On a $\overline{10^{10^n}} = \overline{3^{10^n}}$. Dans le groupe $((\mathbb{Z}/7\mathbb{Z})^*, \times)$, $\overline{3}$ a un ordre qui divise $|\mathbb{Z}/7\mathbb{Z}^*| = 6$. On a $\overline{3}^2 = \overline{2}$, $\overline{3}^3 = \overline{-1}$ et $\overline{3}^6 = \overline{1}$. Donc $\overline{3}^{6k} = \overline{1}$, $\overline{3}^{6k+1} = \overline{3}$, $\overline{3}^{6k+2} = \overline{2}$, $\overline{3}^{6k+3} = \overline{-1}$, $\overline{3}^{6k+4} = \overline{4}$ et $\overline{3}^{6k+5} = \overline{5}$.

On se place maintenant dans $\mathbb{Z}/6\mathbb{Z}$: $\overline{10} = \overline{4}$, $\overline{10}^2 = \overline{4}$ et donc par récurrence sur $n \in \mathbb{N}^*$, $\overline{10^n} = \overline{4}$. Donc il existe $k \in \mathbb{Z}$ tel que $10^n = 6k + 4$. Ainsi, $\overline{10^{10^n}} = \overline{4}$.

Solution 1.20.

1. On a $F_1 = 5$ et $2 + \prod_{k=0}^0 F_k = 2 + 3 = 5$. Soit $n \geq 1$, supposons que $F_n = 2 + \prod_{k=0}^{n-1} F_k$.

Alors

$$\begin{aligned} F_{n+1} - 2 &= 2^{2^{n+1}} - 1 = (2^{2^n})^2 - 1 \\ &= (2^{2^n} + 1)(2^{2^n} - 1) \\ &= F_n(F_n - 2) \\ &= F_n \times \prod_{k=0}^{n-1} F_k \\ &= \prod_{k=0}^n F_k \end{aligned}$$

d'où le résultat par récurrence.

2. Soit p un facteur premier de F_n . S'il existe $k \in \{0, \dots, n-1\}$ tel que $p \mid F_k$, alors d'après la première question on a $p \mid F_n - \prod_{k=0}^{n-1} F_k = 2$. Donc $p = 2$. Or F_n est impair, donc

non divisible par deux, ce qui est absurde. Donc p ne divise aucun F_k pour $k \in \{0, n-1\}$ et il existe donc une infinité de nombres premiers (car les F_n sont tous différents deux à deux).

Remarque 1.7. Si $n \neq m$ alors $F_n \wedge F_m = 1$.

Solution 1.21.

1. On teste uniquement les puissances qui divisent 32 : 2, 4, 8, 16, 32. On a $\bar{5}^2 = \bar{-7}, \bar{5}^4 = \bar{-15}, \bar{5}^8 = \bar{1}$. Donc $\omega(\bar{5}) = 8$.

2. On note

$$\begin{aligned} \psi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} &\rightarrow U \\ (k, \tilde{l}) &\mapsto \bar{-1}^k \times \bar{5}^l \end{aligned}$$

3. On a $\omega(\bar{-1}) = 2$ et $\gamma(\bar{5}) = 8$ donc ψ est bien définie. ψ est bien un morphisme de groupes. Soit $(k, \tilde{l}) \in \ker(\psi)$, on a $\bar{-1}^k \times \bar{5}^l = \bar{1}$. Si $k = \dot{1}$, alors $\bar{-1}^k = \bar{-1} = \bar{5}^{-l} = \bar{5}^l \in \text{gr}\{\bar{5}\}$. Donc $\bar{5}^{2l} = \bar{1}$ et ainsi $8 \mid 2l$ d'où $4 \mid l$. Mais alors $l \in \{0, 4\}$ ce qui est impossible. Donc $k \neq \dot{1}$. De ce fait, $k \neq \dot{1}$. Ainsi, $\bar{5}^l = \bar{1}$ donc $\tilde{l} = \tilde{0}$. Ainsi, $\ker(\psi) = \{(\dot{0}, \tilde{0})\}$ donc ψ est injective, puis bijective car $|\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}| = |U|$.

Remarque 1.8. U n'est pas cyclique car, par isomorphisme, ses éléments ont un ordre qui divise 8.

Solution 1.22.

1. Soit

$$\begin{aligned} f : G_n \times G_m &\rightarrow U_{nm} \\ (\xi, \xi') &\mapsto \xi \times \xi' \end{aligned}$$

Soit $(\xi, \xi') \in G_n \times G_m$, Soit $k \in \mathbb{Z}$ tel que $(\xi \times \xi')^k = 1$. Alors $(\xi \times \xi')^{km} = 1$ d'où $\xi^{km} = 1$ donc $n \mid km$ et $n \mid k$ d'après le théorème de Gauss. De même pour n , on a $m \mid k$ et donc $nm \mid k$. La réciproque est immédiate : $\xi \times \xi' \in G_{nm}$. Donc $f(G_n \times G_m) \subset G_{nm}$ et $|G_n \times G_m| = \varphi(n) \times \varphi(m) = \varphi(nm) = |G_{nm}|$ où φ est l'indicatrice d'Euler.

Montrons que f est injective : soit $(x, y, x', y') \in G_n^2 \times G_m^2$ tel que $xx' = yy'$. On a alors $x^m = y^m$ et $x'^n = y'^n$ d'où $(xy^{-1})^m = 1$ d'où $\omega(xy^{-1}) \mid m$ et $\omega(xy^{-1}) \mid n$. Donc $\omega(xy^{-1}) = 1$ donc $x = y$ et en reportant, on a $x' = y'$. Donc f est injective puis bijective (égalité des cardinaux).

On a alors

$$\begin{aligned}
\mu(n)\mu(m) &= \sum_{\xi \in G_n} \xi \times \sum_{\xi' \in G_m} \xi' \\
&= \sum_{(\xi, \xi') \in G_n \times G_m} \xi \xi' \\
&= \sum_{\xi \in G_{nm}} \xi \text{ [} f \text{ est bijective]} \\
&= \mu(nm)
\end{aligned}$$

2. On a $\mu(1) = 1$. Soit p premier. On a

$$\sum_{k=0}^{p-1} e^{\frac{2ik\pi}{p}} = 0$$

donc

$$\mu(p) \sum_{k=1}^{p-1} e^{\frac{2ik\pi}{p}} = -1$$

. Soit alors $\alpha \in \mathbb{N}$ avec $\alpha \geq 2$, on a

$$\mu(p^\alpha) = \sum_{\substack{k=1 \\ k \wedge p=1}}^{p^\alpha} e^{\frac{2ik\pi}{p^\alpha}} = \sum_{k=1}^{p^\alpha} e^{\frac{2ik\pi}{p^\alpha}} - \sum_{k=1}^{p^{\alpha-1}} e^{\frac{2ik\pi}{p^{\alpha-1}}} = 0$$

Si $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, s'il existe $i \in \{1, \dots, r\}$ tel que $\alpha_i \geq 2$ alors $\mu(n) = 0$. Sinon, on a

$$\mu(n) = \prod_{i=1}^r \mu(p_i) = (-1)^r$$

3. Soit $(f, g) \in (\mathbb{C}^{\mathbb{N}^*})^2$, on a

$$\begin{aligned}
(f \star g)(n) &= \sum_{d_1 d_2 = n} f(d_1) g(d_2) \\
&= \sum_{d_1 d_2 = n} g(d_1) f(d_2) \\
&= (g \star f)(n)
\end{aligned}$$

Donc \star est commutative.

Soit $(f, g, h) \in (\mathbb{C}^{\mathbb{N}^*})^3$, on a

$$\begin{aligned}
(f \star (g \star h))(n) &= \sum_{d_1 d = n} f(d_1)(g \star h)(d) \\
&= \sum_{d_1 d = n} \left[f(d_1) \times \sum_{d_2 d_3 = d} g(d_2)h(d_3) \right] \\
&= \sum_{d_1 d_2 d_3 = n} f(d_1)g(d_2)h(d_3) \\
&= ((f \star g) \star h)(n)
\end{aligned}$$

donc \star est associative.

On vérifie maintenant que l'élément neutre est $e : \mathbb{N}^* \rightarrow \mathbb{C}$ qui à 1 associe 1 et 0 si $n \geq 2$. Soit

$$\begin{aligned}
\psi : \mathbb{N} &\rightarrow \mathbb{Z} \\
n &\mapsto \sum_{d|n} \mu(d)
\end{aligned}$$

On a $\psi(1) = 1$. Soit $n \geq 2$ avec $n = \prod_{i=1}^r p_i^{\alpha_i}$. Les diviseurs de n sont dans $D = \{\prod_{i=1}^r p_i^{\beta_i} \mid \beta_i \leq \alpha_i\}$. Ainsi, $\psi(n) = \sum_{d \in D} \mu(d)$. Or $\mu(d)$ vaut 0 s'il existe $\beta_i \geq 2$ et $(-1)^k$ si k β_i valent 1 et les autres 0. Il y a $\binom{r}{k}$ choix possibles pour que k β_i valent 1. Ainsi,

$$\psi(n) = \sum_{k=0}^r 1^{r-k} (-1)^k \binom{r}{k} = 0$$

Donc $\mu \star 1 = e$, et $\mu^{-1} = 1 : n \mapsto 1$ pour tout $n \in \mathbb{N}$.

4. On note

$$\begin{aligned}
id : \mathbb{N}^* &\rightarrow \mathbb{N}^* \\
n &\mapsto n
\end{aligned}$$

Alors

$$\begin{aligned}
\sum_{d|n} d \mu\left(\frac{n}{d}\right) &= (\mu \star id)(n) \\
&= (id \star \mu)(n) \\
&= (1 \star (\varphi \star \mu))(n) \\
&= \varphi(n)
\end{aligned}$$

la troisième égalité venant du fait que $id = 1 \star \varphi$ car $n = \sum_{d|n} \varphi(d)$.

Solution 1.23. Pour $k \in \{1, \dots, p-1\}$, on a

$$\binom{p+k}{k} = \frac{(p+k) \times \dots \times (p+1)}{k \times \dots \times 1} = 1 + \alpha kp$$

car $(p+k) \times \dots \times (p+1) = k! + p \times \text{qqchse}$. On a $p \mid \binom{p}{k}$ donc

$$\sum_{k=1}^{p-1} \binom{p}{k} \binom{p+k}{k} \equiv \sum_{k=1}^{p-1} \binom{p}{k} [p^2]$$

Pour $k=0$, on a $\binom{p}{0} \binom{p}{0} = 1$ et pour $k=p$, on a $\binom{p}{p} \binom{2p}{p} = \binom{2p}{p}$. Et

$$\sum_{k=1}^{p-1} \binom{p}{k} = \sum_{k=0}^p \binom{p}{k} - 2 = 2^p - 2$$

Il reste donc à prouver que $\binom{2p}{p} \equiv 2[p^2]$.

Or

$$\binom{2p}{p} = \sum_{k=0}^p \binom{p}{k} \binom{p}{p-k} \equiv 2[p^2]$$

la première égalité venant de l'égalité du terme en X^p dans $(1+X)^{2p} = (1+X)^p(1+X)^p$, et la deuxième venant du fait que seuls les termes en $k=0$ et $k=p$ ne contiennent pas de p^2 , et valent chacun 1.

Finalement, on a

$$\sum_{k=0}^p \binom{p}{k} \binom{p+k}{k} \equiv 2^p - 2 + 1 + 2[p^2] \equiv 2^p + 1[p^2]$$

Solution 1.24.

1. Soit G un sous-groupe de (\mathbb{U}, \times) . On note $|G| = d$. On a donc $G \subset \mathbb{U}_d$ car pour tout $x \in G$, $x^d = 1$. Donc $G = \mathbb{U}_d$ est cyclique.

2. On pose

$$\begin{aligned} \psi : SO_2(\mathbb{R}) &\rightarrow (\mathbb{U}, \times) \\ R_\theta &\mapsto e^{i\theta} \end{aligned}$$

qui est un isomorphisme. Donc les sous-groupes de $SO_2(\mathbb{R})$ sont les G_n pour $n \geq 1$ avec

$$G_n = \{R_{\frac{2k\pi}{n}} \mid k \in \{0, \dots, n-1\}\}$$

3. φ est bilinéaire et symétrique. Pour tout $X \in \mathbb{R}^2$, on $\varphi(X, X) = \sum_{M \in G} \|MX\|^2 \geq 0$ et si $\varphi(X, X) = 0$, on a pour tout $M \in G$, $X = 0$. Notamment, $I_2 \in G$ et donc $X = 0$. Donc φ est bien un produit scalaire.

Pour tout $(M_0, X, Y) \in G \times (\mathbb{R}^2)^2$, on a $\varphi(M_0X, M_0Y) = \sum_{M \in G} \langle MM_0X, MM_0Y \rangle$ et $M \mapsto MM_0$ est bijective de G dans G donc $\varphi(M_0X, M_0Y) = \varphi(X, Y)$.

Soit \mathcal{B}_0 la base canonique de \mathbb{R}^2 et \mathcal{B}_1 une base orthonormée pour φ . On note $P_0 = \text{mat}_{\mathcal{B}_0 \rightarrow \mathcal{B}_1}$.

Pour tout $M \in G$, $P_0^{-1}MP_0$ est la matrice d'une isométrie pour φ dans une base orthonormée pour φ . Donc $P_0^{-1}MP_0$ est orthogonale, et $\det(P_0^{-1}MP_0) = 1$ car pour tout $M \in G$, $\det(M) = 1$. Ainsi, $\{P_0^{-1}MP_0 \mid M \in G\}$ est un sous-groupe fini de $SO_2(\mathbb{R})$, donc cyclique. Il est isomorphe à G donc G est cyclique.

Solution 1.25.

1. On a $1 = 1 + 0\sqrt{2} \in E$. On remarque ensuite que pour tout $s = x + y\sqrt{2} \in E$, on a $ss^{-1} = 1$ avec $s^{-1} = x - y\sqrt{2} \in E$. Soit $(s, s') \in E^2$ avec $s = x + y\sqrt{2}$ et $s' = x' + y'\sqrt{2}$. Notons déjà que $x + y\sqrt{2} > 0$ car $x = \sqrt{1 + 2y^2} > |y|\sqrt{2}$. On a donc

$$ss' = \underbrace{xx' + 2yy'}_{\in \mathbb{Z}} + \sqrt{2} \underbrace{(yx' + y'x)}_{\in \mathbb{Z}}$$

On a $xx' \in \mathbb{N}$ et $x > \sqrt{2}|y| \geq 0$ et $x' > \sqrt{2}|y'| \geq 0$ donc $xx' > 2|yy'|$ et ainsi $xx' + 2yy' \in \mathbb{N}^*$. Enfin, on a

$$\begin{aligned} (xx' + 2yy')^2 - 2(yx' + y'x)^2 &= (xx')^2 + 4(yy')^2 - 2(yx')^2 - 2(y'x)^2 \\ &= (x^2 - 2y^2)(x'^2 - 2y'^2) \\ &= 1 \end{aligned}$$

Donc $ss' \in E$. Finalement, E est un sous-groupe de (\mathbb{R}_+^*, \times) .

2. \ln est un isomorphisme de E sur $\ln(E)$, sous-groupe de $(\mathbb{R}, +)$. On sait que si

$$\underbrace{\inf(\ln(E) \cap \mathbb{R}_+)}_{\alpha} > 0$$

alors $\ln(E) = \alpha\mathbb{Z}$ (sous-groupe de $(\mathbb{R}, +)$ dans le cas $\alpha > 0$, pour rappel si $\alpha = 0$ alors le sous-groupe est dense dans \mathbb{R}). On cherche la borne inférieure de $E \cap]1 + \infty[$ que l'on note β . β existe car cet ensemble est non vide, par exemple $3 + 2\sqrt{2}$ y appartient.

Si $\beta = 1$, on peut trouver une suite de termes de E strictement décroissante convergeant vers 1. Alors pour tout $n \in \mathbb{N}$, on a

$$1 < x_{n+1} + y_{n+1}\sqrt{2} < x_n + y_n\sqrt{2}$$

On sait que

$$x_n - y_n\sqrt{2} = (x_n + y_n\sqrt{2})^{-1} < 1 < x_n + y_n\sqrt{2}$$

donc $-y_n\sqrt{2} < 1 - x_n < 0$ donc $y_n > 0$. Ainsi,

$$y_n = \sqrt{\frac{x_n^2 - 1}{2}}$$

Si $x_{n+1} \geq x_n$, alors $y_{n+1} \geq y_n$ d'où $x_{n+1} + \sqrt{2}y_{n+1} > x_n + \sqrt{2}y_n$ ce qui est absurde. Donc $x_{n+1} < x_n$ et on obtient une suite strictement décroissante d'entiers naturels ce qui est impossible. Donc $\beta > 1$ et $E = \{(x_0 + y_0\sqrt{2})^n \mid n \in \mathbb{Z}\}$ est monogène.

On peut identifier β :

$$x_0 = \min\{x \in \mathbb{N}^* \setminus \{1\}, \exists y \in \mathbb{Z}, x + y\sqrt{2} \in E \cap], +\infty[\}$$

Donc $\beta = 3 + 2\sqrt{2}$ Finalement, $x^2 - 2y^2 = 1$ avec $x \in \mathbb{N}, y \in \mathbb{N}$ si et seulement s'il existe $n \in \mathbb{N}$ tel que $x_n + y_n\sqrt{2} = \beta^n$.

Remarque 1.9. En fait, on a

$$\begin{cases} x_n &= \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{2k} 2^{2k} 3^{n-2k} \\ y_n &= \sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} \binom{n}{2k+1} 2^{2k+1} 3^{n-2k-1} \end{cases}$$

Solution 1.26. On a $7 \mid n^n - 3$ si et seulement si $\bar{n}^n = \bar{3}$ dans $\mathbb{Z}/7\mathbb{Z}$. $(\mathbb{Z}/7\mathbb{Z}^*, \times)$ est un groupe de cardinal 6. Donc l'ordre de ses éléments divise 6, et sont donc 1, 2, 3 ou 6. Notamment, on vérifie que $\omega(\bar{3}) = 6$ et donc le groupe engendré par $\bar{3}$ est exactement $(\mathbb{Z}/7\mathbb{Z}^*, \times)$. Ainsi,

$$(\mathbb{Z}/7\mathbb{Z}^*, \times) = \{\bar{3}^k \mid k \in \{0, \dots, 5\}\}$$

(c'est un groupe cyclique). Les générateurs sont $\{\bar{3}^k, k \wedge 6 = 1\} = \{\bar{3}, \bar{3}^5 = \bar{-2} = \bar{5}\}$. Donc $\bar{n} = \bar{3}$ ou $\bar{n} = \bar{5}$.

Si $\bar{n} = 3$, $\bar{3}^n = \bar{3}$ si et seulement si $n \equiv 1[6]$ donc $n \equiv 3[7]$ et $n \equiv 1[6]$. D'après le théorème des restes chinois, on vérifie que ceci équivaut à $n \equiv 31[42]$. La réciproque est immédiate.

Si $\bar{n} = 5$, $\bar{5}^n = \bar{3}$ si et seulement si $n \equiv 5[6]$ et $n \equiv 5[7]$. D'après le théorème des restes chinois, on vérifie que ceci équivaut à $n \equiv 5[42]$.

Donc les solutions sont $n \in \mathbb{N}^*$ tels que $n \equiv 31[42]$ ou $n \equiv 5[42]$.

Solution 1.27. On a

$$\begin{aligned} \sum_{k=1}^{p-1} \frac{1}{k} + \frac{1}{p-k} &= \frac{2a}{(p-1)!} \iff \sum_{k=1}^{p-1} \frac{p}{k(p-k)} = \frac{2a}{(p-1)!} \\ &\iff \sum_{k=1}^{p-1} \frac{p(p-1)!}{k(p-k)} = 2a \\ &\iff p \underbrace{\sum_{k=1}^{p-1} \frac{(p-1)!^3}{k(p-k)}}_{\in \mathbb{N}} = 2a \underbrace{(p-1)!^2}_{p \wedge (p-1)!^2 = 1} \end{aligned}$$

donc $p \mid a$ d'après le théorème de Gauss.

On écrit alors $a = p \times b$ avec $b \in \mathbb{N}$. On a alors

$$\sum_{k=1}^{p-1} \frac{1}{k(p-k)} = \frac{2b}{(p-1)!}$$

comme $(p-1)!, k$ et $p-k$ ($1 \leq k \leq p$) sont inversibles dans $\mathbb{Z}/p\mathbb{Z}$, on a alors

$$\sum_{k=1}^{p-1} \overline{-k}^{-2} = \overline{2b} \times \underbrace{\overline{(p-1)!}^{-1}}_{=-1 \text{ d'après le théorème de Wilson}}$$

Donc

$$\overline{2b} = \sum_{k=1}^{p-1} \overline{k}^{-2}$$

Comme

$$\begin{aligned} f : \mathbb{Z}/p\mathbb{Z}^* &\rightarrow \mathbb{Z}/p\mathbb{Z}^* \\ \overline{k} &\mapsto \overline{k}^{-1} \end{aligned}$$

est bijective, on a

$$\overline{2} \times \overline{b} = \sum_{k=1}^{p-1} \overline{k}^2 = \frac{\overline{p(p-1)(2p-1)}}{6}$$

Or $p \geq 5$ est premier, donc $p - 1$ est pair et p est congru à 1 ou 2 modulo 3. Donc $p - 1 \equiv 0[3]$ ou $2p - 1 \equiv 0[3]$ donc $\frac{(p-1)(2p-1)}{6} \in \mathbb{N}$. Ainsi,

$$\bar{2} \times \bar{b} = \sum_{k=1}^{p-1} \bar{k}^2 = \bar{p} \times \frac{(p-1)(2p-1)}{6} = 0$$

et donc $p \mid b$ par le théorème de Gauss. Donc $p^2 \mid a$.

Solution 1.28. Les racines réelles de P ont une multiplicité paire, le coefficient dominant est positif (car la limite en $+\infty$ est positive) et les racines complexes non réelles sont 2 à 2 conjuguées :

$$(X - \alpha)(X - \bar{\alpha}) = X^2 - 2\Re(\alpha)X + |\alpha|^2 = (X - \Re(\alpha))^2 + |\Im(\alpha)|^2$$

avec $\Im(\alpha) \neq 0$. D'où le résultat en décomposant P sur $\mathbb{C}[X]$.

Solution 1.29.

1. $G = \mathbb{Z} + \alpha\mathbb{Z}$ est un sous-groupe de \mathbb{R} engendré par α et 1. S'il existait $a \in \mathbb{R}_+^*$ tel que $G = a\mathbb{Z}$, alors il existait $(n, m) \in (\mathbb{Z}^*)^2$ tel que $1 = na$ et $\alpha = ma$, d'où $\alpha = \frac{m}{n} \in \mathbb{Q}$ ce qui est absurde. Donc G est dense dans \mathbb{R} . Le fait que $\mathbb{Z} + \alpha\mathbb{N}$ est dense dans \mathbb{R} est alors immédiate.
2. Posons $\beta = \frac{\alpha}{2\pi} \notin \mathbb{Q}$. Alors $\mathbb{Z} + \beta\mathbb{N}$ est dense dans \mathbb{R} . Soit $c < d \in \mathbb{R}^2$. Comme $\frac{c}{2\pi} < \frac{d}{2\pi}$, il existe $x \in \mathbb{Z} + \beta\mathbb{N} \cap]\frac{c}{2\pi}, \frac{d}{2\pi}[$ et alors $2\pi x \in 2\pi\mathbb{Z} + \alpha\mathbb{N} \cap]c, d[$. On pose $c = \arcsin(a)$ et $d = \arcsin(b)$ avec $a < b$. On a bien $c < d$ car \arcsin est strictement croissante. Alors il existe $(m, n) \in \mathbb{Z} \times \mathbb{N}$ tel que $2\pi m + \alpha n = 2\pi x \in]c, d[$ donc $\sin(2\pi x) = \sin(2\pi m + \alpha n) = \sin(\alpha n) \in]a, b[$.
Donc $(\sin(n\alpha))_{n \in \mathbb{N}}$ est dense dans $] -1, 1[$. En particulier, cela vaut pour $\alpha = 1$ car $\pi \notin \mathbb{Q}$. Donc $(\sin(n))_{n \in \mathbb{N}}$ est dense dans $[-1, 1]$.
3. Soit $n \in \mathbb{N}$. 2^n commence par 7 en base 10 si et seulement s'il existe $p \in \mathbb{N}$ avec

$$\begin{aligned} 7 \times 10^p \leq 2^n < 8 \times 10^p &\iff \ln(7) + p \ln(10) \leq n \ln(2) < \ln(8) + p \ln(10) \\ &\iff \frac{\ln(7)}{\ln(10)} \leq \frac{n \ln(2)}{\ln(10)} - p < \frac{\ln(8)}{\ln(10)} \end{aligned}$$

On a alors

$$p = \left\lfloor \frac{n \ln(2)}{\ln(10)} \right\rfloor \in \mathbb{N}$$

On étudie donc $\mathbb{N} \frac{\ln(2)}{\ln(10)} + \mathbb{Z}$. Supposons que $\frac{\ln(2)}{\ln(10)} = \frac{p}{q} \in \mathbb{Q}$. Alors on a $2^q = 10^p$ mais comme $p \neq 0$, on a $5 \mid 10^p$ mais $5 \nmid 2^q$, donc $\frac{\ln(2)}{\ln(10)} \notin \mathbb{Q}$.

On sait que

$$u_n = n \frac{\ln(2)}{\ln(10)} - \left\lfloor \frac{n \ln(2)}{\ln(10)} \right\rfloor \in \left] \frac{\ln(7)}{\ln(10)}, \frac{\ln(8)}{\ln(10)} \right[$$

Par densité, on peut donc construire par récurrence $(u_{n_p})_{p \in \mathbb{N}}$ telle que

$$\frac{\ln(7)}{\ln(10)} < u_{n_{p+1}} < u_{n_p} < \frac{\ln(8)}{\ln(10)}$$

Donc on a bien une infinité de puissance de 2 commençant par 7 en base 10.

Remarque 1.10. $(e^{in\alpha})_{n \in \mathbb{N}}$ est de la même façon dense dans \mathbb{U} . On peut montrer qu'elle est équirépartie, c'est à dire que pour tout $a < b \in [0, 2\pi[$, on a

$$\lim_{N \rightarrow +\infty} \left| \left\{ n \in \{1, \dots, N\} \mid n\alpha - \frac{\lfloor 2\pi n\alpha \rfloor}{2\pi} \in]a, b[\right\} \right| \times \frac{1}{N} = \frac{b-a}{2\pi}$$

Remarque 1.11. Par équirépartition dans $[0, 1[$ des

$$\left\{ n \frac{\ln(2)}{\ln(10)} - \left\lfloor \frac{n \ln(2)}{\ln(10)} \right\rfloor \mid n \in \mathbb{N} \right\}$$

la probabilité pour qu'une puissance de 2 commence par k en base 10 est ($k \in \{1, \dots, 9\}$)

$$\frac{\ln(k+1) - \ln(k)}{\ln(10)} = \frac{\ln(1 + \frac{1}{k})}{\ln(10)}$$

Solution 1.30.

1. Pour $\alpha = a + ib$, on définit le module au carré : $|\alpha|^2 = a^2 + b^2$. Soit $\beta = c + id \neq 0$. Si $\alpha = \beta q + r$ avec $q, r \in \mathbb{Z}[i]^2$ et $|r|^2 < |\beta|^2$, alors $|\alpha - \beta q|^2 < |\beta|^2$ et $\beta \neq 0$ donc

$$\left| \underbrace{\frac{\alpha}{\beta}}_{\in \mathbb{C}} - \underbrace{q}_{\in \mathbb{Z}[i]} \right| < 1$$

On pose $\frac{\alpha}{\beta} = x + iy$. On pose

$$u_x = \begin{cases} \lfloor x \rfloor & \text{si } x \in [\lfloor x \rfloor, \lfloor x \rfloor + \frac{1}{2}[\\ \lfloor x \rfloor + 1 & \text{si } x \in [\lfloor x \rfloor + \frac{1}{2}, \lfloor x \rfloor + 1[\end{cases}$$

et de même pour u_y . On a alors $q = u_x + iu_y \in \mathbb{Z}[i]$ et

$$\left| \frac{\alpha}{\beta} - q \right|^2 = |x - u_x|^2 + |y - u_y|^2 \leq 2 \times \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1$$

On pose donc $r = \alpha - \beta q \in \mathbb{Z}[i]$ et ainsi l'anneau $\mathbb{Z}[i]$ est euclidien.

2. Soit A un anneau euclidien et I un idéal de A non réduit à $\{0\}$. Il existe $x \in I$ tel que

$$v(x_0) = \min\{v(x) \mid x \in I \setminus \{0\}\}$$

On a $x_0 A \subset I$. Soit $x \in I$. Il existe $q, r \in A$ tel que

$$x = x_0 q + r$$

avec $v(r) < v(x_0)$ ou $r = 0$. Or $r \in I$ donc $r = 0$. Ainsi $x \in x_0 A$ et donc $I = x_0 A$. Donc tout anneau euclidien est principal.

Remarque 1.12. C'est encore vrai avec $\mathbb{Z}[i\sqrt{2}] = \{a + ib\sqrt{2} \mid (a, b) \in \mathbb{Z}^2\}$.

Solution 1.31.

1. Si $\bar{x} = \bar{y}^2$ est un carré, d'après le petit théorème de Fermat, on a $\bar{x}^{\frac{p-1}{2}} = \bar{y}^{p-1} = \bar{1}$. Soit

$$\begin{aligned} f: \mathbb{Z}/p\mathbb{Z}^* &\rightarrow \mathbb{Z}/p\mathbb{Z}^* \\ \bar{y} &\mapsto \bar{y}^2 \end{aligned}$$

f est un morphisme multiplicatif, $\text{Im}(f)$ est un sous-groupe de $(\mathbb{Z}/p\mathbb{Z}^*, \times)$.

Comme \mathbb{F}_p est un corps, chaque carré possède exactement deux antécédents. Il y a $p-1$ antécédents, donc il y a $\frac{p-1}{2}$ carrés dans $\mathbb{Z}/p\mathbb{Z}^*$. Donc $|\text{Im}(f)| = \frac{p-1}{2}$ et si \bar{x} est un carré, x est racine de $X^{\frac{p-1}{2}} - \bar{1}$. Le polynôme $X^{\frac{p-1}{2}} - \bar{1}$ possède au plus $\frac{p-1}{2}$ racines et tout carré est racine. Donc les racines sont exactement les carrés et $\bar{x}^{\frac{p-1}{2}} = \bar{1}$ si et seulement si \bar{x} est un carré.

2. On a $p \equiv 1[4]$ si et seulement si $\frac{p-1}{2}$ est pair si et seulement si $(-1)^{\frac{p-1}{2}} = \bar{1}$ si et seulement si $\bar{-1}$ est un carré dans \mathbb{F}_p . Supposons qu'il y ait un nombre fini de nombres premiers p_1, \dots, p_r tous congrus à 1 modulo 4. On pose $n = (p_1 \times \dots \times p_r)^2 + 1$. Soit p un facteur premier de n , on a $n \equiv 1[n_i]$ donc $p \notin \{p_1, \dots, p_r\}$. Dans $\mathbb{Z}/p\mathbb{Z}$, on a $\bar{n} = \bar{0}$ donc $\bar{-1} = \overline{p_1 \times \dots \times p_r}^2$ donc $p \equiv 1[4]$ ce qui est une contradiction.

Donc il y a une infinité de nombres premiers congrus à 1 modulo 4.

Solution 1.32.

1. On pose $P_1 = \sum_{i=0}^n r'_i X^i$, et $\nu_p(r'_i)$ est positif par définition de $c(P)$. Donc $P_1 \in \mathbb{Z}[X]$.

Pour tout $p \in \mathcal{P}$, il existe $i_0 \in \{1, \dots, n\}$ tel que

$$\min_{i \in \{1, \dots, n\}} \nu_p(r_i) = \nu_p(r_{i_0})$$

et $\nu_p(r'_{i_0}) = 0$ donc $p \nmid r'_{i_0}$ donc

$$\bigwedge_{i=1}^n r'_i = 1$$

Si on a $P = \alpha_1 P_1 = \alpha_2 P_2$ avec les conditions requises, soit $p \in \mathcal{P}$, si $\nu_p(\alpha_2) > \nu_p(\alpha_1)$, alors p divise tous les coefficients de P_1 ce qui n'est pas possible, donc $\nu_p(\alpha_2) = \nu_p(\alpha_1)$.

Ceci étant vrai pour tout $p \in \mathcal{P}$, on a aussi $\alpha_1 = \alpha_2$ et donc $P_1 = P_2$.

2. On a $P = c(P)P_1$ et $Q = c(Q)Q_1$ donc $PQ = c(P)c(Q)P_1Q_1$ et $P_1Q_1 \in \mathbb{Z}[X]$.

Soit $p \in \mathcal{P}$ divisant tous les coefficients de P_1Q_1 . On définit, si $R = \sum_{i \in \mathbb{N}} \gamma_i X^i \in \mathbb{Z}[X]$, $\bar{R} = \sum_{i \in \mathbb{N}} \bar{\gamma}_i X^i \in \mathbb{Z}/p\mathbb{Z}[X]$. $R \mapsto \bar{R}$ est un morphisme d'anneaux. Par hypothèse, on a $\overline{P_1Q_1} = \bar{0} = \overline{P_1} \overline{Q_1}$ et par intégrité de $\mathbb{Z}/p\mathbb{Z}[X]$, on a $\overline{P_1} = \bar{0}$ ou bien $\overline{Q_1} = \bar{0}$, ce qui est exclu par les hypothèses. Donc $c(PQ) = c(P)c(Q)$.

3. Soit alors P irréductible dans $\mathbb{Z}[X]$ (les inversibles de $\mathbb{Z}[X]$ étant -1 et 1). Posons

$$\begin{aligned} P &= QR \in \mathbb{Q}[X]^2 \\ &= c(Q)c(R) \underbrace{Q_1 R_1}_{\in \mathbb{Z}[X]} \end{aligned}$$

OR $c(Q)c(R) = c(P)$ c'après le lemme de Gauss et nécessairement, $c(P) = 1$. Donc $P = Q_1 R_1$, et alors $Q_1 = \pm 1$ et $R_1 = \pm 1$, et Q ou R est constant, donc P est irréductible sur $\mathbb{Q}[X]$.

Pour la réciproque, on a $2X$ est irréductible sur $\mathbb{Q}[X]$ car de degré 1, mais pas sur $\mathbb{Z}[X]$ car ni 2 ni X ne sont inversibles.

4. Soit $\theta = \frac{2\pi p}{q}$ avec $p \wedge q = 1$ et $\cos(\theta) \in \mathbb{Q}$. Sur $\mathbb{C}[X]$, on a $P = (X - e^{i\theta})(X - e^{-i\theta}) = X^2 - 2\cos(\theta)X + 1 \in \mathbb{Q}[X]$.

Et $e^{i\theta} \neq e^{-i\theta}$ car $\theta \not\equiv 0[\pi]$. On a $\theta = \frac{2\pi p}{q}$ donc $e^{i\theta} \in \mathbb{U}_q$, et $e^{i\theta}$ et $e^{-i\theta}$ sont des racines de A . Donc, dans $\mathbb{C}[X]$, on a $P \mid A$ et $A \in \mathbb{Q}[X]$, donc il existe $B \in \mathbb{Q}[X]$ tel que

$$\underbrace{A}_{\in \mathbb{Q}[X]} = \underbrace{B}_{\in \mathbb{C}[X]} \times \underbrace{P}_{\in \mathbb{Q}[X]}$$

Or B s'obtient par la division euclidienne de A par P , qui est indépendante du corps de référence, il vient $B \in \mathbb{Q}[X]$ et donc $A \mid P$ dans $\mathbb{Q}[X]$.

On a $c(A) = 1 = c(B)c(P)$ et $A = c(B)c(P)B_1P_1 = B_1P_1 \in \mathbb{Z}[X]$ et le coefficient dominant de A est donc 1. Donc le coefficient dominant de B_1 et de P_1 est aussi 1. En reportant, on a $P = P_1 \in \mathbb{Z}[X]$.

Donc $2 \cos(\theta) \in \mathbb{Z} \cap [-2, 2]$ donc $\cos\{\theta\} \in \{-\frac{1}{2}, \frac{1}{2}, 0\}$ (-1 et 1 ne peuvent y être car on a supposé $\theta \neq 0[\pi]$). Les solutions sont donc

$$\theta \in \left\{0, \frac{\pi}{3}, \frac{\pi}{2}, \frac{2\pi}{3}, \pi, \frac{4\pi}{3}, \frac{3\pi}{2}, \frac{5\pi}{3}\right\}$$

(en rajoutant $\theta = 0$ et π).

Remarque 1.13. On a $\frac{\arccos(\frac{1}{3})}{\pi} \notin \mathbb{Q}$ car $\cos(\theta) = \frac{1}{3}$ n'est pas dans l'ensemble solutions.

Solution 1.33.

1. Soit $P = a \prod_{i=1}^s (X - a_i)^{\alpha_i}$ avec les a_i distincts et $\alpha_i \geq 1$. a_i est racine de P' de multiplicité $\alpha_i - 1$. Il manque donc s racines. Si $\alpha = 0$, le résultat est évident, sinon on pose

$$\begin{aligned} f : \mathbb{R} &\rightarrow \mathbb{R} \\ x &\mapsto P(x)e^{\frac{x}{\alpha}} \end{aligned}$$

et on a pour tout $x \in \mathbb{R}$,

$$f'(x) = \frac{e^{\frac{x}{\alpha}}}{\alpha} (P(x) + \alpha P'(x))$$

Comme P est scindé sur \mathbb{R} , P' est scindé sur \mathbb{R} (appliquer le théorème de Rolle entre les racines distinctes de P), donc f' s'annule $s - 1$ fois entre les racines de P donc $P + \alpha P'$ aussi.

La dernière racine est réelle car sinon, le conjugué de la racine complexe supposée serait aussi racine.

2. On pose $R = \mu \prod_{i=0}^r (X - \beta_i)$. On pose

$$\begin{aligned} \Delta : \mathbb{R}[X] &\rightarrow \mathbb{R}[X] \\ P &\mapsto P' \end{aligned}$$

On a alors

$$\sum_{i=0}^r a_i P^{(i)} = \sum_{i=0}^r a_i \Delta^i(P) = R(\Delta)(P) = \mu \prod_{i=0}^r (\Delta - \beta_i \text{id})(P)$$

Par récurrence sur r , on montre que $\prod_{i=0}^r (\Delta - \beta_i \text{id})(P)$ est scindé d'après la première question.

Remarque 1.14. On a aussi pour tout $\lambda \in \mathbb{R}$, $P' + \lambda P$ est aussi scindé sur \mathbb{R} si P est scindé sur \mathbb{R} .

Solution 1.34. Soit $F = \frac{P'}{P}$ définie sur $\mathbb{R} \setminus \{a_1, \dots, a_n\}$ où a_i sont les racines de P . On note α le coefficient dominant de P , et on a

$$P' = \alpha \sum_{i=1}^n \left(\prod_{\substack{j=1 \\ j \neq i}}^n (X - a_j) \right)$$

On a donc $F = \sum_{i=1}^n \frac{1}{X - a_i}$ et on a

$$F' = - \sum_{i=1}^n \frac{1}{(X - a_i)^2} = \frac{P''P - P'P'}{P^2}$$

Pour $x \notin \{a_1, \dots, a_n\}$, on a

$$\begin{aligned} (n-1)(P'^2(x))(x) &\geq nP(x)P''(x) \iff n(P''(x)P(x) - P'^2(x)) \leq -P'^2(x) \\ &\iff \frac{P'^2(x)}{P^2(x)} \leq n(P''(x)P(x) - P'^2(x)) \times \frac{1}{P^2(x)} \\ &\iff F^2(x) \leq n(-F'(x)) \\ &\iff \left(\sum_{i=1}^n \frac{1}{(X - a_i)} \right)^2 \leq n \times \sum_{i=1}^n \frac{1}{(X - a_i)^2} \end{aligned}$$

qui est l'inégalité de Cauchy-Schwarz dans \mathbb{R}^2 avec $(1 \dots 1)$ et $(\frac{1}{x-a_1} \dots \frac{1}{x-a_n})$.

Remarque 1.15. Si $P = \alpha(X - a_1)^{m_1}(X - a_r)^{m_r}$, alors

$$\frac{P'}{P} = \sum_{i=1}^r \frac{m_i}{X - a_i}$$

Solution 1.35.

1. $P' \in \mathbb{C}[X]$ et $\deg(P') = \deg(P) - 1$. On a $P \wedge P' = 1$ car P est irréductible sur $\mathbb{Q}[X]$.

Comme le pgcd est obtenu par l'algorithme d'Euclide qui est indépendant du corps de référence, on a $P \wedge P' = 1$ sur $\mathbb{C}[X]$ donc P n'a que des racines simples sur \mathbb{C} .

2. Notons $P \in \mathbb{Q}[X]$ le polynôme minimal de α sur \mathbb{Q} (défini car $A(\alpha) = 0$ donc α est algébrique). Comme $A(\alpha) = 0$, on a $P \mid A$ et P est irréductible sur $\mathbb{Q}[X]$. Si $\alpha \notin \mathbb{Q}$, on a $\deg(P) \geq 2$, on peut donc décomposer sur $\mathbb{Q}[X]$:

$$A = P^r \times P_1^{r_1} \times \dots \times P_s^{r_s}$$

avec les P_i irréductibles sur $\mathbb{Q}[X]$ non associés.

α n'est pas racine d'un P_i car sinon $P \mid P_i$ ce qui est impossible. α est racine simple de P donc $m(\alpha) = r > \frac{\deg(A)}{2}$. Par ailleurs, $\deg(P)^r \geq 2r > \deg(A)$ ce qui est impossible.

Donc $\alpha \in \mathbb{Q}$.

Solution 1.36. Soit $x \in A$. Il existe $(n, m) \in \mathbb{N}^2$ avec $n < m$ tel que $x^n = x^m$. Alors $x^{m-n} = e_G \in A$.

$$\begin{aligned} f: \mathbb{N}^* &\rightarrow A \\ n &\mapsto x^n \end{aligned}$$

n'est pas injective, car \mathbb{N}^* est infini et A est fini. Or $m - n \in \mathbb{N}^*$ donc

$$x^{m-n} = e_G \Rightarrow x = x \cdot x^{m-n-1} = e_G$$

donc $x^{-1} = x^{m-n-1} \in A$ et ainsi A est un sous-groupe.

Solution 1.37. Pour $\alpha = 0$, on a $1 + p \equiv 1 + p[p^2]$. Pour $\alpha = 1$, on a

$$(1 + p)^p = \sum_{k=0}^p \binom{p}{k} p^k = 1 + p^2 + \binom{p}{2} p^2 \sum_{k=3}^p \binom{p}{k} p^k$$

Or $\binom{p}{2} p^2 = \frac{p(p-1)p^2}{2} \equiv 0[p^3]$ car p est premier plus grand que trois donc impair, et la somme est aussi congrue à 0 modulo p^3 .

Soit $\alpha \geq 1$, supposons que l'on ait

$$(1 + p)^p \equiv 1 + p^{\alpha+1}[p^{\alpha+2}]$$

Il existe $l \in \mathbb{N}$ tel que

$$(1 + p)^{p^\alpha} = 1 + p^{\alpha+1} + lp^{\alpha+2}$$

Alors

$$(1 + p)^{p^{\alpha+1}} = (1 + \underbrace{p^{\alpha+1} + lp^{\alpha+2}}_x)^p$$

Or

$$(1+x)^p = \sum_{k=0}^p \binom{p}{k} x^k = 1 + px + \sum_{k=2}^p \binom{p}{k} x^k = 1 + p^{\alpha+2} + lp^{\alpha+3} + \underbrace{\sum_{k=2}^p \binom{p}{k} x^k}_{\text{divisible par } x^2}$$

Comme $p^{\alpha+1} \mid x$, $p^{2\alpha+2} \mid x^2$ avec $2\alpha+2 \geq \alpha+3$ ($\alpha \geq 1$). D'où

$$p^{\alpha+3} \mid x^2 \mid \sum_{k=2}^p \binom{p}{k} x^k$$

et

$$(1+p)^{p^{\alpha+1}} \equiv 1 + p^{\alpha+2}[p^{\alpha+3}]$$

Remarque 1.16. Pour $p=2, \alpha=1$, on a $3^2 = 9 \not\equiv 5[8]$.

Solution 1.38. Si $7 = 2x^2 - 5y^2$, on a $\bar{0} = 2\bar{x}^2 - 5\bar{y}^2 = \bar{2}(\bar{x}^2 + \bar{y}^2)$ dans $\mathbb{Z}/7\mathbb{Z}$. Comme 2 et 7 sont premiers entre eux donc $\bar{2}$ est inversible. Donc $\bar{x}^2 + \bar{y}^2 = \bar{0}$. La seule possibilité est $\bar{x} = \bar{0}$ et $\bar{y} = \bar{0}$. Donc $7 \mid x$ et $7 \mid y$. Si $x = 7k$ alors $x^2 = 49k^2$ donc $49 \mid x^2$ et $49 \mid y^2$ donc $49 \mid 2x^2 - 5y^2 = 7$ ce qui est faux.

Solution 1.39. \mathbb{F}_{19} est un corps car 19 est premier. On a donc $\bar{x}^3 = \bar{1}$ si et seulement si $(x - \bar{1})(x^2 + x - \bar{1}) = \bar{0}$. On a donc $x = \bar{1}$ ou $x^2 + x + \bar{1} = \bar{0}$. On a

$$x^2 + x + \bar{1} = (x + \bar{2}^{-1})^2 + \bar{3} \times \bar{4}^{-1} = (x + \bar{10})^2 + \bar{3} \times \bar{50}$$

Donc $(x + \bar{10})^2 = \bar{4}$ d'où $x = \bar{-8} = \bar{11}$ ou $x = \bar{-12} = \bar{7}$.

Solution 1.40.

1. m est inversible si et seulement si $m \wedge 2^n = 1$ si et seulement si $m \wedge 2 = 1$ si et seulement si m est impair. IL y a donc 2^{n-1} inversibles.
2. On a $5^{2^{3-3}} = 5 \equiv 1 + 2^2[2^3]$. Par récurrence, soit $n \geq 3$. Il existe $k \in \mathbb{Z}$ avec $5^{2^{n-3}} = 1 + 2^{n-1} + k2^n$ donc

$$5^{2^{n-1}} = 1 + 2^n + k2^{n+1} + 2^{2n-2}(1 + 2k)^2 \equiv 1 + 2^n[2^{n+1}]$$

car $2n - 2 \geq n + 1$ ($n \geq 3$).

3. On a $5^{2^{n-2}} \equiv 1 + 2^n[2^{n+1}] \equiv 1[2^n]$ et $5^{2^{n-3}} \not\equiv 1[2^n]$. Donc l'ordre de $\bar{5}$ est 2^{n-2} .

4. $\text{gr}\{\overline{-1}\} = \{\overline{-1}, \overline{1}\}$. $\bar{5}$ n'engendre pas $\overline{-1}$ car si $\bar{5}^k = \overline{-1}$, on a $\bar{5}^{2k} = \overline{1}$ d'où $2^{n-2} \mid 2k$ donc $2^{n-3} \mid k$. Ainsi, $k \in \{2^{n-3}, 2^{n-2}, 2^{n-1}\}$. Mais $\bar{5}^{2^{n-2}} = \overline{1}$, $\bar{5}^{2^{n-3}} = \overline{1+2^{n-1}} \neq \overline{-1}$ donc un tel k n'existe pas.

Posons

$$\begin{aligned} \varphi : \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}, + \right) &\rightarrow \left(\mathbb{Z}/2^n\mathbb{Z}^\times, \times \right) \\ (\tilde{a}, \tilde{b}) &\mapsto \overline{-1^a 5^b} \end{aligned}$$

Elle est bien définie car $\omega(\overline{-1}) = 2$ et $\omega(\bar{5}) = 2^{n-2}$. C'est évidemment un morphisme, on a égalité des cardinaux des ensembles de départ et d'arrivée, et on vérifie qu'elle est injective, et donc c'est un isomorphisme.

Solution 1.41. Soit $(x, x') \in G^2$ tel que $x \cdot x' = e$. Alors

$$e \cdot x = x \cdot x' \cdot x = x \cdot e \cdot x' \cdot x$$

si et seulement si

$$e \cdot x \cdot x' = e = x \cdot e \cdot x' \cdot x \cdot x' = x \cdot e \cdot x'$$

Soit $(x, x', x'') \in G^3$ tel que $x \cdot x' = e$ et $x' \cdot x'' = e$. On a alors

$$x \cdot x' \cdot x'' = x \cdot e = x = e \cdot x''$$

Donc $x = e \cdot x''$ et $e = e \cdot x'' \cdot x'$. Si on prouve que $e \cdot x'' = x''$, alors $x = x''$ et $x' \cdot x = e$.

Montrons donc que pour tout $x \in G$, $e \cdot x = x$. Notons que s'il existe $e' \in G$ tel que pour tout $x \in G$, $e' \cdot x = x$, alors $e' \cdot e = e' = e$. Il vient donc

$$x' \cdot x = x' \cdot e \cdot x'' = x' \cdot x'' = e$$

Donc pour tout $x \in G$, l'élément x' est inverse à droite et à gauche : $x \cdot x' = e$.

Donc

$$x \cdot x' \cdot x = e \cdot x = x \cdot x' \cdot x = x \cdot e = x$$

Et donc e est neutre à gauche. Finalement, (G, \cdot) est un groupe.

Remarque 1.17. Si $f: \mathbb{R} \rightarrow \mathbb{R}$ est surjective, on peut définir

$$\begin{aligned} g: \mathbb{R} &\rightarrow \mathbb{R} \\ y &\mapsto f(x) \end{aligned}$$

pour un certain $x \in \mathbb{R}$. On a $f \circ g = id$. Si f n'est pas injective : s'il existait $h: \mathbb{R} \rightarrow \mathbb{R}$ telle que $h \circ f = id$, soit $(x, x') \in \mathbb{R}^2$ telle que $f(x) = f(x')$. En composant par h , on aurait $x = x'$ donc f serait injective ce qui n'est pas.

On on peut avoir un inverse à droite mais pas à gauche.

Solution 1.42. Soit $n \in \mathbb{N}^*$.

$$\underbrace{1 \dots 1}_{n \text{ fois en base } 10} = 1 + 10 + \dots + 10^{n-1} = \frac{10^n - 1}{9}$$

On a

$$\begin{aligned} 21 \mid \frac{10^n - 1}{9} &\iff 3 \mid \frac{10^n - 1}{9} \text{ et } 7 \mid \frac{10^n - 1}{9} \\ &\iff 27 \mid 10^n - 1 \text{ et } 7 \mid 10^n - 1 \end{aligned}$$

car $7 \wedge 9 = 1$. Dans $\mathbb{Z}/7\mathbb{Z}$, on a $\overline{10} = \overline{3}$ donc pour tout $k \in \mathbb{N}$, $\overline{10}^{6k} = \overline{1}$ d'après le petit théorème de Fermat. Dans $\mathbb{Z}/27\mathbb{Z}$, $\tilde{10}$ est inversible car $10 \wedge 27 = 1$. $((\mathbb{Z}/27\mathbb{Z})^\times, +, \times)$ comporte 18 éléments donc pour tout $k' \in \mathbb{N}$, on a $\tilde{10}^{18k'} = \tilde{1}$.

Lorsque $81 \mid n$, on a $21 \mid 1 \dots 1$.

Cherchons plus précisément les ordres de $\overline{10}$ dans $((\mathbb{Z}/7\mathbb{Z})^*, \times)$ et de $\tilde{10}$ dans $((\mathbb{Z}/27\mathbb{Z})^\times, \times)$. Dans $(\mathbb{Z}/7\mathbb{Z})^*$, groupe de cardinal 6, on vérifie que l'ordre de 10 est 6. Dans l'autre groupe, on vérifie que l'ordre de $\tilde{10}$ est 3. Ainsi, $21 \mid 1 \dots 1$ si et seulement si $6 \mid n$.

Il y a donc une infinité de multiples de 21 qui s'écrivent avec uniquement des 1 en base 10.

Remarque 1.18. Il suffit de trouver l'ordre de 10 dans les deux ensembles et de prendre le ppcm.

Solution 1.43.

1. $X^d - 1$ a au plus d racines dans \mathbb{K} . Pour tout $k \in \{0, \dots, d-1\}$, x_0^k est racine de $X^d - 1_{\mathbb{K}}$ car $gr\{x_0\}$ a pour cardinal d . Donc les racines sont exactement les puissances de x_0 .

Soit $x \in \mathbb{K}^*$ d'ordre d . On a $x \in \text{gr}\{x_0\}$ car $x^d = 1$ (racine du polynôme de $X^d = 1_{\mathbb{K}}$).

Or, dans le groupe cyclique engendré par x_0 , il y a $\varphi(d)$ éléments.

2. On a ou bien $\varphi(d)$ ou bien aucun élément d'ordre d dans \mathbb{K} . Soit d tel que $d \mid n$, on note $H_d = \{x \in K \mid \omega(x) = d\}$. On a

$$\mathbb{K}^* = \bigcup_{d \mid n} H_d$$

Alors

$$n = \sum_{d \mid n} |H_d| \leq \sum_{d \mid n} \varphi(d) = n$$

Alors pour tout d tel que $d \mid n$, on a $|H_d| = \varphi(d)$. En particulier, on a $|H_n| = \varphi(n) \geq 1$ donc H_n est non vide. Donc il existe (au moins) un élément d'ordre n , on (\mathbb{K}^*, \times) est cyclique.

Solution 1.44.

1. Soit $x \in M$. On a $\bar{1} - \bar{x}^{-1}$ si et seulement si $\bar{x} = \bar{1}$ et $\bar{1} - \bar{x}^{-1} = \bar{1}$ si et seulement si $\bar{x} = \bar{0}$, ce qui n'est pas possible pour les deux cas. Donc f est bien définie.

Soit $x \in M$, on a

$$\begin{aligned} f^2(x) &= f(\bar{1} - \bar{x}^{-1}) \\ &= \bar{1} - (\bar{1} - \bar{x}^{-1})^{-1} \\ &= (\bar{1} - \bar{x}^{-1})^{-1}(\bar{1} - \bar{x}^{-1} - \bar{1}) \\ &= -\bar{x}^{-1}(\bar{1} - \bar{x}^{-1})^{-1} \end{aligned}$$

Donc

$$\begin{aligned} f^3(x) &= \bar{1} - (\bar{1} - (\bar{1} - \bar{x}^{-1})^{-1})^{-1} \\ &= \bar{1} - (-x\bar{x}^{-1}(\bar{1} - \bar{x}^{-1})^{-1})^{-1} \\ &= \bar{1} + \bar{x}(\bar{1} - \bar{x}^{-1}) \\ &= \bar{1} + \bar{x} - \bar{1} \\ &= \bar{x} \end{aligned}$$

Donc $f^3 = \text{id}_M$.

2. Soit $x \in M$, on a

$$\begin{aligned}
 f(x) = x &\iff \bar{1} - \bar{x}^{-1} = x \\
 &\iff \bar{x}^2 - \bar{x} + \bar{1} = \bar{0} \\
 &\iff (\bar{x} - \bar{2}^{-1})^2 + \bar{3} \times \bar{4}^{-1} = \bar{0} \\
 &\iff \bar{-3} = (\bar{2}\bar{x} - \bar{1})^2
 \end{aligned}$$

f admet un point fixe si et seulement $\bar{-3}$ est un carré dans $\mathbb{Z}/p\mathbb{Z}$ car $\bar{y} = \bar{2}\bar{x} - \bar{1}$ si et seulement si $\bar{x} = \bar{2}^{-1}(\bar{y} + \bar{1})$.

3. Comme p est premier plus grand que 5, on a $p \equiv 1$ ou $2[3]$ donc $p - 2 \equiv 0$ ou $2[3]$ car $f^3 = \text{id}_M$, les longueurs des cycles qui composent f valent 1 ou 3.

Si f n'a pas de point fixe, tous les cycles sont de longueur 3, donc $3 \mid p - 2$ donc $p \equiv 2[3]$.

Si $p \equiv 2[3]$, alors $3 \mid p - 2$, le nombre de points fixes est un multiple de 3 donc aussi du nombre de racine carrés de $\bar{-3}$. Et puisque l'on est dans un corps, il y a au plus 2 racines de $\bar{-3}$. Donc si $p \equiv 2[3]$, il n'y a pas de point fixe.

Solution 1.45. Soit $x \in \mathbb{R}$. Supposons que x possède un développement décimal périodique. Alors il existe $(n_0, T) \in \mathbb{N} \times \mathbb{N}^*$ tels que pour tout $n \geq n_0$, $a_{n+T} = a_n$. On a alors

$$\begin{aligned}
 |x| &= \underbrace{b_m \dots b_0, a_0 \dots a_{n_0-1}}_{\in \mathbb{Q}} + \frac{1}{10^{n_0-1}} \underbrace{(0, a_{n_0} \dots a_{n_0+T-1} a_{n_0} \dots)}_{=y} \\
 10^T y - y &= a_{n_0} \dots a_{n_0+T-1} \in \mathbb{N}
 \end{aligned}$$

et donc

$$y = \frac{a_{n_0} \dots a_{n_0+T-1}}{10^T - 1} \in \mathbb{Q}$$

Donc $x \in \mathbb{Q}$.

Réciproquement, soit $x = \frac{p}{q} \in \mathbb{Q}$ avec $q \in \mathbb{N}^*$. Il existe $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$ tel que $p = aq + b$ avec $b \in \{0, \dots, q-1\}$. Si $b = 0$, on arrête. On a sinon

$$x = a + \frac{1}{10^k} \frac{10^k b}{q}$$

où $k = \min\{m \geq 1 \mid 10^m b > q\}$. On réitère l'algorithme avec $\frac{10^k b}{q}$ car on a $\left\lfloor \frac{10^k b}{q} \right\rfloor \in \{1, \dots, 9\}$ par définition de k .

Il y a q restes possibles dans la division euclidienne par q . Ainsi, au bout d'au plus de $q + 1$ itérations, on retrouve un reste précédent. Par unicité de la division euclidienne, on obtient un développement décimal périodique.

Remarque 1.19. On peut écrire $q = 2^a 5^b q'$ avec $q' \wedge 2 = q' \wedge 5 = 1$. On se ramène alors à $q \wedge 2 = q \wedge 5 = 1$. En reportant dans l'écriture décimale de x , on a

$$\frac{\alpha}{q} = \frac{\beta}{10^T - 1}$$

avec $\alpha \wedge q = 1$. On a donc $q \mid 10^T - 1$ d'après le lemme de Gauss. T revient donc à l'ordre de $\overline{10}$ dans $(\mathbb{Z}/q\mathbb{Z}^\times, \times)$ qui contient $\varphi(q)$ éléments. Par défaut, on a donc $T = \varphi(q)$.

Solution 1.46.

1. Soit $m \in \mathbb{Z}$. Si $m \in \{0, \dots, n-1\}$, on a $H_n(m) = 0 \in \mathbb{Z}$. Si $m \geq n$, on a $H_n(m) = \binom{m}{n} \in \mathbb{Z}$. Si $m < 0$, on a

$$H_n(m) = \frac{m(m-1) \dots (m-n+1)}{n!} = (-1)^n \binom{-m+n-1}{-m-1} \in \mathbb{Z}$$

Donc $H_n(\mathbb{Z}) \subset \mathbb{Z}$.

2. Supposons qu'il existe $n \in \mathbb{N}$ et $(a_0, \dots, a_n) \in \mathbb{Z}^{n+1}$ et $P = \sum_{k=0}^n a_k H_k$. On a $H_k(\mathbb{Z}) \subset \mathbb{Z}$ donc $P(\mathbb{Z}) \subset \mathbb{Z}$. Supposons $P(\mathbb{Z}) \subset \mathbb{Z}$. $(H_k)_{k \in \mathbb{N}}$ est une base étagée en degré de $\mathbb{C}[X]$. Donc il existe $(a_0, \dots, a_n) \in \mathbb{C}^{n+1}$ tel que $P = \sum_{k=0}^n a_k H_k$. Par récurrence, on a $P(0) = a_0 \in \mathbb{Z}$. Soit $k \in \{0, n-1\}$, supposons $(a_0, \dots, a_k) \in \mathbb{Z}^{k+1}$. On a alors

$$P(k+1) = \underbrace{\sum_{i=0}^k \underbrace{a_i}_{\in \mathbb{Z}} H_i}_{\in \mathbb{Z}} + a_{k+1} \underbrace{H_{k+1}(k+1)}_{=1}$$

Donc $a_{k+1} \in \mathbb{Z}$.

Remarque 1.20. Les translation $X + \alpha$ sont les seules pour lesquelles on a $(X + \alpha)(\mathbb{Z}) = \mathbb{Z}$. En effet, si $P \in \mathbb{C}[X]$ est tel que $P(\mathbb{Z}) = \mathbb{Z}$, on a $P \in \mathbb{Q}[X]$ d'après ce qui précède. Si $\deg(P) \geq 2$, quitte à remplacer P par $-P$, on peut supposer le coefficient dominant de P strictement positif. On a alors $\lim_{x \rightarrow +\infty} P'(x) = +\infty$ donc il existe $A > 0$ tel que P est strictement croissant sur $[A, +\infty[$. De plus, $P(x+1) - P(x) \rightarrow +\infty$ quand $x \rightarrow +\infty$. Donc il existe $A' > 0$ tel que $P(x+1) > P(x) + 1$. Pour $n \geq \max(A, A')$, on a $P(n+1) \geq P(n) + 2$ ce qui contredit $P(\mathbb{Z}) = \mathbb{Z}$. Donc le degré de P est inférieur à 1.

Solution 1.47. Le coefficient en X^k s'écrit $a_{k-1} - \alpha a_k \in \mathbb{Q}$. Si $a_k \in \mathbb{Q}$, on a donc $a_{k-1} \in \mathbb{Q}$. Il est donc impossible d'avoir deux coefficients consécutifs rationnels. Or $x_{n-1} \in \mathbb{Q}$ car c'est le coefficient dominant de P . Donc α est nécessairement racine simple.

Solution 1.48. Soit $\Delta = P \wedge P' = \Delta$. On a $\deg(\Delta) \in \{1, 2, 3, 4\}$ car $\Delta \mid P'$.

Si $\deg(\Delta) = 4$, alors $\Delta = P'$ (car associé). Donc il existe $\beta \in \mathbb{C}$ d'où $\underbrace{P}_{\in \mathbb{Q}[X]} = (X - \beta) \underbrace{P'}_{\in \mathbb{Q}[X]}$.

Par division euclidienne, $X - \beta \in \mathbb{Q}[X]$ et $\beta \in \mathbb{Q}$ d'après l'algorithme de la division euclidienne.

Si $\deg(\Delta) = 1$, on a $P = X - \beta$ avec $\beta \in \mathbb{Q}$ racine de P .

Si $\deg(\Delta) = 2$, si $\Delta = (X - \beta)^2$, on a $\Delta' = 2(X - \beta) \in \mathbb{Q}[X]$ donc $\beta \in \mathbb{Q}$ racine de Δ donc de P . Si $\Delta = (X - \alpha_1)(X - \alpha_2)$ avec $\alpha_1 \neq \alpha_2$. α_1 et α_2 sont racines doubles de P donc $P = (X - \beta) \underbrace{(X - \alpha_1)^2(X - \alpha_2)^2}_{=\Delta^2 \in \mathbb{Q}[X]}$ Par division euclidienne, $X - \beta \in \mathbb{Q}[X]$ et donc $\beta \in \mathbb{Q}$.

Si $\deg(\Delta) = 3$, si $\Delta = (X - \beta)^3$, on a $\Delta^{(2)} = 6(X - \beta) \in \mathbb{Q}[X]$ donc $\beta \in \mathbb{Q}$. Si $\Delta = (X - \alpha_1)(X - \alpha_2)(X - \alpha_3)$ avec α_1, α_2 et α_3 distinctes. α_1, α_2 et α_3 seraient racines doubles de P ce qui contredit $\deg(P) = 5$. Si $\Delta = (X - \alpha)^2(X - \beta)$, α est racine triple de P et β racine double de P donc $P = (X - \alpha)^3(X - \beta)^2 \in \mathbb{Q}[X]$. Par division euclidienne, $(X - \alpha)(X - \beta) \in \mathbb{Q}[X]$ et

$$X - \alpha = \frac{\Delta}{(X - \alpha)(X - \beta)} \in \mathbb{Q}[X]$$

donc $\alpha \in \mathbb{Q}$.

Solution 1.49.

1. $1 \in \mathbb{Z}[i], 0 \in \mathbb{Z}[i], i \in \mathbb{Z}[i]$. Soit $(a, b, a', b') \in \mathbb{Z}^4$:

$$\begin{cases} (a + ib) - (a' + ib') = (a - a') + i(b - b') \in \mathbb{Z}[i] \\ (a + ib) \times (aa' - bb') + i(ab' + ba') \in \mathbb{Z}[i] \end{cases}$$

Donc $\mathbb{Z}[i]$ est un sous-anneau de \mathbb{C} contenant i .

Soit A un sous anneau de \mathbb{C} contenant i . A est stable par x donc $i^4 = 1 \in A$. A est stable par $+$ donc $\mathbb{Z} \subset A$, puis $i\mathbb{Z} \subset A$ donc $\mathbb{Z}[i] \subset A$. $\mathbb{Z}[i]$ est donc le plus petit sous anneau de \mathbb{C} contenant i .

2. Si $|z|^2 = 1$ c'est-à-dire $a^2 + b^2 = 1$, alors

$$\frac{1}{z} = \frac{a - ib}{|z|^2} = a - ib \in \mathbb{Z}[i]$$

Si z est inversible dans $\mathbb{Z}[i]$, il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$ donc $|z|^2|z'|^2 = 1$ donc $|z|^2 = 1$.

Soit $(a, b) \in \mathbb{Z}^2$. Si $|a| \geq 2$ ou $|b| \geq 2$, alors $a^2 + b^2 \geq 4$ donc si $|z|^2 = 1$, alors $a^2 + b^2 = 1$ et $(|a| = 1 \text{ et } |b| = 0)$ ou $(|a| = 0 \text{ et } |b| = 1)$. Donc

$$U = \{1, -1, i, -i\}$$

3. (a) Si $x \in \mathbb{R}$, il existe $n \in \mathbb{Z}$ tel que $|x - n| \leq \frac{1}{2}$ (faire un dessin et le montrer grâce aux parties entières). Soit alors $z_0 = x_0 + iy_0 \in \mathbb{C}$, on prend un $(a, b) \in \mathbb{Z}^2$ tel que $|x_0 - a| \leq \frac{1}{2}$, $|y_0 - b| \leq \frac{1}{2}$. Et pour $z = a + ib \in \mathbb{Z}[i]$, on a $|z - z_0|^2 = (x_0 - a)^2 + (y_0 - b)^2 \leq \frac{1}{2}$.

(b) Soit $(q, r) \in \mathbb{Z}[i]^2$, on a $z_1 = qz_2 + r$ si et seulement si $\frac{z_1}{z_2} - q = \frac{r}{z_2}$. On a $|r| < |z_1|$ si et seulement si $|\frac{z_1}{z_2} - q| < 1$. On a $\frac{z_1}{z_2} \in \mathbb{C}$ donc d'après 3.(a), il existe $q \in \mathbb{Z}[i]$ tel que $|\frac{z_1}{z_2} - q| \leq \frac{\sqrt{2}}{2} < 1$. On pose alors $r = z_1 - qz_2 \in \mathbb{Z}[i]$ par stabilité. Il vient donc $|r| < |z_2|$

Il n'y a pas unicité : par exemple $z_2 = 1$ et $z_1 = \frac{1+i}{2}$. On peut prendre $q \in \{0, 1, i, 1+i\}$.

(c) Soit $I \neq \{0\}$ un idéal de $\mathbb{Z}[i]$. On note $n_0 = \min\{|z|^2 \mid z \in I \setminus \{0\}\}$ (partie non vide de \mathbb{N}^*). Soit $z_0 \in I \setminus \{0\}$ tel que $|z_0|^2 = n_0$. On a directement $z_0\mathbb{Z}[i] \subset I$ (I est un idéal).

Réciproquement, soit $z \in I$, d'après 3.(b), il existe $(q, r) \in \mathbb{Z}[i]^2$ tel que

$$r = \underbrace{z}_{\in I} - \underbrace{z_0}_{\in I} \underbrace{q}_{\in \mathbb{Z}[i]} \in I$$

et $|r|^2 < n_0$. Nécessairement, $r = 0$ et $z = z_0q \in z_0\mathbb{Z}[i]$. Donc $I = z_0\mathbb{Z}[i]$. Finalement, $\mathbb{Z}[i]$ est principal.

4. Si $|z|^2 = 1$, alors $z \in U$ donc c'est bon. On travaille ensuite par récurrence sur $n \in \mathbb{N}^*$. Supposons que la décomposition existe pour $z \in \mathbb{Z}[i]$ avec $|z|^2 \leq n$. Soit $z \in \mathbb{Z}[i]$ tel que $|z|^2 = n + 1$. On a $|z|^2 \geq 2$ donc $z \in U$. Si z est irréductible, c'est bon. Sinon, il existe

$(z_1, z_2) \in \mathbb{Z}[i]^2$ tel que $z = z_1 z_2$ et z_1 et z_2 non inversibles. Alors $|z_1|^2 \geq 2$ et $|z_2|^2 \geq 2$. Or $|z|^2 = n + 1 = |z_1|^2 |z_2|^2$ donc $|z_1|^2 \leq n$ et $|z_2|^2 \leq n$. Par hypothèse de récurrence, on peut décomposer z_1 et z_2 , donc z est décomposable.

Pour l'unicité, soit $z \in \mathbb{Z}[i] \setminus \{0\}$ tel que $z = u \prod_{\rho \in \mathcal{P}_0} \rho^{\nu_\rho(z)} = v \prod_{\rho \in \mathcal{P}_0} \rho^{\mu_\rho(z)}$. Le théorème de Gauss est valable dans $\mathbb{Z}[i]$, car c'est un anneau principal. S'il existe $\rho_0 \in \mathcal{P}_0$ tel que $\nu_{\rho_0}(z) < \mu_{\rho_0}(z)$, alors

$$\rho_0 \mid \prod_{\rho \in \mathcal{P}_0 \setminus \{\rho_0\}} \rho^{\nu_\rho(z)}$$

ce qui est proscrit par le théorème de Gauss. On a donc pour tout $\rho \in \mathcal{P}_0$, $\nu_\rho(z) = \mu_\rho(z)$. En reportant, on a $u = v$. D'où l'unicité de la décomposition.

Solution 1.50.

1. On a $\bar{1} \in R$. Soit $(\bar{x}_1, \bar{x}_2) \in R^2$, il existe $(\bar{y}_1, \bar{y}_2) \in (\mathbb{F}_p^*)^2$ tel que $\bar{x}_1 = \bar{y}_1^2$ et $\bar{x}_2 = \bar{y}_2^2$. On a alors

$$\bar{x}_1 \bar{x}_2^{-1} = (\bar{y}_1 \bar{y}_2^{-1})^2 \in R$$

donc R est un sous groupe de (\mathbb{F}_p^*, \times) . Soit

$$\begin{aligned} \varphi : \mathbb{F}_p^* &\rightarrow \mathbb{F}_p^* \\ \bar{y} &\mapsto \bar{y}^2 \end{aligned}$$

On a $\text{Im}(\varphi) = R$. Comme \mathbb{F}_p est un corps, chaque élément de R a exactement 2 antécédents par φ . Donc $|R| = \frac{|\mathbb{F}_p^*|}{2} = \frac{p-1}{2}$.

S'il existe $\bar{y} \in \mathbb{F}_p^*$ tel que $\bar{a} = \bar{y}^2$, on a $\bar{a}^{\frac{p-1}{2}} = \bar{y}^{p-1} = \bar{1}$ par le théorème de Fermat.

Réciproquement, si $\bar{a}^{\frac{p-1}{2}} = \bar{1}$, $X^{\frac{p-1}{2}} - \bar{1}$ admet au plus $\frac{p-1}{2}$ racines dans \mathbb{F}_p^* . Tous les éléments de R sont racines de ce polynôme, ce sont donc ses seules racines. Donc $a \in R$.

2. Si $p = a^2 + b^2$, alors $\bar{0} = \bar{a}^2 + \bar{b}^2$. Si $\bar{a} = \bar{b} = \bar{0}$, on a $p \mid a$ et $p \mid b$ donc $p^2 \mid p$ ce qui est exclu. Par exemple, si $\bar{a} \neq \bar{0}$, on a $\bar{1} = -\bar{b}^2 \bar{a}^{-2}$ donc $\overline{-1} = (\bar{a}^{-1} \bar{b})^2 \in R$ d'après 1. On a donc $(\overline{-1})^{\frac{p-1}{2}} = \bar{1}$ si et seulement si $2 \mid \frac{p-1}{2}$ (car p est premier plus grand que 3) d'où $4 \mid p-1$ donc $p \equiv 1[4]$.
3. On a $|\mathbb{F}_p| = p$, $E(\sqrt{p}) \leq \sqrt{p} < E(\sqrt{p}) + 1$ et $|\{0, \dots, E(\sqrt{p})\}|^2 = (E(\sqrt{p}) + 1)^2 > p$ (p est premier, ce n'est pas un carré) donc f n'est pas injective (cardinalité).

Donc il existe

$$((a_1, b_1), (a_2, b_2)) \in (\{0, \dots, E(\sqrt{p})\}^2)^2$$

avec $(a_1, b_1) \neq (a_2, b_2)$ et $f(a_1, b_1) = f(a_2, b_2)$. Donc

$$\overline{a_1} - \overline{kb_1} = \overline{a_2} - \overline{kb_2} \Rightarrow \overline{a_1} - \overline{a_2} = \overline{k}(\overline{b_1} - \overline{b_2})$$

Si $\overline{b_1} = \overline{b_2}$, alors $\overline{a_1} = \overline{a_2}$ donc $p \mid b_1 - b_2$ et $p \mid a_1 - a_2$ donc $(a_1, b_1) = (a_2, b_2)$ ce qui n'est pas vrai. Donc $\overline{b_1} \neq \overline{b_2}$. Posons $b_0 = b_1 - b_2$ et $a_0 = a_1 - a_2$. On a $\overline{b_0} \neq \overline{0}$. Il vient donc $(|a_0|, |b_0|) \in \{1, \dots, E(\sqrt{p})\}^2$, $\overline{a_0} = \overline{kb_0}$ donc $\overline{k} = \overline{a_0} \overline{b_0}^{-1}$.

4. Si $p \equiv 1[4]$, en remontant les calculs, on a $(\overline{-1})^{\frac{p-1}{2}} = \overline{1}$ donc $\overline{-1} \in R$ et il existe $\overline{k} \in \mathbb{F}_p^*$ tel que $\overline{-1} = \overline{k}^2$. Alors d'après 3., il existe (a_0, b_0) tels que $\overline{k} = \overline{a_0} \overline{b_0}^{-1}$. Il vient alors $\overline{-1} = \overline{a_0}^2 (\overline{b_0}^{-1})^2$ donc $\overline{-b_0}^2 = \overline{a_0}^2$. On a

$$p \mid a_0^2 + b_0^2 \in \{2, \dots, 2E(\sqrt{p})\}^2 \subset \{2, \dots, 2p-1\}$$

Nécessairement, $a_0^2 + b_0^2 = p$ et p est somme de deux carrés.

Solution 1.51.

1. Soit $(m, n) \in A^2$. Il existe $(a, b, c, d) \in \mathbb{N}^4$ tel que $m = a^2 + b^2 = |a + ib|^2$ et $n = c^2 + d^2 = |c + id|^2$. Donc

$$m \times n = |ac - bd6i(bc + ad)|^2 = (ac - bd)^2 + (bc + ad)^2 \in A$$

2. On a

$$n = \underbrace{\prod_{p \in \mathcal{P}_1} p^{\nu_p(n)}}_{\in A \text{ car } \mathcal{P}_1 \subset A} \times \underbrace{\prod_{p \in \mathcal{P}_2} p^{\nu_p(n)}}_{= \prod_{p \in \mathcal{P}_2} p^{2\alpha_p} \in A} \in A$$

3. Soit $n \in A$, il existe $(a, b) \in \mathbb{N}^2$ avec $n = a^2 + b^2$. Soit $p \in \mathcal{P}_1 \cup \mathcal{P}_2$, on a $p \mid a^2 + b^2$ donc $\overline{a^2 + b^2} = \overline{0}$ dans $\mathbb{Z}/p\mathbb{Z}$. Si $p \nmid a$ ou $p \nmid b$, alors $\overline{1 + \frac{b^2}{a^2}} = \overline{0}$ donc $\overline{-1} \in R$ (résidus quadratiques, voir exercice précédent). Donc $p = 2$ ou $p \equiv 1[4]$.

Si $p \mid a$ et $p \mid b$, $a = p^k a'$, $b = p^l b'$ avec $p \nmid a'$ et $p \nmid b'$. On suppose $1 \leq k \leq l$ (quitte à échanger a et b). On a

$$a^2 + b^2 = p^{2k}(a'^2 + p^{2(l-k)}b'^2) = n$$

donc

$$p \mid a'^2 + p^{2(l-k)}b'^2$$

et $\overline{a'^2} + \overline{p^{2(l-k)}b'^2} = \overline{0}$. Nécessairement, $l = k$. De même $p \in \mathcal{P}_1$. Par contraposée, ν_p est pair.

- 2 Séries numériques et familles sommables
- 3 Probabilités sur un univers dénombrable
- 4 Calcul matriciel

5 Réduction des endomorphismes

Solution 5.1. Si on a (i), soit x un vecteur propre associé à $\rho(u) = \rho e^{i\theta}$. On a $\|u(x)\| = \|\rho(u)x\| = \rho(u)\|x\|$ et comme $x \neq 0$, on a $\rho(u) \leq \|\rho(u)\| < 1$ d'où (ii).

Si (ii), on utilise la décomposition de Dunford $u = n + d$ avec n nilpotent, d diagonalisable et $dn = nd$. Soit $m = \dim(E)$. Pour tout $p \geq m$, on a

$$u^p \sum_{k=0}^p \binom{p}{k} n^k d^{p-k} = \sum_{k=0}^{m-1} \binom{p}{k} n^k \underbrace{d^{p-k}}_{\xrightarrow{p \rightarrow +\infty} 0}$$

En effet, on a $k \geq m-1$ fixé, il existe une base \mathcal{B} de E telle que

$$\binom{p}{k} \text{mat}_{\mathcal{B}}(d^p) = \binom{p}{k} \text{diag}(\lambda_1^p, \dots, \lambda_m^p) \xrightarrow{p \rightarrow +\infty} 0$$

car $|\lambda_i| < 1$ pour tout $i \in \{1, \dots, m\}$ et

$$\binom{p}{k} \underset{p \rightarrow +\infty}{\sim} \frac{p^k}{k!} = \underset{p \rightarrow +\infty}{o} \left(\frac{1}{\rho(u)^p} \right)$$

donc on a (iii).

Si (iii), soit x un vecteur propre associé à $\lambda \in \mathbb{C}$, on a $u^p \xrightarrow{p \rightarrow +\infty} 0$ donc en particulier, $u^p(x) = \lambda^p \xrightarrow{p \rightarrow +\infty} 0$, donc $\rho(u)^p \xrightarrow{p \rightarrow +\infty} 0$ et $\rho(u) \geq 0$ donc $\rho(u) < 1$. Posons encore $u = d + n$ la décomposition de Dunford de u . Soit $\varepsilon > 0$, il existe $\mathcal{B}_0 = (e_1, \dots, e_n)$ base de E dans laquelle les coefficients de $\text{mat}_{\mathcal{B}_0}(n)$ sont en module $\leq \varepsilon$. Définissons sur E

$$\left\| \sum_{i=1}^m x_i e_i \right\|_{\infty} = \max_{1 \leq i \leq m} |x_i|$$

Soit $M = \text{mat}_{\mathcal{B}_0}(u) = (m_{i,j})_{1 \leq i,j \leq m}$ triangulaire supérieure avec $m_{ii} = \lambda_i$ et pour tout $j \neq i$, $|m_{i,j}| < \varepsilon$.

Soit donc $x = \sum_{i=1}^m x_i e_i \in \mathbb{C}^m$, on a

$$\|Mx\|_{\infty} = \max_{1 \leq i \leq n} \underbrace{\left| \sum_{j=1}^m m_{i,j} x_j \right|}_{(|\lambda_i| + (m-1)\varepsilon)\|x\|_{\infty}}$$

donc

$$\|u\| \leq \underbrace{\rho(u)}_{< 1} + (m-1)\varepsilon$$

et on choisit

$$\varepsilon < \underbrace{\frac{1 - \rho(u)}{m - 1}}_{>0}$$

d'où $\|u\| < 1$ et donc on a (i) et finalement on a bien l'équivalence.

Remarque 5.1. $u \mapsto \rho(u)$ n'est pas une norme car pour u nilpotente non nulle, $\rho(u) = 0$.

Solution 5.2. Supposons (i), soit Y un vecteur propre de A avec $AY = \lambda Y$ pour $\lambda \in \mathbb{C}$. Pour tout $k \in \mathbb{N}$, $BA^k Y = \lambda^k BY$ et il existe $k_0 \in \mathbb{N}$ tel que $\lambda^{k_0} BY \neq 0$ et $BY \neq 0$ donc on a (ii).

Si (ii), supposons qu'il existe $Y \in \mathbb{C}^n \setminus \{0\}$ tel que $\varphi = 0$. On note

$$\chi_A = \prod_{i=1}^r (X - \lambda_i)^{m_i}$$

avec les λ_i distincts. Alors $Y = \sum_{i=1}^r Y_i$ où $Y_i \in \ker(A - \lambda_i I_n)$. Il existe $i_0 \in \{1, \dots, r\}$ tel que $Y_{i_0} \neq 0$ car $Y \neq 0$. On a alors, pour $t \in \mathbb{R}$,

$$B \exp(tA)Y = \sum_{i=1}^r B \exp(t\lambda_i)Y_i = 0$$

Pour tout $k \in \{0, \dots, r-1\}$, on a $\varphi^{(k)}(t) = \sum_{i=1}^r B \lambda_i^k \exp(t\lambda_i)Y_i = 0$. Pour $t = 0$ on a $\sum_{i=1}^r \lambda_i^k BY_i = 0$ ce qui, pour $t = 0$, donne le système

$$\begin{cases} BY_1 + \dots + BY_r & = 0 \\ \lambda_1 BY_1 + \dots + \lambda_r BY_r & = 0 \\ & \vdots \\ \lambda_1^{r-1} BY_1 + \dots + \lambda_r^{r-1} BY_r & = 0 \end{cases}$$

Pour tout $P \in \mathbb{C}_{r-1}[X]$, on a donc $\sum_{i=1}^r P(\lambda_i) BY_i = 0$. Pour $i \in \{0, \dots, r-1\}$ et $P = \prod_{j \neq i} \frac{(X - \lambda_j)}{\lambda_i - \lambda_j}$, on obtient pour tout $i \in \{1, \dots, r\}$, $BY_i = 0$. En particulier, $BY_{i_0} = 0$ et Y_{i_0} est un vecteur propre de A car non nul. C'est une contradiction. On a donc (iii).

Soit $Y \in \mathbb{C}^n \setminus \{0\}$, supposons que pour tout $k \in \{0, \dots, n-1\}$, $BA^k Y = 0$. Soit $k \geq n$, il existe $(Q_k, R_k) \in \mathbb{C}[X] \times \mathbb{C}_{n-1}[X]$ tel que

$$X^k = Q_k \chi_A + R_k$$

et le théorème de Cayley-Hamilton donne donc $A^k = R_k(A)$ d'où $BA^kY = BR_k(A)Y = 0$. Alors pour tout $t \in \mathbb{R}$,

$$\begin{aligned} B \exp(tA)Y &= B \sum_{k=0}^{+\infty} \frac{t^k A^k}{k!} Y \\ &= \sum_{k=0}^{+\infty} \frac{t^k (BA^kY)}{k!} \\ &= 0 \end{aligned}$$

Par contraposée, on a bien ce qu'il faut, d'où l'équivalence.

6 Espaces vectoriels normés

Solution 6.1.

1. A $(x, y) \in \mathbb{R}^2$ fixé, la fonction

$$\begin{aligned}\varphi: \mathbb{R} &\rightarrow \mathbb{R} \\ t &\mapsto x \cos(t) + y \sin(2t)\end{aligned}$$

est bornée, donc le sup sur \mathbb{R} existe. Pour la séparation, prendre $t = 0$ et $t = \frac{\pi}{4}$. Pour l'inégalité triangulaire, montrer l'inégalité à t fixé puis passer au sup sur \mathbb{R} .

2. Si $|x| + |y| \leq 1$, alors $N(x, y) \leq 1$ donc on a la première inclusion.

Si $N(x, y) \leq 1$, utiliser $t = 0$ pour avoir $|x| \leq 1$ et $t = \frac{\pi}{4}$ puis $t = -\frac{\pi}{4}$ pour pouvoir justifier

$$|2y| \leq \left| x \frac{\sqrt{2}}{2} + y \right| + \left| y - x \frac{\sqrt{2}}{2} \right| \leq 2$$

et donc $|y| \leq 1$. D'où la deuxième inclusion.

3. On fixe $(x, y) \in S_N(0, 1) \cap (\mathbb{R}_+)^2$. φ est 2π -périodique, $\varphi(\pi - t) = \varphi(t)$ et $\sup_{t \in \mathbb{R}} |\varphi(t)| = 1$. On peut donc se limiter à un intervalle de longueur 2π pour l'étude de φ .

On note que si $t \in [-\pi, 0]$, $\cos(t)$ et $\sin(2t)$ sont de signes opposés. Donc

$$|\varphi(t)| \leq x |\cos(t)| + y |\sin(2t)| = |\varphi(-t)|$$

et $-t \in [0, \pi]$. Donc le sup est atteint sur $[0, \pi]$.

On note maintenant, comme $|\varphi(\pi - t)| = |\varphi(t)|$ sur $[0, \frac{\pi}{2}]$, que si $t \in [\frac{\pi}{4}, \frac{\pi}{2}]$,

$$0 \leq \varphi(t) = \underbrace{x \cos(t)}_{\in [0, \frac{\sqrt{2}}{2}]} + y \sin(2t) \leq \underbrace{x \cos(\frac{\pi}{2} - t)}_{\in [\frac{\sqrt{2}}{2}, 1]} + y \sin(2 \times (\frac{\pi}{2} - t)) = \varphi(\frac{\pi}{2} - t)$$

Donc le sup est atteint sur $[0, \frac{\pi}{4}]$. Soit maintenant $t_0 \in [0, \frac{\pi}{4}]$ tel que $\varphi(t_0)$ réalise le sup (existe car φ est continue sur un compact). Comme c'est aussi le sup sur \mathbb{R} qui est ouvert, on a la condition d'Euler du premier ordre : $\varphi'(t_0) = 0$.

On a donc $x \cos(t_0) + y \sin(2t_0) = 1$ et $-x \sin(t_0) + 2y \cos(2t_0) = 0$. On en déduit les valeurs de x et y en fonction de t_0 , en faisant attention que $\cos(t_0) \neq 0$ sinon $\sin(t_0) = 0$ aussi ce qui n'est pas le cas, et au cas où $t_0 = 0$.

Réciproquement, s'il existe $t_0 \in [0, \frac{\pi}{4}]$ tel que x et y s'écrivent de la façon demandée, alors t_0 est l'unique point satisfaisant $\varphi(t_0) = 1$ et $\varphi'(t_0) = 0$. Mais alors le sup de φ sur $[0, \frac{\pi}{4}]$ est atteint en un point t_1 qui vérifie les mêmes choses, donc $t_1 = t_0$ d'où $N(x, y) = 1$.

Solution 6.2.

1. Pour l'inégalité triangulaire, introduire la forme bilinéaire symétrique positive sur E

$$\begin{aligned}\varphi : E \times E &\rightarrow \mathbb{R} \\ (f, g) &\mapsto f(0)g(0) + \int_0^1 f'(t)g'(t)dt\end{aligned}$$

Alors $N(f) = \sqrt{\varphi(f, f)}$ et on utilise l'inégalité de Minkowski.

2. Pour $x \in [0, 1]$, écrire $|f(x)| = |f(0) + f(x) - f(0)|$, $f(x) - f(0) = \int_0^x f'(t)dt$, utiliser Cauchy-Schwarz avec f' et 1 puis que $\sqrt{a} + \sqrt{b} \leq \sqrt{2}\sqrt{a+b}$, pour enfin passer au sup sur x .
3. Utiliser, pour $n \in \mathbb{N}^*$, la fonction

$$\begin{aligned}f_n : [0, 1] &\rightarrow \mathbb{R} \\ t &\mapsto t^n\end{aligned}$$

Solution 6.3. Si f est ouverte, $f(\mathbb{R}^n)$ est un sous-espace vectoriel ouvert de \mathbb{R}^p . Donc f est surjective.

Si f est surjective, on prend F un supplémentaire de $\ker(f)$ dans \mathbb{R}^n avec $\dim(\ker(f)) = n - p$ et $\dim(F) = p$. Soit (e_1, \dots, e_p) une base de F et (e_{p+1}, \dots, e_n) une base de $\ker(f)$. On vérifie que $(f(e_1), \dots, f(e_p))$ est une base de \mathbb{R}^p . On définit

$$\begin{aligned}N_1 : \mathbb{R}^n &\rightarrow \mathbb{R} \\ \sum_i^n x_i e_i &\mapsto \max_{1 \leq i \leq n} |x_i|\end{aligned}$$

norme sur \mathbb{R}^n et

$$\begin{aligned}N_2 : \mathbb{R}^p &\rightarrow \mathbb{R} \\ \sum_i^p y_i f(e_i) &\mapsto \max_{1 \leq i \leq p} |y_i|\end{aligned}$$

norme sur \mathbb{R}^p .

Soit Θ un ouvert de \mathbb{R}^n , soit $y_0 \in f(\Theta)$, il existe $x_0 \in \Theta$: $y_0 = f(x_0)$. Si $x_0 = \sum_{i=1}^n \alpha_i e_i$, alors $y_0 = \sum_{i=1}^p \alpha_i f(e_i)$. Comme Θ est un ouvert, il existe $r_0 > 0$ tel que

$$B_{N_1}(x_0, r_0) \subset \Theta$$

Soit $y = \sum_{i=1}^p \beta_i f(e_i) \in \mathbb{R}^p$, si $N_2(y - y_0) < r_0$, pour tout $i \in \{1, \dots, p\}$, $|\beta_i - \alpha_i| < r_0$ et

$$y = f\left(\sum_{i=1}^p \beta_i e_i + \sum_{i=p+1}^n \alpha_i e_i\right) \stackrel{\text{def}}{=} f(x)$$

avec $N_1(x - x_0) = \max_{1 \leq i \leq p} |\beta_i - \alpha_i| < r_0$. Ainsi $x \in \Theta$ et $y \in f(\Theta)$, donc $B_{N_2}(y_0, r_0) \subset f(\Theta)$ et $f(\Theta)$ est un ouvert.

Solution 6.4.

1. Classique.

2.

$$|f(x)| \leq |f(0)| + |f(x) - f(0)| \leq |f(0)| + \kappa(f)x \leq N(f)$$

car $x \leq 1$, donc $N_\infty \leq N$. Pour la non-équivalence, prendre

$$\begin{aligned} f_n : [0, 1] &\rightarrow \mathbb{R} \\ t &\mapsto t^n \end{aligned}$$

3. On a $|f(0)| \leq N_\infty(f)$ donc $N(f) \leq N'(f)$. Ensuite, $N_\infty \leq N$ donne $N' \leq N + \kappa \leq 2N$.

Donc N et N' sont équivalentes.

Remarque 6.1. Exemple de normes qui, en dimension infinie, ne se dominent pas mutuellement. On prend $(e_i)_{i \in I}$ une base (de Hamel), $J = (i_n)_{n \in \mathbb{N}} \subset I$ dénombrable. Si $x = \sum_{i \in I} x_i e_i$, on peut vérifier que

$$N_1(x) = \sum_{n \in \mathbb{N}} |x_{i_n}| + \sum_{i \in I \setminus J} |x_i|$$

et

$$N_2(x) = \sum_{n \in \mathbb{N}} n |x_{i_{2n}}| + \sum_{n \in \mathbb{N}} \frac{1}{n+1} |x_{i_{2n+1}}| + \sum_{i \in I \setminus J} |x_i|$$

ne se dominent pas.

Solution 6.5. Il existe $\alpha > 0$ tel que $B_{\|\cdot\|_\infty}(I_n, \alpha) \subset G$. Soient $i \neq j$ et $\lambda \in \mathbb{C}$. Il existe $p \in \mathbb{N}^*$ tel que $\frac{|\lambda|}{p} < \alpha$. Alors

$$\left\| T_{i,j} \left(\frac{\lambda}{p} \right) - I_n \right\|_\infty = \left| \frac{\lambda}{p} \right| < \alpha$$

donc $T_{i,j}(\lambda) \in G$ ($T_{i,j}$ est la matrice de transvection : $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$).

Ainsi,

$$T_{i,j}(\lambda) = \left(T_{i,j} \left(\frac{\lambda}{p} \right) \right)^p \in G$$

Soit $\delta = \rho e^{i\theta} \in \mathbb{C}^*$. On a $\lim_{n \rightarrow +\infty} \rho^{\frac{1}{p}} e^{i\frac{\theta}{p}} = 1$ donc il existe $p \in \mathbb{N}^*$ tel que $|\rho^{\frac{1}{p}} e^{i\frac{\theta}{p}} - 1| < \alpha$.

On a alors

$$\left\| D_n \left(\rho^{\frac{1}{p}} e^{i\frac{\theta}{p}} \right) - I_n \right\|_\infty < \alpha$$

donc $D_n(\delta) = D_n(\rho^{\frac{1}{p}} e^{i\frac{\theta}{p}})^p \in G$ (matrice de dilatation).

Comme les matrices de transvection et de dilatation engendrent $GL_n(\mathbb{C})$, on a bien $G = GL_n(\mathbb{C})$.

Remarque 6.2. C'est faux sur \mathbb{R} . Contre-exemple : matrices de déterminant positif.

Solution 6.6. Si f n'est pas continue en 0, il existe $\varepsilon_0 > 0$ tel que pour tout $\alpha > 0$, il existe $h \in E$ avec $\|h\| \leq \alpha$ et $\|f(h)\| > \varepsilon_0$. On prends $\alpha_n = \frac{1}{n+1}$, d'où $\|nh_n\| \leq 1$ mais $\underbrace{\|f(nh_n)\|}_{\leq M} > n\varepsilon_0 \xrightarrow{n \rightarrow +\infty} +\infty$.

Donc f est continue en 0. Comme f est linéaire, pour tout $x \in E$,

$$\lim_{\|h\| \rightarrow 0} f(x+h) = \lim_{\|h\| \rightarrow 0} f(x) + f(h) = f(x)$$

donc f est continue.

On a $f(px) = p(fx)$ pour tout $p \in \mathbb{Z}$ puis $qf(\frac{p}{q}x) = f(px) = pf(x)$ pour tout $(p, q) \in \mathbb{Z} \times \mathbb{N}^*$ donc pour tout $r \in \mathbb{Q}$, $f(rx) = rf(x)$. Soit $\lambda \in \mathbb{E}$, il existe une suite de rationnels telle que

$\lim_{n \rightarrow +\infty} r_n = \lambda$. Comme f est continue, on a

$$\begin{aligned} f(\lambda x) &= \lim_{n \rightarrow +\infty} f(r_n x) \\ &= \lim_{n \rightarrow +\infty} r_n f(x) \\ &= \lambda f(x) \end{aligned}$$

Donc f est linéaire.

Remarque 6.3. Soit $e_0 = 1$ et $e_1 = \sqrt{2}$ et $(e_i)_{i \in I}$ une \mathbb{Q} -base de \mathbb{R} ($0 \in I$). On définit

$$f\left(\sum_{i \in I} \lambda_i e_i\right) = \lambda_0 e_0 + \sqrt{2} \sum_{i \in I \setminus \{0\}} \lambda_i e_i$$

f vérifie $f(x + y) = f(x) + f(y)$, mais si $(r_n)_{n \in \mathbb{N}}$ est une suite de rationnels tendant vers $\sqrt{2}$, $f(r_n) = r_n \rightarrow \sqrt{2} \neq f(\sqrt{2}) = 2$.

Solution 6.7.

1. On a $\alpha(A) \subset \overline{A}$ donc $\overline{\overline{A}} \subset \overline{A}$ donc $\alpha(\alpha(A)) \subset \alpha(A)$. Comme $\alpha(A)$ est un ouvert inclus dans $\overline{\overline{A}} \subset \overline{A}$ donc $\alpha(A) \subset \alpha(\alpha(A))$.
2. Si $\beta(A) = \overline{\overline{A}}$, on montre aussi que $\beta(\beta(A)) = \beta(A)$. On a donc $A, \overline{A}, \overset{\circ}{A}, \overline{\overset{\circ}{A}}, \overline{\overline{\overset{\circ}{A}}}$ et $\overline{\overline{\overline{\overset{\circ}{A}}}}$ et c'est tout.

Solution 6.8.

1. Si $d_A = d_B$,

$$\overline{A} = \{x \in E \mid d_A(x) = 0\} = \{x \in E \mid d_B(x) = 0\} = \overline{B}$$

Réciproquement, soit $x \in E$ et $\varepsilon > 0$, il existe $a_1 \in \overline{A}$, $\|x - a_1\| \leq d_{\overline{A}}(x) + \frac{\varepsilon}{2}$ (par définition de l'inf). Il existe $a_2 \in A$, $\|a_1 - a_2\| \leq \frac{\varepsilon}{2}$ (par définition de la fermeture). Ainsi,

$$d_A(x) \leq \|x - a_2\| \leq \|x - a_1\| + \|a_1 - a_2\| \leq d_{\overline{A}}(x) + \varepsilon$$

Ceci valant pour tout $\varepsilon > 0$, $d_A(x) \leq d_{\overline{A}}(x)$. Comme $A \subset \overline{A}$, $d_{\overline{A}} \leq d_A$, on a $d_A = d_{\overline{A}} = d_{\overline{B}} = d_B$.

2. Soit $x \in A$, on a $d_B(x) = |d_B(x) - d_A(x)| \leq \rho(A, B)$ donc $\sup_{x \in A} d_B(x) \leq \rho(A, B)$, de même pour $\sup_{y \in B} d_A(y)$ donc on a une première inégalité.

Réciproquement, soit $x \in E$ et $\varepsilon > 0$, il existe $a \in A$ et $b \in B$ tel que $\|x - a\| \leq d_A(x) + \varepsilon$ et $\|x - b\| \leq d_B(x) + \varepsilon$. On a alors

$$d_A(x) \leq \|x - a\| \leq \|a - b\| + \|x - b\| \leq d_B(x) + \varepsilon + \alpha(A, B)$$

Ceci vaut pour tout $\varepsilon > 0$, donc $d_A(x) \leq d_B(x) + \alpha(A, B)$. De même, $d_B(x) \leq d_A(x) + \alpha(A, B)$ donc $\rho(A, B) \leq \alpha(A, B)$.

Solution 6.9.

1. Soit $(y_n)_{n \in \mathbb{N}} \in P(F)^{\mathbb{N}}$ qui converge vers $y \in \mathbb{C}$ donc il existe $(x_n) \in F^{\mathbb{N}}$ telle que l'on ait pour tout $n \in \mathbb{N}$, $P(x_n) = y_n$. $(x_n)_{n \in \mathbb{N}}$ est bornée car $\lim_{z \rightarrow +\infty} |P(z)| = +\infty$ (car P est non constant), donc on peut extraire (Bolzano-Weierstrass) $x_{\sigma(n)} \rightarrow x$ et $x \in F$ car F est fermé. Par continuité de $z \mapsto P(z)$ sur \mathbb{C} , on a $y = P(x) \in P(F)$.
2. Soit Θ un ouvert de \mathbb{C} , soit $y \in P(\Theta)$, $\exists x \in \Theta$ tel que $P(x) = y$ et il existe $r > 0$, $B(x, r) \subset \Theta$. Soit $y' \in \mathbb{C}$, supposons que pour tout $x' \in \mathbb{C}$ tel que $P(x') = y'$, on a $|x - x'| > r$. Soit $Q(X) = P(X) - y' = a \prod_{i=1}^n (X - x_i)$ non constant où a est le coefficient dominatrice de P . Par hypothèse, pour tout $i \in \{1, \dots, n\}$: $|x_i - x| > r$ (car $P(x_i) = y'$), ainsi

$$|Q(x)| = |y - y'| \geq |a|r^n$$

Par contraposée, si $|y - y'| \leq \frac{|a|r^n}{2}$, alors il existe $x' \in \mathbb{C}$ tel que $P(x') = y'$ et $|x' - x| < r$. Ainsi, $x' \in B(x, r) \subset \Theta$ et $y' \in P(\Theta)$. Donc $B(y, |a|r^n) \subset P(\Theta)$ et $P(\Theta)$ est un ouvert.

Solution 6.10.

1. Si $P \notin \mathcal{S}$, il existe $z_0 \in \mathbb{C} \setminus \mathbb{R}$ tel que $P(z_0) = 0$ et $|\Im(z_0)|^n > 0 = P(z_0)$. Par contraposée, si pour tout $z \in \mathbb{C}$, $|P(z)| \geq |\Im(z)|^n$, alors $P \in \mathcal{S}$.

Réciproquement, si $P = \prod_{i=1}^n (X - \lambda_i) \in \mathcal{S}$ avec $(\lambda_i)_{1 \leq i \leq n}$ réels, soit $z = a + ib \in \mathbb{C}$. On a

$$|P(z)| = \prod_{i=1}^n |a - \lambda_i + ib| \geq |b|^n$$

2. Soit $(P_p)_{p \in \mathbb{N}} \in \mathcal{S}^{\mathbb{N}}$ telle que $P_p \xrightarrow{p \rightarrow +\infty} P \in F$. Soit $z \in \mathbb{C}$, on a pour tout $p \in \mathbb{N}$, $|P_p(z)| \geq |\Im(z)|^n$ donc quand $p \rightarrow +\infty$, $|P(z)| \geq |\Im(z)|^n$ donc $P \in \mathcal{S}$ et \mathcal{S} est fermé.

3. Soit $(M_p)_{p \in \mathbb{N}}$ une suite de matrice trigonalisable sur \mathbb{R} qui converge vers $M \in \mathcal{M}_n(\mathbb{R})$.
 On bite χ_p le polynôme caractéristique de M_p . Pour tout $p \in \mathbb{N}$, $\chi_p \in \mathcal{S}$ et $\chi_p \xrightarrow{p \rightarrow +\infty} \chi_M$.
 Comme \mathcal{S} est fermé, $\chi_M \in \mathcal{S}$ et M est trigonalisable sur \mathbb{R} .

Solution 6.11.

1. φ est linéaire et $\dim(\mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X]) = m + n - 1 = \dim(\mathbb{K}_{n+m-1}[X])$.
 Si φ est bijective, elle est surjective et il existe $(U, V) \in \mathbb{K}[X]^2$ tel que $UA + BV = 1$ et d'après le théorème de Bézout, on a $A \wedge B = 1$.
 Réciproquement, si φ n'est pas surjective, il existe $(U, V) \in (\mathbb{K}_{m-1}[X] \times \mathbb{K}_{n-1}[X]) \setminus \{(0, 0)\}$ tel que $\varphi(U, V) = 0$ d'où $AU = -BV$. Soit $\delta = A \wedge B$, on écrit $A = \delta A_1$ et $B = \delta B_1$ avec $A_1 \wedge B_1 = 1$ et on a $A_1 U = -B_1 V$. D'après le théorème de Gauss, on a $A_1 \mid V$ et $B_1 \mid U$. Si $U = 0$, on a $V = 0$ et de même si $V = 0$, on a $U = 0$. On peut donc supposer $U \neq 0$ et $V \neq 0$, et on a alors $\deg(A_1) \leq \deg(V) \leq n - 1 < n = \deg(A)$ mais $A = \delta A_1$ donc $\deg(\delta) \geq 1$ et $A \wedge B \neq 1$.
 2. Φ est continue car $R_{A,B}$ est un polynôme en les coefficients de A et B .
 3. Comme on est dans \mathbb{C} , $\Delta = \{P \in \mathbb{C}_p[X] \mid P \wedge P' = 1\} = \{P \in \mathbb{C}_p[X] \mid R_{P,P'} \neq 0\}$.
 $\Phi_{P,P'}$ est continue d'après la question précédente, $\delta = \Phi_{P,P'}^{-1}(\mathbb{C}^*)$ donc Δ est ouvert.
 Sur \mathbb{R} , on n'a pas la caractérisation de scindé à racines simples si et seulement si $P \wedge P' = 1$ (contre-exemple : $P = X^2 + 1$). Dans $\mathbb{R}_3[X]$, X est scindé à racines simples et $X(1 + \varepsilon X)^2 \xrightarrow{\varepsilon \rightarrow 0} X$ et $-\frac{1}{\varepsilon}$ est racine double, donc Δ n'est pas ouvert.

Remarque 6.4. On peut cependant considérer

$$\Delta_n = \{P \in \mathbb{C}_p[X] \mid P \text{ scindé à racines simples sur } \mathbb{R} \text{ et } \deg(P) = n\}$$

Si $\lambda_1 < \lambda_2 < \dots < \lambda_n$ sont les racines (distinctes) de R sur \mathbb{R} , on choisit $\alpha_0 \in]-\infty, \lambda_1, \alpha_n \in]\lambda_n, +\infty[$ et $\alpha_i \in]\lambda_i, \lambda_{i+1}[$ si $i = 1, \dots, n - 1$.

Pour tout $k \in \{0, \dots, n - 1\}$, on a $P(\alpha_k)P(\alpha_{k+1}) < 0$ (car les racines de P provoquent des changements de signe). Soit

$$\begin{aligned} \Psi : \mathbb{R}_n[X] &\rightarrow \mathbb{R}^n \\ Q &\mapsto (Q(\alpha_k)Q(\alpha_{k+1}))_{0 \leq k \leq n-1} \end{aligned}$$

Ψ est continue sur $\mathbb{R}_n[X]$ et $\Psi(P) \in (\mathbb{R}_-^*)^n$ qui est ouvert, donc il existe $r > 0$ tel que si $\|P - Q\| < r$, alors $\Psi(Q) \in (\mathbb{R}_-^*)^n$. Donc Q change n fois de signe, et admet au moins n racines. Mais $\deg(Q) = n$, donc Q est scindé à racines simples sur \mathbb{R} , donc Δ_n est ouvert dans $\{P \in \mathbb{R}[X] \mid \deg(P) = n\}$.

Remarque 6.5.

$$\{M \in \mathcal{M}_n(\mathbb{C}) \mid M \text{ diagonalisable à racines simples}\} = \{M \in \mathcal{M}_n(\mathbb{C}) \mid \chi_M \text{ sciné à racines simples}\}$$

est un ouvert de $\mathcal{M}_n(\mathbb{C})$ car $M \mapsto \chi_M$ est continue sur $\mathcal{M}_n(\mathbb{C})$, et c'est aussi vrai sur \mathbb{R} .

Solution 6.12.

1. Soit

$$\begin{aligned} f : \mathcal{M}_n(\mathbb{R}) &\rightarrow \mathcal{M}_n(\mathbb{R}) \\ A &\mapsto A^n \end{aligned}$$

f est continue et $F = f^{-1}(\{0\})$ donc $F = \overline{F}$.

Soit $M_0 \in F$, X^n annule M_0 donc M_0 est trigonalisable : on écrit M_0 dans une base où les coefficients diagonaux sont tous nuls. Soit alors M_ε la même matrice dans la même base en rajoutant simplement ε en première position de la diagonale. Alors $M_\varepsilon \xrightarrow{\varepsilon \rightarrow 0} M_0$ et $M_\varepsilon \notin F$ donc $\overset{\circ}{F} = \emptyset$. Notons que cela signifie que F est dense.

2. La norme dérive du produit scalaire $(A|B) \mapsto \text{Tr}(A^\top B)$. Soit $M \in F$, on a $\|M - I_n\|^2 = \|M\|^2 + \|I_n\|^2 - 2(M|I_n)$. On a $(M|I_n) = \text{Tr}(M) = 0$ car M est nilpotente. Donc $\|M - I_n\|^2$ est minimale pour $\|M\|^2$ minimale, donc pour $M = 0 \in F$. Donc $d(I_n, F) = \|I_n\| = \sqrt{n}$ (et la distance est atteinte pour $0_{\mathcal{M}_n(\mathbb{R})}$).

Solution 6.13.

1. $A \mapsto \det(A)$ est continue et $GL_n(\mathbb{K}) = \det^{-1}(\mathbb{K}^*)$ est donc ouvert. Si $A \in \mathcal{M}_n(\mathbb{K})$, pour $p \in \mathbb{N}$, on pose $A_p = A - \frac{1}{p+1}I_n$. Comme $\text{Sp}(A)$ est fini, il existe $N \in \mathbb{N}$, tel que pour tout $p \geq N$, $\frac{1}{p+1} \notin \text{Sp}(A)$. Donc pour tout $p \geq N$, $A_p \in GL_n(\mathbb{K})$, et $A_p \xrightarrow{p \rightarrow +\infty} A$ donc $GL_n(\mathbb{K})$ est dense dans $\mathcal{M}_n(\mathbb{K})$.
2. On fixe $B \in \mathcal{M}_n(\mathbb{K})$. Soit $A \in GL_n(\mathbb{K})$. On écrit $BA = A^{-1}(AB)A$ donc AB et BA sont semblables donc $\chi_{AB} = \chi_{BA}$. Comme, à B fixé, $A \mapsto \chi_{AB}$ et $A \mapsto \chi_{BA}$ sont continues sur $\mathcal{M}_n(\mathbb{K})$, on a le résultat par densité.

Solution 6.14.

1. On a $v_p \circ (id_E - u) = (id_E - u) \circ v_p = \frac{1}{p}(id_E - u^p)$, donc $\|v_p \circ (id_E - u)\| \leq \frac{1}{p}(\|id_E\| + \|u^p\|) \xrightarrow{p \rightarrow +\infty} 0$.

Soit $x \in \ker(u - id_E) \cap \text{Im}(u - id_E)$, on a $u(x) = x$ et il existe $y \in E$, $x = (u - id_E)(y)$.

On a $v_p(x) = \frac{1}{p}(px) = x$ et $v_p(x) = v_p \circ (u - id_E)(y) \xrightarrow{p \rightarrow +\infty} 0$ d'où $x = 0$. Le théorème du rang permet de conclure.

2. Soit $x \in E$, on écrit $x = x_1 + x_2$ avec $\Pi(x) = x_1$ et $x_2 = (u - id_E)(y_2)$. Alors $v_p(x) = x_1 + v_p \circ (u - id_E)(y_2) \xrightarrow{p \rightarrow +\infty} x_1 = \Pi(x)$.

Solution 6.15.

1. Pour tout $x \in A$, $f_n(x) \in A$ car A est convexe. Soit $(x, y) \in A^2$, on a

$$\|f_n(x) - f_n(y)\| = \left(1 - \frac{1}{n}\right)\|f(x) - f(y)\| \leq \left(1 - \frac{1}{n}\right)\|x - y\|$$

Donc f_n est $(1 - \frac{1}{n})$ -lipschitzienne. On forme

$$\begin{aligned} g_n : A &\rightarrow \mathbb{R} \\ x &\mapsto \|f_n(x) - x\| \end{aligned}$$

qui est continue. Soit $x_n \in A$ telle que $g_n(x_n) = \min_{x \in A} g_n(x)$ (existe car A est compact et g_n continue). On a $x_n \in A$, d'où $f_n(x_n) \in A$ et

$$g_n(f_n(x_n)) = \|f_n(f_n(x_n)) - f_n(x_n)\| \leq \left(1 - \frac{1}{n}\right)\|f_n(x_n) - x_n\| = \left(1 - \frac{1}{n}\right)g_n(x_n)$$

Si $g_n(x_n) \neq 0$, alors on aurait $g_n(f_n(x_n)) < g_n(x_n)$ ce qui n'est pas possible. Donc $g_n(x_n) = 0$ et $f_n(x_n) = x_n$.

Soit y_n un autre point fixe, on a

$$\|f_n(x_n) - f_n(y_n)\| = \|x_n - y_n\| \leq \left(1 - \frac{1}{n}\right)\|x_n - y_n\|$$

donc $x_n = y_n$.

2. On a $(x_n)_{n \in \mathbb{N}} \in A^{\mathbb{N}}$ et on extrait (car A est compact) et on a

$$x_{\sigma(n)} \xrightarrow{n \rightarrow +\infty} x \in A$$

On a

$$f_{\sigma(n)}(x_{\sigma(n)}) = x_{\sigma(n)} = \underbrace{\frac{1}{\sigma(n)}f(x_0)}_{\xrightarrow{n \rightarrow +\infty} 0} + \underbrace{\left(1 - \frac{1}{\sigma(n)}\right)f(x_{\sigma(n)})}_{\xrightarrow{n \rightarrow +\infty} f(x)}$$

par continuité de f . Donc $f(x) = x$.

3. Soit $(x, y) \in A^2$, points fixes de f , et $t \in [0, 1]$, on pose $z = tx + (1 - t)y$. On a

$$\begin{aligned} \|x - y\| &= \|f(x) - f(y)\| \\ &\leq \|f(x) - f(z)\| + \|f(z) - f(y)\| \\ &\leq \|x - z\| + \|z - y\| \\ &= (1 - t)\|x - y\| + t\|x - y\| \\ &= \|x - y\| \end{aligned}$$

On a donc égalité partout : $\|f(x) - f(y)\| = \|f(x) - f(z)\| + \|f(z) - f(y)\|$ et $\|f(x) - f(z)\| = \|x - z\|$, $\|f(z) - f(y)\| = \|z - y\|$ car f est 1-lipschitzienne.

Comme la norme est euclidienne, il existe $\lambda \in \mathbb{R}_+$ tel que $f(x) - f(z) = \lambda(f(z) - f(y))$ d'où $f(x) + \lambda f(y) = (\lambda + 1)f(z)$ d'où $f(z) = \frac{x + \lambda y}{\lambda + 1} = t'x + (1 - t')y$ avec $t' = \frac{1}{\lambda + 1} \in [0, 1]$.

En reportant, on a

$$\|f(x) - f(z)\| = \|x - t'x - (1 - t')y\| = (1 - t')\|x - y\| = \|x - z\| = (1 - t)\|x - y\|$$

Si $x \neq y$, alors $t = t'$ et $f(z) = tx + (1 - t)y = z$.

4. Soit dans \mathbb{R}^2 , $\overline{B_{\|\cdot\|}(0, 1)} = [-1, 1]^2 = A$. Soit

$$\begin{aligned} f : A &\rightarrow A \\ (x, y) &\mapsto (x, |x|) \end{aligned}$$

On a

$$\begin{aligned} \|f(x_1, y_1) - f(x_2, y_2)\|_\infty &= \|(x_1, |x_1|)(x_2, |x_2|)\|_\infty \\ &= \max\{|x_1 - x_2|, ||x_1| - |x_2||\} \\ &= |x_1 - x_2| \\ &\leq \|(x_1, y_1) - (x_2, y_2)\|_\infty \end{aligned}$$

Donc f est 1-lipschitzienne, on a $f(x, y) = (y, x)$ si et seulement si $y = |x|$. Donc ici, F n'est pas convexe.

Solution 6.16.

1. On a pour tout $(x, y) \in E^2$, $f(x + y) = f(x) + f(y)$ et par récurrence, pour tout $n \in \mathbb{Z}$, $f(nx) = nf(x)$. Pour $r = \frac{p}{q} \in \mathbb{Q}$, on a $f(qrx) = qf(rx) = f(px) = pf(x)$ donc $f(rx) = rf(x)$. Par densité de \mathbb{Q} dans \mathbb{R} et continuité de f , on a pour tout $\lambda \in \mathbb{R}$, $f(\lambda x) = \lambda f(x)$. Donc f est linéaire.

Pour $\mathbb{K} = \mathbb{C}$, cela ne marche pas. Contre-exemple : la conjugaison dans \mathbb{C} .

2. On étudie la série, pour x fixé de terme général

$$\|v_{n+1}(x) - v_n(x)\| = \frac{1}{2^n} \|f(2^{n+1}x) - 2f(2^n x)\| \leq \frac{M}{2^{n+1}}$$

qui est donc convergente. Donc $(v_n)_{n \in \mathbb{N}}$ converge.

3. On a $v_0(x) = f(x)$, donc $\sum_{n=0}^{+\infty} v_{n+1}(x) - v_n(x) = g(x) - f(x)$. f étant continue, v_n l'est aussi, et pour tout $n \in \mathbb{N}$, comme pour tout $x \in E$, $\|(v_{n+1} - v_n)(x)\| \leq \frac{M}{2^{n+1}}$, donc g est continue.

4. On a, pour tout $(x, y) \in E^2$,

$$\|v_n(x + y) - v_n(x) - v_n(y)\| = \left\| \frac{1}{2^n} f(2^n(x + y)) - \frac{1}{2^n} (f(2^n x) + f(2^n y)) \right\| \leq \frac{M}{2^n}$$

Donc quand $n \rightarrow +\infty$, $g(x + y) = g(x) + g(y)$.

On a pour tout $x \in E$,

$$\|g(x) - f(x)\| = \left\| \sum_{n=0}^{+\infty} v_{n+1}(x) - v_n(x) \right\| \leq \sum_{n=0}^{+\infty} \|v_{n+1}(x) - v_n(x)\| \leq \sum_{n=0}^{\infty} \frac{M}{2^n} = M$$

Soit maintenant h linéaire continue telle que $h - f$ soit bornée, soit $M' = \sup_{x \in E} \|h(x) - f(x)\|$. On a donc

$$\|v_n(x) - h(x)\| = \left\| \frac{1}{2^n} f(2^n x) - \frac{1}{2^n} h(2^n x) \right\| \leq \frac{M'}{2^n}$$

car h est linéaire. Donc quand $n \rightarrow +\infty$, $g(x) = h(x)$ car $\lim_{n \rightarrow +\infty} v_n(x) = g(x)$.

Solution 6.17. En particulier, pour $t = f(0)$, $f^{-1}(\{f(0)\}) = \{x \in E \mid f(x) = f(0)\}$ est borné (car compact). Donc il existe A tel que $f^{-1}(\{f(0)\}) \subset \overline{B(0, A)}$. Par contraposée, pour tout $x \in E$, si $\|x\| > A$, alors $f(x) \neq f(0)$.

On montre alors que $E \setminus \overline{B(0, A)}$ est connexe par arcs (faire le tour de la boule par l'extérieur).

f étant continue, d'après le théorème des valeurs intermédiaires, on a soit pour tout $x \in E \setminus \overline{B(0, A)}$, $f(x) > f(0)$ soit $f(x) < f(0)$. Quitte à remplacer f par $-f$, on se place dans le cas $f(x) > f(0)$. Comme on est en dimension finie sur $\overline{B(0, A)}$ compact, f atteint son minimum et ce minimum est plus petit que $f(0)$, c'est donc un minimum global.

Remarque 6.6. C'est faux pour $n = 1$. Contre-exemple : $f = id_{\mathbb{R}}$.

Solution 6.18. Si c'était le cas, on prend un cercle \mathcal{C} compact (et connexe par arcs). $f(\mathcal{C})$ est compact connexe par arc dans \mathbb{R} . On note $f(\mathcal{C}) = [a, b]$ (avec $a < b$ car f injective). Si $x \in \mathcal{C}$ est tel que $f(x) = \frac{a+b}{2}$, on $\underbrace{f(\mathcal{C} \setminus \{x\})}_{\text{connexe par arc}} = \underbrace{[a, b] \setminus \left\{ \frac{a+b}{2} \right\}}_{\text{pas connexe par arc}}$ donc une telle fonction n'existe pas.

Solution 6.19.

1. Pour tout $n \in \mathbb{N}$, $\|e_n\|_{l^1} = 1$ et $|K_n| = |\varphi(e_n)| \leq \|\varphi\|$ donc $(K_n)_{n \in \mathbb{N}}$ est bornée. On note $M = \sup |K_n| \leq \|\varphi\|$.

Soit maintenant $u = (u_n)_{n \in \mathbb{N}} \in l^1$. On a, pour $N \in \mathbb{N}$,

$$\left\| u - \sum_{n=0}^N u_n e_n \right\|_1 \leq \sum_{n=N+1}^{\infty} |u_n| \xrightarrow{N \rightarrow +\infty} 0$$

(reste d'une série convergente). Par continuité de φ , on a donc

$$|\varphi(u)| \leq \sum_{n=0}^{\infty} |u_n| |K_n| \leq M \|u\|_1$$

Ainsi, $\|\varphi\| \leq M$ et donc $\|\varphi\| = M$.

2. F est linéaire et une isométrie d'après la question précédente, donc injective.

Soit $(K_n)_{n \in \mathbb{N}} \in l^\infty$. On définit

$$\begin{aligned} \varphi : l^1 &\rightarrow \mathbb{R} \\ u = (u_n)_{n \in \mathbb{N}} &\mapsto \sum_{n=0}^{\infty} u_n K_n \end{aligned}$$

Elle est bien définie car $\sum_{n=0}^{+\infty} |u_n| < +\infty$ et $(K_n)_{n \in \mathbb{N}}$ est bornée. Elle est linéaire, et continue car $|\varphi(u)| \leq \|(K_n)_{n \in \mathbb{N}}\|_\infty \|u\|_1$.

Enfin, pour tout $n \in \mathbb{N}$, $\varphi(e_n) = K_n$. Donc $F(\varphi) = (K_n)_{n \in \mathbb{N}}$ et F est surjective. Donc F est une isométrie bijective et le dual topologique de l^1 est équivalent à l^∞ .

Solution 6.20.

1. Soit φ une forme linéaire non nulle telle que $K = \ker(\varphi)$. Si F est dense, φ est discontinue. Soit $(a, b) \in (E \setminus H)^2$ et $(x_n)_{n \in \mathbb{N}} \in H^{\mathbb{N}}$ qui converge vers $b - a$ (existe car H est dense). La suite $(a + x_n)_{n \in \mathbb{N}}$ converge vers b . Pour $n \in \mathbb{N}$, on a $\varphi(a + x_n) = \varphi(a) \neq 0$, et pour $t \in [0, 1]$, $\varphi(t(a + x_n) + (1 - t)(a + x_{n+1})) = \varphi(a) \neq 0$. Donc $[a + x_n, a + x_{n+1}] \subset E \setminus H$. Soit $\gamma : [0, 1] \rightarrow E \setminus H$ telle que

$$\begin{cases} \gamma(t) = \alpha_n t + \beta_n \in [a + x_n, a + x_{n+1}] \subset E \setminus H & \text{si } t \in [1 - \frac{1}{n}, 1 - \frac{1}{n+1}] \\ \gamma(1) = b \\ \gamma(t) = a + tx_0 & \text{si } t \in [0, \frac{1}{2}] \end{cases}$$

On cherche à définir α_n et β_n : on veut $\gamma(1 - \frac{1}{n}) = a + x_n$ et $\gamma(1 - \frac{1}{n+1}) = a + x_{n+1}$ (pour la continuité en se raccordant au x_n). En résolvant le système, on trouve $\alpha_n = n(n+1)(x_n - x_{n+1})$ et $\beta_n = a + x_n - (n-1)(n+1)(x_n - x_{n+1})$.

Soit alors $\varepsilon > 0$, il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$: $\|x_n + a - b\| < \varepsilon$ et pour tout $n \geq N$, pour tout $t \in [1 - \frac{1}{n}, 1 - \frac{1}{n+1}]$, $\gamma(t) \in [a + x_n, a + x_{n+1}] \subset B(b, \varepsilon)$ par convexité de la boule. Donc $\lim_{t \rightarrow 1} \gamma(t) = b$ et γ est continue. Donc $E \setminus H$ est connexe par arcs.

2. Soit φ une forme linéaire telle que $\ker(f) = H$ est fermé. Alors φ est continue (à redémontrer). Soit $x \in E \setminus H$, on a $\varphi(x)\varphi(-x) < 0$ et d'après le théorème des valeurs intermédiaires, si $E \setminus H$ était connexe par arcs, φ s'annulerait sur $E \setminus H$ ce qui n'est pas vrai. Donc $E \setminus H$ n'est pas connexe par arcs.

3. Si $\mathbb{K} = \mathbb{C}$, si H est dense alors $E \setminus H$ est connexe par arc d'après la première question. Si H est fermé, soit φ une forme linéaire continue telle que $\ker(f) = H$. Soit $(x_1, x_2) \in (E \setminus H)^2$.

— Si $\frac{\varphi(x_1)}{\varphi(x_2)} \notin \mathbb{R}_+^*$, alors pour tout $t \in [0, 1]$, $\varphi(\underbrace{tx_1 + (1-t)x_2}_{\in E \setminus H}) \neq 0$ et on peut relier directement x_1 et x_2 .

— Sinon, il existe $\theta \in \mathbb{R}$, $(\rho, \rho') \in (\mathbb{R}_+^*)^2$ avec $\varphi(x_1) = \rho e^{i\theta}$ et $\varphi(x_2) = \rho' e^{i(\theta+\pi)}$. Alors $x_3 = ix_1$ est tel que $[x_1, x_3] \subset E \setminus H$ et $[x_2, x_3] \subset E \setminus H$ (on contourne l'origine par une rotation de l'angle $\frac{\pi}{2}$). Par conséquent, on peut utiliser x_3 pour relier x_1 et x_2 donc $E \setminus H$ est connexe par arcs.

Solution 6.21. Soit

$$\begin{aligned}\varphi: \mathbb{R}_+^* &\rightarrow \mathbb{R} \\ x &\mapsto ((x, \sin(\frac{1}{x})))\end{aligned}$$

φ est continue et $\Gamma \cup \varphi(\mathbb{R}_+^*)$ est connexe par arcs.

On a $\bar{\Gamma} = \Gamma \cup \Gamma'$ avec $\Gamma' = \{(0, y) \mid y \in [-1, 1]\}$. En effet, pour tout $y \in [-1, 1]$, on pose $x_k = \frac{1}{\arcsin(y) + 2k\pi}$. On a $\sin(\frac{1}{x_k}) = y \xrightarrow[k \rightarrow +\infty]{} y$ donc $(0, y) = \lim_{k \rightarrow +\infty} (x_k, \sin(\frac{1}{x_k})) \in \bar{\Gamma}$.

Réciproquement, si $(x, y) \in \bar{\Gamma}$, il existe $(x_k) \in (\mathbb{R}_+^*)^{\mathbb{N}}$ avec $x = \lim_{k \rightarrow +\infty} x_k$ et $y = \lim_{k \rightarrow +\infty} \sin(\frac{1}{x_k})$. Si $x > 0$, par continuité, $y = \sin(\frac{1}{x})$ et $(x, y) \in \Gamma$. Si $x = 0$, $y \in [-1, 1]$ donc $(x, y) \in \Gamma'$.

Si $\bar{\Gamma}$ est connexe par arcs, il existe

$$\begin{aligned}\gamma: [0, 1] &\rightarrow \bar{\Gamma} \\ t &\mapsto (x(t), y(t))\end{aligned}$$

continue telle que $\gamma(0) = (0, 0)$ et $\gamma(1) = (\frac{1}{\pi}, 0)$. La première projection $t \mapsto x(t)$ est continue avec $x(0) = 0$ et $x(1) = \frac{1}{\pi}$. On définit maintenant $t_1 = \sup\{t \in [0, 1] \mid x(t) = 0\}$. Par continuité, $x(t_1) = 0$ et donc $t_1 < 1$. Donc pour tout $t > t_1$, $x(t) > 0$ et $\gamma(t) = (x(t), \sin(\frac{1}{x(t)}))$ pour $t > t_1$ et $\gamma(t_1) = (0, y_1)$ avec $y_1 \in [-1, 1]$.

Or, -1 et 1 n'appartiennent pas simultanément à $]y_1 - \frac{1}{2}, y_1 + \frac{1}{2}[$. On peut supposer que $1 \notin]y_1 - \frac{1}{2}, y_1 + \frac{1}{2}[$. Comme γ est continue, il existe $t_2 > t_1$ tel que pour tout $t \in]t_1, t_2]$, $\sin(\frac{1}{x(t)}) \in]y_1 - \frac{1}{2}, y_1 + \frac{1}{2}[$. Or $x(t_2) > 0$ et $x(t_1) = 0$ donc il existe $k \in \mathbb{N}^*$, $t_0 \in]t_1, t_2]$ tel que $x(t_0) = \frac{1}{2k\pi + \frac{\pi}{2}}$ (théorème des valeurs intermédiaires). Mais alors $\sin(\frac{1}{x(t_0)}) = 1 \notin]y_1 - \frac{1}{2}, y_1 + \frac{1}{2}[$ ce qui contredit ce qui précède.

Donc $\bar{\Gamma}$ n'est pas connexe par arcs.

Solution 6.22.

1. Pour tout $n \in \mathbb{N}$, $u_n \in K$ car u_n est le barycentre de $(a, T(a), \dots, T^n(a))$ et K est convexe. Comme K est compact, on peut extraire $u_{\sigma(n)} \xrightarrow[n \rightarrow +\infty]{} u \in K$. Alors

$$(id_E - T)(u_{\sigma(n)}) = \frac{1}{\sigma(n) + 1} (id_E - T^{\sigma(n)+1})(a)$$

d'où

$$\|(id_E - T)(u_{\sigma(n)})\| \leq \frac{1}{\sigma(n) + 1} \times 2M \xrightarrow{n \rightarrow +\infty} 0$$

avec $M = \sup_{x \in K} \|x\|$ (existe car K est compact donc borné). Par continuité de T , on a $T(u) = u$.

2. Posons $F' = \{u \in K \mid T(u) = u\}$ fermé car $K' = K \cap \left(\underbrace{(id_E - T)^{-1}\{0\}}_{\text{continu}} \right)$. Donc K' est compact et non vide d'après la première question. De plus, pour tout $(u_1, u_2) \in K'^2$, pour tout $t \in [0, 1]$, par linéarité de T , on a

$$T(tu_1 + (1 - t)u_2) = tu_1 + (1 - t)u_2$$

donc K' convexe. De plus, comme $U \circ T = T \circ U$, pour tout $u \in K'$, on a $T(U(u)) = U(T(u)) = U(u)$ donc $U(u) \in K'$. On applique alors la question 1 à K' est il existe $y \in K' : U(y) = y$ et $T(y) = y$.

Solution 6.23.

1. C'est le théorème du rang car $\text{rg}(u) \leq n \leq p - 2$, et $H = \{(\alpha_1, \dots, \alpha_p) \mid \sum_{i=1}^p \alpha_i = 0\}$ est de dimension $p - 1$ donc $H \cap \ker(u) \neq \{0\}$ (formule de Grassmann).
2. On a

$$\sum_{i=1}^p (\lambda_i + t\alpha_i)x_i = \sum_{i=1}^p \lambda_i x_i + t \sum_{i=1}^p \alpha_i x_i = x$$

et

$$\sum_{i=1}^p (\lambda_i + t\alpha_i) = \sum_{i=1}^p \lambda_i + t \sum_{i=1}^p \alpha_i = 1$$

Soit $I_+ = \{i \in \{1, \dots, p\} \mid \alpha_i > 0\}$ et $I_- = \{i \in \{1, \dots, p\} \mid \alpha_i < 0\}$. On a $I_+ \neq \emptyset$ et $I_- \neq \emptyset$ car $\sum_{i=1}^p \alpha_i = 0$ et $(\alpha_1, \dots, \alpha_p) \neq (0, \dots, 0)$. Soit $t \geq 0$. Pour tout $i \in I_+$, $\lambda_i + t\alpha_i \geq 0$. Pour $i \in I_-$, $\lambda_i + t \underbrace{\alpha_i}_{<0} \geq 0$ si et seulement si $t \leq -\frac{\lambda_i}{\alpha_i}$. Prenons alors

$$t = \min_{i \in I_-} \left(-\frac{\lambda_i}{\alpha_i} \right)$$

On a aussi pour tout $i \in I_-$, $\lambda_i + t\alpha_i \geq 0$ et il existe $i_0 \in I_-$ tel que $\lambda_{i_0} + t\alpha_{i_0} = 0$.

3. Par récurrence descendante, on se ramène à $n+1$ points car si x est barycentre de p points avec $p \geq n + 2$, alors il est barycentre de $p - 1$ points.

4. Soit $A = \{(\lambda_1, \dots, \lambda_{n+1}) \in \mathbb{R}_+^{n+1} \mid \sum_{i=1}^{n+1} \lambda_i = 1\}$ fermé et borné en dimension finie donc compact. Soit

$$\begin{aligned} f : \quad A \times K^{n+1} &\rightarrow \operatorname{conv}(K) \\ ((\lambda_1, \dots, \lambda_n), (x_1, \dots, x_{n+1})) &\mapsto \sum_{i=1}^{n+1} \lambda_i x_i \end{aligned}$$

f est surjective et continue, donc $\operatorname{conv}(K)$ est l'image continue d'un compact donc $\operatorname{conv}(K)$ est compact.

Solution 6.24. Pour tout $u \in A_p$, $\operatorname{Sp}(u) \subset \{\alpha_1, \dots, \alpha_r\}$ distincts et u est diagonalisable. Réciproquement, si u est diagonalisable et $\operatorname{Sp}(u) \subset \{\alpha_1, \dots, \alpha_r\}$ alors dans une base la matrice de u est diagonale avec des α_i (éventuellement plusieurs selon leur multiplicités), donc $u \in A_p$.

Si $u \in A_p$, on écrit donc le polynôme caractéristique de u

$$\chi_u = \prod_{i=1}^r (X - \alpha_i)^{m_i}$$

avec $0 \leq m_i \leq \dim(E) = n$ et $\sum_{i=1}^r m_i = n$. $u \mapsto \chi_u$ est continue. Pour $(m_1, \dots, m_r) \in \{0, \dots, n\}^r$ tel que $\sum_{i=1}^r m_i = n$, notons

$$A_{m_1, \dots, m_r} = \left\{ u \in A_p \mid \chi_u = \prod_{i=1}^r (X - \alpha_i)^{m_i} \right\}$$

et

$$\left[u \mapsto \chi_u(A_p) \right] = \left\{ \bigcup_{(m_1, \dots, m_r) \in D_{n,r}} \left\{ \prod_{i=1}^r (X - \alpha_i)^{m_i} \right\} \right\}$$

où

$$D_{n,r} = \left\{ (m_1, \dots, m_r) \in \{0, \dots, n\}^r \mid \sum_{i=1}^r m_i = n \right\}$$

Donc d'après la contraposée du théorème des valeurs intermédiaires,

si $(m_1, \dots, m_r) \neq (m'_1, \dots, m'_r)$, alors A_{m_1, \dots, m_r} et $A_{m'_1, \dots, m'_r}$ ne sont pas dans la même composante connexe par arcs car

$$\left[u \mapsto \chi_u \left(A_{m_1, \dots, m_r} \cup A_{m'_1, \dots, m'_r} \right) \right] = \underbrace{\left\{ \prod_{i=1}^r (X - \alpha_i)^{m_i} \right\} \cup \left\{ \prod_{i=1}^r (X - \alpha_i)^{m'_i} \right\}}_{\text{pas connexe par arcs}}$$

Si $\gamma: [0, 1] \rightarrow A_p$ est continue, $t \mapsto \chi_{\gamma(t)} = a_0(t) + a_1(t)X + \cdots + a_{n-1}(t)X^{n-1} + X^n$ est continue sur $[0, 1]$ et prend un nombre fini de valeurs donc est constante. $a_i: [0, 1] \rightarrow \mathbb{R}$ continues et prend un nombre fini de valeurs donc est constante.

Soit $u_0 \in A_{m_1, \dots, m_r}$, soit $u \in A_{m_1, \dots, m_r}$, alors il existe une base \mathcal{B}_0 base de E telle que $\text{mat}_{\mathcal{B}_0}(u_0) = M_0$ soit diagonale avec des α_1 sur les m_1 premières lignes de la diagonale, α_2 sur les m_2 lignes suivantes, etc. Soit $M = \text{mat}_{\mathcal{B}_0}(u)$. M est semblable à M_0 donc il existe $P \in GL_n(\mathbb{C})$ telle que $M = PM_0P^{-1}$.

Or $GL_n(\mathbb{C})$ est connexe par arcs, donc il existe $\varphi: [0, 1] \rightarrow GL_n(\mathbb{C})$ continue telle que $\varphi(0) = P$ et $\varphi(1) = I_n$. On pose alors

$$\begin{aligned} \Phi: [0, 1] &\rightarrow A_{m_1, \dots, m_r} \\ t &\mapsto \varphi(t)M_0\varphi^{-1}(t) \end{aligned}$$

Alors A_{m_1, \dots, m_r} est connexe par arcs.

Le nombre de composantes est donc égal au cardinal de

$$D_{n,r} = \{(m_1, \dots, m_r) \in \{0, \dots, n\}^r \mid \sum_{i=1}^r m_i = n\}$$

qui vaut $\binom{m+r-1}{r-1}$ possibilités (place n points sur une droite et les séparer avec $r-1$ barres : le nombre de points dans chaque segment donne un m_i , il y a $m+r-1$ possibilités pour placer les $r-1$ barres).

Solution 6.25.

1. Pour tout $i \in \{1, \dots, n\}$, $|AX|_i = \sum_{j=1}^n \underbrace{a_{i,j}x_j}_{>0} \geq 0$. Si $|AX|_i = 0$ alors pour tout $j \in \{1, \dots, n\}$, $\underbrace{a_{i,j}}_{>0} x_j = 0$ donc $x_j = 0$, impossible car $X \neq 0$.
2. Si $|AX| = A|X|$. On a pour tout $i \in \{1, \dots, n\}$,

$$\left| \sum_{j=1}^n a_{i,j}x_j \right| = \sum_{j=1}^n a_{i,j}|x_j|$$

donc les $(a_{i,j}x_j)_{1 \leq j \leq n}$ ont tous même argument. On prend $\theta = \arg(x_j)$.

3. K est fermé et borné en dimension finie : c'est un compact. On a $I_x \neq \emptyset$ car $AX \geq 0$ donc $0 \in I_x$. Soit $(t_n)_{n \in \mathbb{N}} \in I_x^{\mathbb{N}}$ convergeant vers $t \in \mathbb{R}$. Pour tout $k \in \mathbb{N}$, $AX - t_k X \geq 0$

donc pour tout $i \in \{1, \dots, n\}$, $(AX - t_k X)_i \geq 0$ et par passage à la limite, $AX - tX \geq 0$
donc I_x est fermé.

Si $t \in I_x$,

$$|tX|_1 = t = \sum_{i=1}^n t \underbrace{x_i}_{\geq 0} \leq \sum_{i=1}^n \underbrace{\sum_{j=1}^n a_{i,j} x_j}_{=(AX)_i} \leq n \max_{1 \leq i, j \leq n} |a_{i,j}|$$

car $\sum_{j=1}^n x_j = 1$. On note $M = n \max_{1 \leq i, j \leq n} |a_{i,j}|$.

4. Pour tout $x \in K$, $\theta(X) \leq M$ donc θ est bien borné sur K . Par définition de r_0 , il existe $(X_k)_{k \in \mathbb{N}} \in K^{\mathbb{N}}$ tel que $\lim_{k \rightarrow +\infty} \theta(X_k) = r_0$. On note $\theta(X_k) = t_k$. Comme K est compact, il existe $\sigma: \mathbb{N} \rightarrow \mathbb{N}$ strictement croissante telle que $X_{\sigma(k)}$ converge vers $X^+ \in K$. A priori, $\theta(X^+) \leq r_0$. On a $AX_{\sigma(k)} - t_{\sigma(k)} X_{\sigma(k)} \geq 0$ pour tout $k \in \mathbb{N}$ donc par passage à la limite, $AX^+ - r_0 X^+ \geq 0$ et donc $r_0 \leq \theta(X^+)$ donc $r_0 = \theta(X^+)$.

5. Soit $Y = A^+ - r_0 X^+ \geq 0$. Si $Y \neq 0$, alors $AY > 0$ d'après la question 1 donc

$$AY = A \underbrace{(AX^+)}_{>0} - r_0 \underbrace{(AX^+)}_{>0} > 0$$

On a $AY > \varepsilon AX^+$ si et seulement si pour tout $i \in \{1, \dots, n\}$, $|AY|_i > \varepsilon |AX^+|_i$ (car $AY > 0$). On pose alors

$$\varepsilon = \frac{1}{2} \min_{1 \leq i \leq n} \frac{|AY|_i}{|AX^+|_i}$$

On a alors $AY - \varepsilon AX^+ > 0$ d'où

$$A \underbrace{\frac{AX^+}{\|AX^+\|_1}}_{\in K} - (r_0 + \varepsilon) \frac{AX^+}{\|AX^+\|_1} > 0$$

donc $r_0 + \varepsilon \in I_{\frac{AX^+}{\|AX^+\|_1}}$ c'est-à-dire

$$r_0 + \varepsilon \leq \theta\left(\frac{AX^+}{\|AX^+\|_1}\right) \leq r_0$$

ce qui est impossible. Nécessairement $Y = 0$.

6. Pour tout $i \in \{1, \dots, n\}$, on a

$$|AV|_i = \left| \sum_{j=1}^n a_{i,j} v_j \right| \leq \sum_{j=1}^n |a_{i,j}| |v_j| = (A|V|)_i$$

donc $|\lambda| = |AV| \leq A|V|$. De plus, $|V| \in K$ donc $|\lambda| \leq \theta(|V|) \leq r_0$. Notons que cela implique que le rayon spectral de A est $\rho(A)$ est plus petit que r_0 et que l'on a même égalité.

7. Si $|\lambda| = r_0$, on a $|\lambda| = \theta(|V|) = r_0$ et d'après la question 5 on a $A|V| = r_0|V| = |AV|$.

D'après la question 2, il existe $\theta \in \mathbb{R}$ tel que $V = e^{i\theta}|V|$. Or

$$AV = \lambda V = e^{i\theta}A|V| = e^{i\theta}r_0|V|$$

et comme $|K| \in K$, $|V| \neq 0$ et on a donc $\lambda = r_0$.

8. Soit $V \in \mathcal{M}_{n,1}(\mathbb{C})$ tel que $\|V\|_1 = 1$ et $AV = r_0V$. D'après la question précédente, on a $V = e^{i\theta}|V|$ et $A|V| = r_0|V|$. Soit alors $t \in \mathbb{R}$, on a

$$A(X^+ + t|V|) = r_0(X^+ + t|V|)$$

Notons maintenant que si $Y \geq 0$ avec $Y \neq 0$ vérifie $AY = r_0Y$, alors $Y > 0$. En effet, d'après la première question, $AY > 0$. On a $r_0 \neq 0$ car sinon $\text{Sp}_{\mathbb{C}} = \{0\}$ et $A^n = 0$ ce qui est impossible car ses coefficients sont strictement positifs. D'où $Y > 0$.

Ainsi, par définition de X^+ , on a $X^+ > 0$ et $|V| > 0$. On a alors

$$(X^+)_i + t|v_i| \geq 0$$

si et seulement si

$$t \geq -\frac{|X^+|_i}{|v_i|}$$

On prend

$$t = \min_{1 \leq i \leq n} -\frac{|X^+|_i}{|v_i|}$$

Finalement, on a $X^+ + t|V| \geq 0$ et une de ses coordonnées vaut 0 (car on a pris le minimum sur les i). Nécessairement, $X^+ + t|V| = 0$ (car $A(X^+ + t|V|) = r_0(X^+ + t|V|)$) et donc $|V| \in \mathbb{R}X^+$. Donc $V = e^{i\theta}|V| \in \mathbb{C}X^+$ et ainsi

$$\dim(\ker(A - r_0I_n)) = 1$$

Solution 6.26. Soit

$$\begin{aligned} \varphi : U \times V &\rightarrow \mathbb{R} \\ (x, y) &\mapsto \|x - y\| \end{aligned}$$

On a

$$|\varphi(x, y) - \varphi(x', y')| = ||x - y| - |x' - y'|| \leq |(x - y) - (x' - y')| \leq \|x - x'\| + \|y - y'\| \leq 2\|(x, y) - (x', y')\|_\infty$$

donc φ est continue.

$U \times V$ est compact, donc il existe $(x_1, y_1) \in (U \times V)$ telle que $\varphi(x_1, y_1) = \min_{(x, y) \in U \times V} \varphi(x, y)$.

Comme U et V sont disjoints, $x_1 \neq y_1$ et $\varphi(x_1, y_1)d(U, V) > 0$.

Soit $\alpha = \frac{d(U, V)}{3}$. On pose $U' = \{x \in E \mid d(x, U) < \alpha\}$ et $V' = \{x \in E \mid d(x, V) < \alpha\}$. $x \mapsto \|x\|$ est continue car 1-lipschitzienne donc U' et V' sont des ouverts et on a bien $U \subset U'$ et $V \subset V'$. Soit ensuite $x \in U' \cap V'$, on a $d(x, U) < \alpha$ et $d(x, V) < \alpha$ donc il existe $(u, v) \in U \times V$, $d(x, u) < \alpha$ et $d(x, v) < \alpha$. Alors $d(u, v) \leq 2\alpha$ ce qui est absurde. Donc $U' \cap V' = \emptyset$.

Solution 6.27.

1. f est 1-lipschitzienne donc est continue. On forme

$$\begin{aligned} g : K &\rightarrow \mathbb{R} \\ x &\mapsto \|x - f(x)\| \end{aligned}$$

g est continue, K est compact donc il existe $a \in K$ tel que $g(a) = \min_{x \in K} g(x)$. Si $a \neq f(a)$, alors $\|f(a) - f^2(a)\| = g(f(a)) < \|a - f(a)\| = g(a)$ ce qui est impossible par définition de a . Donc $f(a) = a$. S'il existe $a' \neq a$ tel que $f(a') = a'$, alors $\|f(a) - f(a')\| = \|a - a'\| < \|a - a'\|$ ce qui est impossible. Donc a est unique.

2. S'il existe $n_0 \in \mathbb{N}$ tel que $u_{n_0} = a$ alors pour tout $n \geq n_0$, $u_n = a$ et $\lim_{n \rightarrow +\infty} u_n = a$. Si pour tout $n \in \mathbb{N}$, $u_n \neq a$, alors pour tout $n \in \mathbb{N}$, on a

$$\|u_{n+1} - a\| = \|f(u_n) - f(a)\| < \|u_n - a\|$$

donc la suite $(\|u_n - a\|)_{n \in \mathbb{N}}$ est strictement décroissante dans \mathbb{R}_+ donc elle converge vers $l \geq 0$. Par compacité de K , il existe une extraction σ telle que $\lim_{n \rightarrow +\infty} u_{\sigma(n)} = \alpha \in K$. Par continuité,

$$\lim_{n \rightarrow +\infty} \|u_{\sigma(n)} - a\| = \|\alpha - a\| = l$$

et

$$\lim_{n \rightarrow +\infty} \|\underbrace{u_{\sigma(n)+1}}_{f(u_{\sigma(n)})} - f(a)\| = \|f(\alpha) - f(a)\| = l = \|\alpha - a\|$$

par continuité de f . Ainsi, on a $\alpha = a$ et $l = 0$ donc $\lim_{n \rightarrow +\infty} u_n = a$.

3. f est \mathcal{C}^1 sur \mathbb{R} . Soit $x < y \in \mathbb{R}^2$, il existe $z \in]x, y[$ tel que (égalité des accroissements finis)

$$\left| \frac{f(x) - f(y)}{x - y} \right| = |f'(z)| = \left| \frac{z}{\sqrt{z^2 + 1}} \right| < 1$$

donc f vérifie bien l'hypothèse de contraction. Cependant, pour tout $a \in \mathbb{R}$, on a $\sqrt{a^2 + 1} > a$ donc pas de point fixe. La démonstration tombe en défaut car \mathbb{R} n'est pas compact.

Solution 6.28. La condition est équivalente à pour tout $(M_1, M_2, M_3) \in K_1 \times K_2 \times K_3$, M_1, M_2 et M_3 ne sont pas alignés.

On forme alors

$$\begin{aligned} f : K_1 \times K_2 \times K_3 &\rightarrow \mathbb{R}_+ \\ (M_1, M_2, M_3) &\mapsto R(M_1, M_2, M_3) \end{aligned}$$

où $R(M_1, M_2, M_3)$ est le rayon du cercle circonscrit au triangle formé par M_1, M_2 et M_3 .

On note $M_i = (x_i, y_i)$ et Δ_i la médiatrice de $[M_j M_k]$. Établissons une équation de Δ_i . On a $M = (x, y) \in \Delta_i$ si et seulement si $\|M \vec{M}_j\|_2^2 = \|M \vec{M}_k\|_2^2$ si et seulement si $(M \vec{M}_j + M \vec{M}_k \mid M \vec{M}_j - M \vec{M}_k) = 0$ (produit scalaire), si et seulement si $(M \vec{C}_i \mid M_j \vec{M}_k) = 0$ où C_i est le milieu de $[M_j M_k]$, si et seulement si (calculer le produit scalaire)

$$\left(\frac{x_j + x_k}{2} - x \right) (x_k - x_j) + \left(\frac{y_j + y_k}{2} - y \right) (y_k - y_j) = 0$$

Soit alors $M_0 = (x_0, y_0)$ le centre du cercle circonscrit. $M_0 \in \Delta_i \cap \Delta_j$ avec $i \neq j$. Par exemple, $M_0 \in \Delta_3 \cap \Delta_1$ si et seulement si

$$\begin{cases} \left(\frac{x_2 + x_1}{2} - x_0 \right) (x_2 - x_1) + \left(\frac{y_2 + y_1}{2} - y_0 \right) (y_2 - y_1) = 0 \\ \left(\frac{x_3 + x_2}{2} - x_0 \right) (x_3 - x_2) + \left(\frac{y_3 + y_2}{2} - y_0 \right) (y_3 - y_2) = 0 \end{cases}$$

si et seulement si $(L_2 \leftarrow L_1(x_3 - x_2) + L_2(x_1 - x_2))$

$$\begin{cases} x_0(x_1 - x_2) + y_0(y_1 - y_2) = \frac{x_1^2 - x_2^2 + y_1^2 - y_2^2}{2} \\ x_0(x_2 - x_3) + y_0(y_2 - y_3) = \frac{x_2^2 - x_3^2 + y_2^2 - y_3^2}{2} \end{cases}$$

si et seulement si $(L_1 \leftarrow L_2(y_2 - y_1) + L_1(y_2 - y_3))$

$$\begin{cases} x_0 = \frac{\frac{x_1^2 - x_2^2 + y_1^2 - y_2^2}{2}(y_2 - y_3) - (y_1 - y_2)\frac{x_2^2 - x_3^2 + y_2^2 - y_3^2}{2}}{(x_1 - x_2)(y_2 - y_3) - (x_2 - x_3)(y_1 - y_2)} \\ y_0 = \frac{\frac{x_2^2 - x_3^2 + y_2^2 - y_3^2}{2}(x_1 - x_2) - (x_2 - x_3)\frac{x_1^2 - x_2^2 + y_1^2 - y_2^2}{2}}{(x_1 - x_2)(y_2 - y_3) - (x_2 - x_3)(y_1 - y_2)} \end{cases}$$

et $R(M_1, M_2, M_3) = \sqrt{(x_0 - x_3)^2 + (y_0 - y_3)^2}$. En reportant, f est continue sur $K_1 \times K_2 \times K_3$ compact donc f atteint son minimum.

Solution 6.29.

1. Pour tout $f \in E$, $T(f)$ est \mathcal{C}^1 et $(T(f))' = f$, $T(f)(0) = 0$. T est clairement linéaire, soit ensuite $x \in [0, 1]$, on a

$$|T(f)(x)| = \left| \int_0^x f(t) dt \right| \leq \int_0^x |f(t)| dt \leq x \|f\|_\infty \leq \|f\|_\infty$$

Donc $\|T(f)\|_\infty \leq \|f\|_\infty$ donc T est continue et $\|T\| \leq 1$. Pour $f = 1$, on a $\|f\|_\infty = 1$ et pour tout $x \in [0, 1]$, $T(f)(x) = x$ donc $\|T(1)\|_\infty = 1$. Ainsi, $\|T\| = 1$.

2. $\text{id}_E - T$ est continue. Soit $(f, g) \in E^2$, on a $g = f - T(f)$ si et seulement si $g = y' - y$ et $y(0) = 0$. On a $g(x)e^{-x} = \underbrace{e^{-x}(y'(x) - y(x))}_{(e^{-x}y(x))'}$ donc en intégrant de 0 à x on a

$$y(x) = e^x \int_0^x e^{-t} g(t) dt$$

Donc $T(f)$ vérifie le problème de Cauchy si et seulement si pour tout $x \in \mathbb{R}$, $T(f)(x) = e^x \int_0^x e^{-t} g(t) dt$ si et seulement si pour tout $x \in [0, 1]$,

$$f(x) = g(x) + e^x \int_0^x e^{-t} g(t) dt$$

Donc $\text{id}_E - T$ est bijective. Enfin, on a pour tout $x \in [0, 1]$,

$$|f(x)| \leq |g(x)| + \left| \int_0^x g(t) e^{x-t} dt \right| \leq \|g\|_\infty (1 + x e^x) \leq \|g\|_\infty (1 + e)$$

Ainsi,

$$\|f\|_\infty = \|(\text{id}_E - T)^{-1}(g)\|_\infty \leq \|g\|_\infty (1 + e)$$

donc $(\text{id}_E - T)^{-1}$ est continue. Ainsi, $\text{id}_E - T$ est un homéomorphisme.

Solution 6.30.

(i) \Rightarrow (ii) $f^{-1}(K)$ est fermé car f est continue. K est borné, donc il existe $M > 0$, tel que pour tout $y \in K$, $\|y\| \leq M$. Donc pour tout $x \in f^{-1}(K)$, $\|f(x)\| \leq M$. Par contraposée de (i) pour $A = M + 1$, il existe $B > 0$ tel que $\|f(x)\| < A \Rightarrow \|x\| < B$. Donc pour $x \in f^{-1}(K)$, $\|x\| < B$ donc $f^{-1}(K)$ est borné. C'est donc un compact.

(ii) \Rightarrow (i) Soit $A \geq 0$. Soit $K = \overline{B(0, A)}$ compact car fermé et borné en dimension finie. D'après (ii), $f^{-1}(K)$ est compact donc borné : il existe $B > 0$ tel que pour tout $x \in f^{-1}(K)$, $\|x\| \leq B$. Par contraposée, si $\|x\| > B$ alors $x \notin f^{-1}(K)$ et $f(x) \notin K$ donc $\|f(x)\| > A$. Ainsi, $\lim_{\|x\| \rightarrow +\infty} \|f(x)\| = +\infty$.

Remarque 6.7. Exemple pour l'exercice précédent : les fonctions polynômiales non constantes. Contre-exemple : l'exponentielle, cf $\exp([0, 1]) = \mathbb{R}_+$ non compact.

Solution 6.31.

1. Soit $(x, y) \in K^2$ compact. Soit σ une extraction telle que

$$(f^{\sigma(n)}(x), f^{\sigma(n)}(y)) \xrightarrow{n \rightarrow +\infty} (l, l') \in K^2$$

On a

$$f^{\sigma(n+1)}(x) - f^{\sigma(n)}(x) \xrightarrow{n \rightarrow +\infty} 0$$

de même pour y . Soit $\varepsilon > 0$,

$$\begin{cases} \exists N_1 \in \mathbb{N}, \forall n \geq N_1, \|f^{\sigma(n+1)}(x) - f^{\sigma(n)}(x)\| \leq \varepsilon \\ \exists N_1 \in \mathbb{N}, \forall n \geq N_1, \|f^{\sigma(n+1)}(y) - f^{\sigma(n)}(y)\| \leq \varepsilon \end{cases}$$

Pour $N = \max(N_1, N_2)$ et $p = \sigma(N + 1) - \sigma(N) \in \mathbb{N}^*$, on a

$$d(x, f^p(x)) \leq d(f^{\sigma(n+1)}(x), f^{\sigma(n)}(x)) \leq \varepsilon$$

et de même pour y avec le même p .

2. On a

$$\begin{aligned} d(x, y) &\leq d(f(x), f(y)) \\ &\leq d(f^p(x), f^p(y)) \\ &\leq d(f^p(x), x) + d(x, y) + d(y, f^p(y)) \\ &\leq 2\varepsilon + d(x, y) \end{aligned}$$

Ceci valant pour tout $\varepsilon > 0$, on a égalité tout du long. On a donc notamment, $\|x - y\| = \|f(x) - f(y)\|$ et donc f est une isométrie.

3. f est 1-lipschitzienne donc continue. Donc $f(K)$ est compact donc fermé. Il suffit donc de montrer que $f(K)$ est dense dans K . Soit $x \in K$ et $\varepsilon > 0$, il existe $p \in \mathbb{N}^*$ tel que $\|x - \underbrace{f^p(x)}_{\in f(K)}\| \leq \varepsilon$ d'après la première question. Donc $f(K)$ est dense dans K et $f(K) = \overline{f(K)} = K$.

Remarque 6.8. Exemple pour l'exercice précédent : une rotation sur la sphère unité.

Solution 6.32. Soit

$$f: K \rightarrow \mathbb{R}$$

$$M \mapsto f(M) = \text{rayon du cercle circonscrit au triangle } MAB$$

On a $F = f(K)$. Soit (C, i, j) un repère orthonormé où C est le milieu de $[AB]$ et $A(-\alpha, 0)$ et $B(\alpha, 0)$ avec $\alpha > 0$. La médiatrice Δ de $[A, B]$ a pour équation $x = 0$. Si $M(x, y)$, soit $\varphi(M)$ le centre du cercle circonscrit. On a $\varphi(M) \in \Delta$ donc $\varphi(M)(0, y_1)$ et $\varphi(M)$ appartient à la médiatrice de $[MA]$. On a $y_1 \neq 0$ car $M \notin (AB)$.

Notons M' le milieu de $[MA]$. On a $M'(\frac{x-\alpha}{2}, \frac{y}{2})$ d'où $M'\vec{\varphi}(M) \cdot \vec{MA} = 0$ d'où (en développant le produit scalaire),

$$y_1 = \left((\alpha + x) \left(\frac{\alpha - x}{2} \right) - \frac{y^2}{2} \right) \left(-\frac{1}{y} \right)$$

φ est donc continue donc f également et $f(K) = F$ est compact.

Solution 6.33.

1. Soit $\lambda \in \text{Sp}(\tau)$ et $P \in \mathbb{R}[X] \setminus \{0\}$ avec $\tau(P) = \lambda P$. Si P n'est pas constant, notons $\alpha \in \mathbb{C}$ alors $P(\alpha) = 0$. Alors $P(\alpha + 1) = 0$. En itérant, pour tout $n \in \mathbb{N}$, $P(\alpha + n) = 0$, impossible car P n'est pas constant donc pas nul. Finalement, P est constant et $\lambda = 1$: $\text{Sp}(\tau) = \{1\}$.
2. $f: x \mapsto P(x)e^{-x}$ est continue et $\lim_{x \rightarrow +\infty} f(x) = 0$ donc le sup est bien défini. Il est ensuite facile de vérifier que $\|P\|$ est une norme.
3. On a

$$\|\tau(P)\| = \sup_{x \geq 0} |P(x+1)e^{-x}| = \sup_{x' \geq 1} |P(x')e^{-x'}e| \leq \sup_{x' \geq 0} |P(x')e^{-x'}e| \leq e\|P\|$$

4. Utiliser $P = X$.

Solution 6.34.

1. Pour x fixé, $\min(x, \varphi(t)) = \frac{x + \varphi(t) - |x - \varphi(t)|}{2}$ est continue. Donc $T(f)$ est définie.

Si $x \leq \varphi(0)$,

$$T(f)(x) = \int_0^1 x f(t) dt = x \int_0^1 f(t) dt$$

et si $x \geq \varphi(1)$,

$$T(f)(x) = \int_0^1 \varphi(t) f(t) dt$$

et si $\varphi(0) \leq x \leq \varphi(1)$, il existe un unique $t_1 = \varphi^{-1}(x)$ (car φ induit un homéomorphisme de $[0, 1]$ dans $\varphi([0, 1])$).

Si $t \leq t_1$, on a $\varphi(t) \leq x$, donc $\min(x, \varphi(t)) = \varphi(t)$. Si $t \geq t_1$, on a $\min(x, \varphi(t)) = x$. On a donc

$$\begin{aligned} T(f)(x) &= \int_0^{t_1} \varphi(t) f(t) dt + \int_{t_1}^1 x f(t) dt \\ &= \underbrace{\int_0^{\varphi^{-1}(x)} \varphi(t) f(t) dt}_{=F_1(\varphi^{-1}(x))} + x \underbrace{\int_{\varphi^{-1}(x)}^1 f(t) dt}_{=F_2(\varphi^{-1}(x))} \end{aligned}$$

et f et φ étant continues, F_1 et F_2 sont continues.

Donc $T(f)$ continue et T linéaire, c'est un endomorphisme de E .

2. On a

$$|T(f)(x)| \leq \|f\|_\infty \underbrace{\int_0^1 \min(x, \varphi(t)) dt}_{=A(x)}$$

donc

$$\|T(f)\|_\infty \leq \|f\|_\infty \|A\|_\infty$$

donc T est continue et $\|T\| \leq \|A\|_\infty$. De plus pour $f = 1$, on a $\|T\| = \|A\|_\infty$.

3. On a

$$A(x) = \int_0^1 \min(x, \varphi(t)) dt = \begin{cases} x & \text{si } x \leq \varphi(0) \\ \int_0^1 \varphi(t) dt & \text{si } x \geq \varphi(1) \end{cases}$$

Dans tous les cas,

$$\|A\|_\infty \leq \int_0^1 \varphi(t) dt$$

donc

$$\|A\|_\infty = \int_0^1 \varphi(t) dt$$

Solution 6.35.

1. φ est une forme linéaire. et on a

$$|\varphi(P)| \leq \sum_{k \in \mathbb{N}} \left| \frac{a_k}{2^k} \right| \leq 2\|P\|_\infty$$

donc φ est continue et $\|\varphi\| \leq 2$. Pour $p \neq 0$, $|\varphi(P)| < 2\|P\|_\infty$: pour avoir égalité, il faudrait pour tout $k \in \mathbb{N}$, $a_k = \text{constante} \neq 0$ ce qui n'est pas possible. Pour $P_n = \sum_{k=0}^n X^k$, on a $\|P_n\|_\infty = 1$ et $\lim_{n \rightarrow +\infty} |\varphi(P_n)| \xrightarrow{n \rightarrow +\infty} 2$ donc $\|\varphi\| = 2$. De plus, $\ker(\varphi) = \varphi^{-1}(\{0\})$ est fermé.

2. Soit $P = \sum_{k \in \mathbb{N}} a_k X^k \in \ker(\varphi)$. On a $\varphi(P) = 0$ d'où $a_0 = -\sum_{k=1}^{+\infty} \frac{a_k}{2^k}$ (et il existe $N_0 \in \mathbb{N}, \forall n \geq N_0, a_n = 0$). On a donc

$$P(X) - 1 = (a_0 - 1) + \sum_{k \in \mathbb{N}^*} a_k X^k$$

et si $\|P - 1\|_\infty \leq \frac{1}{2}$, on a

$$\begin{cases} |a_0 - 1| \leq \frac{1}{2} \\ \forall k \in \mathbb{N}^*, |a_k| \leq \frac{1}{2} \end{cases}$$

et

$$|a_0| = \left| \sum_{k=1}^{+\infty} \frac{a_k}{2^k} \right| \leq \sum_{k=1}^{+\infty} \frac{|a_k|}{2^k} \leq \sum_{k=1}^{+\infty} \frac{1}{2^{k+1}} = \frac{1}{2}$$

Et $\frac{1}{2} \leq 1 - |a_0| \leq |1 - a_0| \leq \frac{1}{2}$. Donc $|a_0| = \frac{1}{2}$ et $|1 - a_0| = \frac{1}{2}$.

$$\begin{aligned} a_0 = \frac{1}{2} e^{i\theta} &\Rightarrow \left| 1 - \frac{1}{2} e^{i\theta} \right|^2 = \frac{1}{4} \\ &\Rightarrow \left(1 - \frac{1}{2} \cos(\theta) \right)^2 + \left(\frac{1}{2} \sin(\theta) \right)^2 = \frac{1}{4} \\ &\Rightarrow 1 - \cos(\theta) + \frac{1}{4} = \frac{1}{4} \\ &\Rightarrow \cos(\theta) = 1 \end{aligned}$$

et donc $a_0 = \frac{1}{2}$.

Par ailleurs, on a

$$\frac{1}{2} = \sum_{k=1}^{+\infty} \frac{|a_k|}{2^k} = \sum_{k=1}^{+\infty} \frac{1}{2^{k+1}}$$

Donc pour tout $k \in \mathbb{N}$, $|a_k| = \frac{1}{2}$, impossible car $P \in \mathbb{C}[X]$, ainsi $\|P - 1\|_\infty > \frac{1}{2}$.

3. On définit, pour $n \geq 1$, $P_n = \frac{1}{2} + \sum_{k=1}^n (-\frac{1}{2} + \varepsilon_n) X^k$ avec $\varepsilon_n \in \mathbb{R}$ tel que $P_n \in \ker(\varphi)$.

On a

$$\begin{aligned} P_n \in \ker(\varphi) &\Rightarrow \frac{1}{2} + \sum_{k=1}^n \left(-\frac{1}{2} + \varepsilon_n\right) \frac{1}{2^k} = 0 \\ &\Rightarrow \varepsilon_n = -\frac{1}{2^{n+1}} \times \frac{1}{1 - \frac{1}{2^n}} \end{aligned}$$

et donc $\varepsilon_n \xrightarrow[n \rightarrow +\infty]{} 0$ (et $\varepsilon_n < 0$). On a donc $\|P_n - 1\|_\infty = \frac{1}{2} - \varepsilon_n \xrightarrow[n \rightarrow +\infty]{} \frac{1}{2}$.

Donc $d(1, \ker(\varphi)) = \frac{1}{2}$ et cette distance n'est pas atteinte.

Solution 6.36. Prouvons d'abord l'existence. Soit $M \in \mathbb{R}^n$, on définit $r(M) = \sup\{\|M - A\| \mid A \in K\}$ et $\varphi: A \mapsto \|M - A\|$ est continue sur K compact donc le sup est en fait un max. On a notamment $r(M) = \{R > 0 \mid K \subset B(M, R)\}$. Soit

$$\begin{aligned} r : \mathbb{R}^n &\rightarrow \mathbb{R} \\ M &\mapsto r(M) \end{aligned}$$

Soit $(M, M') \in (\mathbb{R}^n)^2$. Pour tout $A \in K$, on a

$$\|M - A\| \leq \|M - M'\| + \|M' - A\| \leq \|M - M'\| + r(M')$$

En particulier, on a

$$r(M) \leq \|M - M'\| + r(M')$$

et en échangeant M et M' , on a $|r(M) - r(M')| \leq \|M - M'\|$. Donc r est 1-lipschitzienne donc continue. Soit $A_0 \in K$, $R(M) \geq \|M - A_0\| \geq \|M\| - \|A_0\| \xrightarrow[\|M\| \rightarrow +\infty]{} +\infty$. Donc il existe $M_0 \in \mathbb{R}^n$ tel que $r(M_0) = \min_{M \in \mathbb{R}^n} r(M) = r_0$, d'où l'existence d'une boule fermée de rayon minimal.

Pour l'unicité, soit $(M_1, M_2) \in (\mathbb{R}^n)^2$ tel que $r(M_1) = r(M_2) = r_0$. On suppose que $\|M_1 - M_2\| = \varepsilon > 0$. Soit M_3 le milieu de $[M_1 M_2]$. On a $K \subset B_{M_1, r_0} \cap B_{M_2, r_0}$. On prend $r^2 + \left(\frac{\varepsilon}{2}\right)^2 = r_0^2$ d'où

$$r = \sqrt{r_0^2 - \frac{\varepsilon^2}{4}} < r_0$$

Soit $M \in B(M_1, r_0) \cap B(M_2, r_0)$, on a

$$\begin{aligned}
\|M - M_3\|^2 &= \frac{1}{4} \left(\|M - M_1 + M - M_2\|^2 \right) \\
&= \frac{1}{4} \left(2\|M - M_1\|^2 + 2\|M - M_2\|^2 - \underbrace{\|M_1 - M_2\|^2}_{=\varepsilon^2} \right) \\
&\leq \frac{1}{4} (2r_0^2 + 2r_0^2 - \varepsilon^2) \\
&\leq r_0^2 - \frac{\varepsilon^2}{4} = r^2
\end{aligned}$$

Donc $B_1 \cap B_2 \subset \overline{B(M_3, r)}$ d'où $K \subset \overline{B(M_3, r)}$, ce qui est absurde car $r < r_0$. Donc $M_1 = M_2$.

Solution 6.37. φ est évidemment définie et linéaire. Soit $f \in \mathcal{C}^0([0, 1], \mathbb{R})$.

$$\begin{aligned}
|\varphi(f)| &= \left| \int_0^{\frac{1}{2}} f - \int_{\frac{1}{2}}^1 f \right| \\
&\leq \left| \int_0^{\frac{1}{2}} f \right| + \left| \int_{\frac{1}{2}}^1 f \right| \\
&\leq \int_0^{\frac{1}{2}} |f| + \int_{\frac{1}{2}}^1 |f| \\
&\leq \int_0^1 \|f\|_\infty = \|f\|_\infty
\end{aligned}$$

Donc φ est continue et $\|\varphi\| \leq 1$. Notons que si l'on a $|\varphi(f)| = \|f\|_\infty$, alors on a égalité partout au-dessus et pour tout $t \in [0, 1]$, $|f(t)| = \|f\|_\infty$ et comme $\left| \int f \right| = \int |f|$ implique que f est de signe constant sur l'intervalle d'intégration, si l'on a $|\varphi(f)| = \|f\|_\infty$, alors f est de signe constant sur $[0, \frac{1}{2}]$ et sur $[\frac{1}{2}, 1]$. Or $\left| \int_0^{\frac{1}{2}} f - \int_{\frac{1}{2}}^1 f \right| = \left| \int_0^{\frac{1}{2}} f \right| + \left| \int_{\frac{1}{2}}^1 f \right|$, f est de signe opposé sur les deux segments. Or f est continue en $\frac{1}{2}$, donc f est nulle. Donc pour f non nulle, on a $|\varphi(f)| < \|f\|_\infty$ donc la norme triple n'est pas atteinte. Enfin, pour montrer que $\|\varphi\| = 1$, on utilise pour $n \geq 1$,

$$f_n(t) = \begin{cases} 1 & \text{si } t \in [0, \frac{1}{2} - \frac{1}{n}] \\ (\frac{1}{2} - t)n & \text{si } t \in [\frac{1}{2} - \frac{1}{n}, \frac{1}{2} + \frac{1}{n}] \\ -1 & \text{si } t \in [\frac{1}{2} + \frac{1}{n}, 1] \end{cases}$$

On a bien $\|f_n\|_\infty = 1$.

Solution 6.38.

1. Non car on applique l'application trace.
2. On a le résultat par récurrence.
3. On a

$$(n+1)\|v^n\| = \|u \circ v^n \circ v - v^n \circ v \circ r\| \leq 2\|u\|\|v\|\|v^n\|$$

Si pour tout $n \in \mathbb{N}$, on a $v^n = 0$, alors pour tout $n \in \mathbb{N}$,

$$n+1 \leq 2\|u\|\|v\|$$

ce qui est impossible. Donc il existe $n \in \mathbb{N}^*$ tel que $v^n = 0$. Alors $u \circ v^n - v^n \circ u = nv^{n-1} = 0$ donc $v^{n-1} = 0$ et de proche en proche $v = 0$: contradiction.

4. Pour tout $P \in \mathbb{R}[X]$,

$$(D \circ T - T \circ D)(P) = (XP)' - XP' = P$$

donc $D \circ T - T \circ D = id$. D'après ce qui précède, T et D ne peuvent pas être continus simultanément.

Solution 6.39.

1. $\sum_{k \geq 0} (A - I_n)^k$ converge absolument car $\|A - I_n\|^k \leq \alpha^k$ et $\alpha < 1$.

Si $AX = 0$, $\|(A - I_n)X\| = \|X\| \leq \alpha\|X\|$ donc $\|X\| = 0$ et $X = 0$ donc $A \in GL_n(\mathbb{C})$, idem pour B . On a alors

$$A \sum_{k=0}^{+\infty} (I_n - A)^k = ((A - I_n) + I_n) \sum_{k=0}^{+\infty} (I_n - A)^k = I_n$$

par télescopage. Donc

$$A^{-1} = \sum_{k=0}^{+\infty} (I_n - A)^k$$

et

$$\|A^{-1}\| \leq \sum_{k=0}^{+\infty} \alpha^k = \frac{1}{1-\alpha}$$

et de même pour B . On écrit alors

$$ABA^{-1}B^{-1} - I_n = (AB - BA)A^{-1}B^{-1} = ((A - I_n)(B - I_n) - (B - I_n)(A - I_n))A^{-1}B^{-1}$$

d'où

$$\|ABA^{-1}B^{-1} - I_n\| \leq \frac{2\|A - I_n\|\|B - I_n\|}{(1-\alpha)(1-\beta)}$$

2. On prend $\alpha = \beta = \frac{1}{4}$.

3. Pour tout $M \in G$, il existe $r > 0$ tel que $B(M, r) \cap G = \{M\}$. Montrons que G est discret si et seulement si I_n est isolé. En effet, si I_n est isolé, il existe $r_0 > 0$ tel que $B(I_n, r_0) \cap G = \{I_n\}$. Soit $M \in G$, alors pour tout $M' \in G$, $M - M' = M(I_n - M^{-1}M')$ d'où $I_n - M^{-1}M' = M^{-1}(M - M')$. Si

$$\|M - M'\| < \frac{r_0}{\|M^{-1}\|}$$

on a $\|I_n - M^{-1}M'\| < r_0$ et donc $M' = M$ et M est isolé. Ainsi G est discret. La réciproque est évidente.

C est dans le commutant si et seulement si C commute avec A et B si et seulement si

$$\begin{cases} ACA^{-1}C^{-1} = I_n \\ BCB^{-1}C^{-1} = I_n \end{cases}$$

Notons maintenant que

$$\overline{B_{\|\cdot\|}(I_n, \frac{1}{4})} \cap G = \mathcal{A}$$

est fini. En effet, si cet ensemble était infini, il existerait $(M_p)_{p \in \mathbb{N}}$ une suite injective dans \mathcal{A} . La suite étant bornée, on peut extraire $(M_{\sigma(p)})_{p \in \mathbb{N}}$ qui converge et alors pour tout $p \in I_n$

$$\underbrace{M_{\sigma(p)} M_{\sigma(p+1)}^{-1}}_{\xrightarrow{p \rightarrow +\infty} I_n} \in G \setminus \{I_n\}$$

ce qui est impossible car I_n est isolé.

Comme $A \in \mathcal{A} \setminus \{I_n\}$, il existe $C \in \mathcal{A} \setminus \{I_n\}$ telle que $\|C - I_n\|$ soit minimale et $\|C - I_n\| \leq \frac{1}{4}$. D'après la question 2 on a

$$\|ACA^{-1}C^{-1} - I_n\| < \|C - I_n\|$$

et même chose pour B . Donc nécessairement, $ACA^{-1}C^{-1} = I_n$ et de même pour B . Ainsi, C commute avec toutes les matrices de G .

Solution 6.40.

1. $\mathbb{C}_{n-1}[A]$ est un sous-espace vectoriel de dimension finie donc c'est un fermé. Par division euclidienne par χ_A , d'après le théorème de Cayley-Hamilton, $\mathbb{C}[A] = \mathbb{C}_{n-1}[A]$. Comme

$$\exp(A) = \lim_{n \rightarrow +\infty} \sum_{k=0}^n \frac{A^k}{k!}$$

$$\exp(A) \in \mathbb{C}[A] = \mathbb{C}_{n-1}[A].$$

2. Si A est diagonalisable, il existe $P \in GL_n(\mathbb{C})$ tel que

$$A = P^{-1} \text{diag}(\lambda_1, \dots, \lambda_n) P$$

et donc

$$\exp(A) = P^{-1} \text{diag}(e^{\lambda_1}, \dots, e^{\lambda_n}) P$$

et $\exp(A)$ est diagonalisable.

Si $\exp(A)$ est diagonalisable, on utilise la décomposition de Dunford : $A = D + N$ avec $DN = ND$, D diagonalisable et N nilpotente. On a donc

$$\exp(A) = \exp(D) \underbrace{\exp(N)}_{=\sum_{k=0}^{n-1} \frac{N^k}{k!}} = \exp(D) + \exp(D) \left(\sum_{k=1}^{n-1} \frac{N^k}{k!} \right) = \exp(D) + N'$$

avec N' nilpotente et $\exp(D)$ est diagonalisable d'après le sens direct. N' commute avec $\exp(D)$. Par unicité de la décomposition de Dunford, $\exp(A)$ étant diagonalisable, on a $N' = 0$. Comme $\exp(D)$ est inversible,

$$N \times \underbrace{\sum_{k=1}^{n-1} \frac{N^{k-1}}{k!}}_{=I_n + N''} = 0$$

avec N'' nilpotente. $I_n + N''$ est donc inversible et ainsi $N = 0$ et A est diagonalisable.

3. D'après ce qui précède, $\exp(A) = I_n$ est diagonalisable et

$$\text{Sp}_{\mathbb{C}}(\exp(A)) = \{e^\lambda \mid \lambda \in \text{Sp}_\lambda(\mathbb{C})\} = \{I_n\}$$

Donc $\text{Sp}_{\mathbb{C}}(A) \subset 2i\pi\mathbb{Z}$.

Réciproquement, si A est diagonalisable avec $\text{Sp}(A) \subset 2i\pi\mathbb{Z}$, en diagonalisant, on a bien $\exp(A) = I_n$.

4. Sur \mathbb{R} , si A est diagonalisable, $\exp(A)$ l'est aussi. Cependant, la réciproque n'est pas vrai, par exemple

$$M = \begin{pmatrix} 2i\pi & 0 \\ 0 & -2i\pi \end{pmatrix} \text{ semblable à } \begin{pmatrix} 0 & -4\pi^2 \\ 1 & 0 \end{pmatrix} = A$$

On a $\chi_M = X^2 + 4\pi^2$, $\exp(A) = I_2$ et A n'est pas diagonalisable sur \mathbb{C} .

Solution 6.41.

1. On a $\ln(1+x) = P(x) + x^2O(1)$ et $\exp(y) = Q(y) + y^nO(1)$ d'où

$$\exp(\ln(1+x)) = 1+x = Q(\ln(1+x)) + \underbrace{\ln(1+x)^nO(1)}_{O(x^n)}$$

alors $1+x = Q(P(x) + O(x^n)) + O(x^n) = Q(P(x)) + O(x^n)$. Soit $B(X) = Q(P(X)) + O(x^n) \in \mathbb{R}[X]$, on a $\frac{B(x)}{x^n} = O(1)$ donc $X^n \mid B$ et

$$Q(P(X)) = 1 + X + B(X) = 1 + X + X^n A(X)$$

2. On a $N^n = 0$ donc $P(N)$ est aussi nilpotente et on a

$$\exp(P(N)) = \sum_{k=0}^{n-1} \frac{P(N)^k}{k!} = Q(P(N)) = I_n + N + 0$$

3. Soit $M \in GL_n(\mathbb{C})$ et sa décomposition de Dunford : $M = D + N$ avec D diagonalisable, N nilpotente et $DN = ND$. On a $\text{Sp}(D) = \text{Sp}(M) \subset \mathbb{C}^*$ et on écrit

$$M = D \underbrace{(I_n + D^{-1}N)}_{\substack{\text{nilpotente} \\ = \exp(P(D^{-1}N))}}$$

si $D = P_1 \text{diag}(\lambda_1, \dots, \lambda_n) P_1^{-1}$, pour tout $k \in \{1, \dots, n\}$ il existe $\mu_k \in \mathbb{C}$ tel que $\lambda_k = \exp(\mu_k)$ (car \exp est surjectif sur \mathbb{C}^*). Alors

$$D = \exp(P_1 \text{diag}(\mu_1, \dots, \mu_n) P_1^{-1}) \in \mathbb{C}[D]$$

puis

$$\begin{aligned} M &= \exp\left(P_1 \text{diag}(\mu_1, \dots, \mu_n) P_1^{-1}\right) \exp\left(P(D^{-1}N)\right) \\ &= \exp\left(P_1 \text{diag}(\mu_1, \dots, \mu_n) P_1^{-1} + P(D^{-1}N)\right) \end{aligned}$$

car les matrices commutent.

Donc \exp est surjective.

Solution 6.42. On a $A \subset \overline{A}$, $0 = \lim_{n \rightarrow +\infty} \left(\frac{2}{n}\right)^{2n} \in \overline{A}$ et $e = \lim_{n \rightarrow +\infty} \left(1 + \frac{1}{n}\right)^{n+1} \in \overline{A}$.

Si $n \geq 2$ et $p \geq 2$, $\left(\frac{1}{n} + \frac{1}{p}\right)^{n+p} \leq 1$. Donc si $\left(\frac{1}{n} + \frac{1}{p}\right)^{n+p} \geq 1$, alors $n = 1$ ou $p = 1$.

Si $x > e$, à partir d'un certain rang, on a $\left(1 + \frac{1}{n}\right)^{n+1} \leq \frac{e+x}{2}$ et si $x \notin A$, $x \notin \overline{A}$. Si $1 \leq x < e$, à partir d'un certain rang, on a $\left(1 + \frac{1}{n}\right)^{n+1} > x$ donc si $x \notin A$, $x \notin \overline{A}$.

Soit $x < 1$, si $n \geq 2$ et $p \geq 3$ ou $n \geq 3$ et $p \geq 2$, on a $\frac{1}{n} + \frac{1}{p} \leq \frac{5}{6}$ et

$$\begin{aligned} \left(\frac{1}{n} + \frac{1}{p}\right)^{n+p} &= \exp\left((n+p) \ln\left(\frac{1}{n} + \frac{1}{p}\right)\right) \\ &\leq \exp\left((n+p) \ln\left(\frac{5}{6}\right)\right) \\ &\leq \max\left(\underbrace{\left(\frac{5}{6}\right)^n}_{\xrightarrow[n \rightarrow +\infty]{} 0}, \underbrace{\left(\frac{5}{6}\right)^p}_{\xrightarrow[p \rightarrow +\infty]{} 0}\right) \end{aligned}$$

Il existe N_0 tel que pour tout $n \geq N_0$, $\left(\frac{5}{6}\right)^n \leq \frac{x}{2}$. Si n ou p est plus grand que N_0 , on a donc

$$\left(\frac{1}{n} + \frac{1}{p}\right)^{n+p} \leq \frac{x}{2}$$

Donc il n'y a qu'un nombre fini d'éléments de A plus grand que $\frac{x}{2}$. Ainsi,

$$\overline{A} = A \cup \{e, 0\}$$

Solution 6.43. On note

$$\mathbb{V} = \bigcup_{m \geq 1} \mathbb{U}_m = \left\{ e^{\frac{2ik\pi}{m}} \mid m \geq 1, k \in \{0, \dots, m-1\} \right\}$$

Soit $M \in H$. $X^m - 1$ est scindé à racines simples sur \mathbb{C} donc M est diagonalisable sur \mathbb{C} avec ses valeurs propres dans \mathbb{V} . Réciproquement, si M est diagonalisable sur \mathbb{C} et $\text{Sp}_{\mathbb{C}}(M) \subset \mathbb{V}$. Alors pour tout $\lambda \in \text{Sp}_{\mathbb{C}}(M)$, $\exists m_\lambda \in \mathbb{N}^*$, $\lambda \in \mathbb{U}_{m_\lambda}$ et soit $m = \text{ppcm}_{\lambda \in \text{Sp}_{\mathbb{C}}(M)}(m_\lambda)$. Alors $M^m = I_n$.

Soit $A \in \overline{H}$, il existe $(M_p)_{p \in \mathbb{N}} \in H^{\mathbb{N}}$ telle que $\lim_{p \rightarrow +\infty} M_p = A$. Comme le polynôme caractéristique est une fonction continue des coefficients, pour tout $\lambda \in \text{Sp}_{\mathbb{C}}(A)$, on a

$$\lim_{p \rightarrow +\infty} \chi_{M_p}(\lambda) = \chi_A(\lambda) = 0$$

Or

$$|\chi_{M_p}(\lambda)| = |\lambda - \lambda_{1,p}| \dots |\lambda - \lambda_{n,p}| \geq d(\lambda, \mathbb{U})^n$$

avec $\lambda_{i,p} \in \mathbb{V}$ pour tout $i \in \{1, \dots, n\}$. Donc $d(\lambda, \mathbb{U}) = 0$ et comme \mathbb{U} est fermé, $\lambda \in \mathbb{U}$.

Réciproquement, soit $A \in \mathcal{M}_n(\mathbb{C})$ tel que $\text{Sp}_{\mathbb{C}}(A) \subset \mathbb{U}$. Soit

$$\{e^{i\theta_1}, \dots, e^{i\theta_r}\}$$

les valeurs propres distinctes de A de multiplicités m_1, \dots, m_r . Il existe $Q \in GL_n(\mathbb{C})$ tel que

$$A = Q \text{diag}(\underbrace{e^{i\theta_1}, \dots, e^{i\theta_1}}_{m_1 \text{ fois}}, \dots, \underbrace{e^{i\theta_r}, \dots, e^{i\theta_r}}_{m_r \text{ fois}}) Q^{-1}$$

On a

$$\theta = \lim_{k \rightarrow +\infty} \frac{2\pi}{k} \lfloor k \frac{\theta}{2\pi} \rfloor$$

donc on peut former, pour $p \in \mathbb{N}^*$,

$$A = Q \text{diag}(\underbrace{e^{i\theta_{1,p}}, \dots, e^{i\theta_{1,p}}}_{m_1 \text{ fois}}, \dots, \underbrace{e^{i\theta_{r,p}}, \dots, e^{i\theta_{r,p}}}_{m_r \text{ fois}}) Q^{-1}$$

avec $\theta_{i,p} = \frac{2\pi}{p} \lfloor p \frac{\theta_j}{2\pi} \rfloor + \frac{2j\pi}{p}$. Pour p suffisamment grand, les $(\theta_{j,p})$ sont deux à deux distincts donc A_p est diagonalisable et $A_p \in H$, et donc $A \in \overline{H}$.

Solution 6.44.

1. On a l'inégalité triangulaire et l'homogénéité. On a cependant $N_a(X^k) = |a_k|$ et pour tout $k \in \mathbb{N}$, $X^k \neq 0$. Donc N_a est une norme implique que a ne s'annule pas sur \mathbb{N} . Réciproquement, si pour tout $k \in \mathbb{N}$, $a_k \neq 0$, si $P \neq 0$, il existe $k \in \mathbb{N}$ avec p_k et donc $N_a(P) > 0$. Donc N_a est une norme si et seulement si pour tout $k \in \mathbb{N}$, $a_k \neq 0$.
2. Si N_a et N_b sont équivalentes, alors il existe $(\alpha, \beta) \in (\mathbb{R}_+^*)^2$ tel que pour tout $k \in \mathbb{N}$,

$$\beta N_b(X^k) \leq N_a(X^k) \leq \alpha N_b(X^k)$$

d'où

$$\beta |b_k| \leq N_a(X^k) \leq \alpha |b_k|$$

Donc $a = O(b)$ et $b = O(a)$.

Réciproquement, si $a = O(b)$ et $b = O(a)$, alors on a l'inégalité précédente sur les a_k et b_k , d'où

$$\beta \sum_{k=0}^{+\infty} |p_k b_k| \leq \sum_{k=0}^{+\infty} |p_k a_k| \leq \alpha \sum_{k=0}^{+\infty} |p_k b_k|$$

et donc pour tout $P \in \mathbb{C}[X]$

$$\beta N_b(P) \leq N_a(P) \leq \alpha N_b(P)$$

et N_a et N_b sont équivalentes.

3. Δ est continue pour N_a si et seulement s'il existe $c \geq 0$ tel que pour tout $P \in \mathbb{C}[X]$, $N_a(\Delta P) \leq c N_a(P)$. Si Δ est continue alors il existe $c \geq 0$ tel que $N_a(kX^k) \leq c N_a(X^k)$ alors pour tout $k \in \mathbb{N}^*$,

$$|ka_{k-1}| \leq c|a_k| \quad (6.1)$$

Réciproquement, si on a (6.1), pour tout $P \in \mathbb{C}[X]$ $N_a(\Delta P) \leq c N_a(P)$. Pour tout $k \in \mathbb{N}$, $a_k = k!$, (6.1) est vérifiée pour $c = 1$. Si $b_k = 1$ pour tout $k \in \mathbb{N}$, (6.1) n'est pas vérifiée donc Δ n'est pas continue pour N_b .

Solution 6.45.

1. On a $d(x, A) = 0$ si et seulement si $\inf_{a \in A} \|x - a\| = 0$ si et seulement si $\varepsilon > 0, \exists a \in A: \|x - a\| < \varepsilon$ si et seulement si $x \in \overline{A}$.

On a $A \subset \overline{A}$ donc $d(x, \overline{A}) \leq d(x, A)$. Soit $\varepsilon > 0$, il existe $a' \in \overline{A}$ tel que $\|x - a'\| < d(x, \overline{A}) + \varepsilon$ et il existe $a \in A$ tel que $\|a - a'\| < \varepsilon$. Ainsi,

$$d(x, A) \leq \|x - a\| \leq d(x, \overline{A}) + 2\varepsilon$$

Ceci valant pour tout $\varepsilon > 0$, on a $d(x, A) \leq d(x, \overline{A})$ et donc on a égalité.

2. $A \times B \subset \overline{A} \times \overline{B}$ donc $d(A, B) \geq d(\overline{A}, \overline{B})$. De plus, pour tout $\varepsilon > 0$, il existe $(a', b') \in \overline{A} \times \overline{B}$ tel que $\|a' - b'\| < d(\overline{A}, \overline{B}) + \varepsilon$ et il existe $(a, b) \in A \times B$ tel que $\|a - a'\| < \varepsilon$ et $\|b - b'\| < \varepsilon$. En utilisant l'inégalité triangulaire, on a donc

$$d(A, B) \leq \|a - b\| < d(\overline{A}, \overline{B}) + 3\varepsilon$$

Ceci valant pour tout $\varepsilon > 0$, on a bien l'égalité.

Solution 6.46. φ_{x_0} est une forme linéaire. Elle est continue si et seulement $C > 0$ tel que pour tout $P \in \mathbb{C}[X]$,

$$|P(x_0)| \leq C \|P\|_\infty$$

Si $P = \sum_{k=0}^n a_k X^k$, on a

$$|P(x_0)| \leq \|P\|_\infty \sum_{k=0}^n |x_0|^k$$

Si $|x_0| < 1$, on a

$$|P(x_0)| \leq \|P\|_\infty \frac{1}{1 - |x_0|}$$

donc φ_{x_0} est continue et si $x_0 = |x_0|e^{i\theta_0}$, soit $n \in \mathbb{N}$ et $P_n = \sum_{k=0}^n e^{-ik\theta_0} X^k$, on a $\|P_n\|_\infty = 1$ et

$$|\varphi_{x_0}(P_n)| = \sum_{k=0}^n |x_0|^k \xrightarrow{n \rightarrow +\infty} \frac{1}{1 - |x_0|}$$

donc $\|\varphi_{x_0}\| = \frac{1}{1 - |x_0|}$.

Si $|x_0| \geq 1$,

$$|\varphi_{x_0}(P_n)| = \sum_{k=0}^n |x_0|^k \xrightarrow{n \rightarrow +\infty} +\infty$$

donc φ_{x_0} n'est pas continue.

Solution 6.47. Pour le sens indirect, soit $\lambda \in \text{Sp}_{\mathbb{C}}(M)$. Pour tout $p \in \mathbb{N}$, $\lambda \in \text{Sp}_{\mathbb{C}}(M_p)$ donc $\det(M_p - \lambda I_n) = 0$. Par continuité du déterminant, on a $0 = \det(M_p - \lambda I_n) \xrightarrow{p \rightarrow +\infty} \det(-\lambda I_n)$. Donc $\lambda = 0$ et $\text{Sp}_{\mathbb{C}}(M) = \{0\}$ donc M est nilpotente.

Pour le sens direct, soit $u \in \mathcal{L}(\mathbb{C}^n)$ canoniquement associée à M . On trigonalise u sur une base $\mathcal{B} = (\varepsilon_1, \dots, \varepsilon_n)$ avec $u(\varepsilon_1) = 0, u(\varepsilon_2) = a_{1,2}\varepsilon_1, \dots, u(\varepsilon_n) = a_{1,n}\varepsilon_1 + \dots + a_{n-1,n}\varepsilon_{n-1}$. Posons pour $i \in \{1, \dots, n\}$, $\varepsilon_{i,p} = \frac{\varepsilon_i}{p^{i-1}}$. On pose $\mathcal{B}_p = (\varepsilon_{1,p}, \dots, \varepsilon_{n,p})$ et $M_p = \text{mat}_{\mathcal{B}_p}(u)$, semblable à M et $M_p \xrightarrow{p \rightarrow +\infty} 0$ car $\|M_p\| \leq \frac{1}{p} \|M_1\|$.

Solution 6.48. On pose $u \in \mathcal{L}(\mathbb{C}^n)$ canoniquement associée à M .

Pour le sens indirect, si M n'est pas diagonalisable, il existe une base $B = (\varepsilon_1, \dots, \varepsilon_n)$ de \mathbb{C}^n telle que

$$\text{mat}_B(u) = D + N$$

où D est diagonale et N est nilpotente (décomposition de Dunford). En reprenant les bases \mathcal{B}_p définies à l'exercice précédent, on a

$$\text{mat}_{\mathcal{B}_p}(u) = D + N_p \xrightarrow{p \rightarrow +\infty} D$$

Si $D \in S_M$, alors M est diagonalisable ce qui est exclu par hypothèse. Donc S_M n'est pas fermé.

Pour le sens direct, si M est diagonalisable, soit $(M_p)_{p \in \mathbb{N}} \in (S_M)^{\mathbb{N}}$ avec $M_p \xrightarrow{p \rightarrow +\infty} M'$. Soit $\lambda \in \mathbb{C}$. On a $\chi_{M_p}(\lambda) = \det(\lambda I_n - M_p) = \chi_M(\lambda)$ car M et M_p sont semblables. Par continuité du déterminant, on a $\chi_{M'}(\lambda) = \chi_M(\lambda)$, donc $\chi_{M'} = \chi_M$. De plus, $A \mapsto \Pi_M(A)$ (polynôme minimal) est continue sur $\mathcal{M}_n(\mathbb{C})$ et pour tout $p \in \mathbb{N}$, on a $\Pi_M(M_p) = 0$ donc $\Pi_M(M') = 0$. M' est donc annulée par Π_M , donc M' est diagonalisable et comme $\chi_M = \chi_{M'}$, M et M' ont les mêmes valeurs propres avec les mêmes multiplicités. Donc $M' \in S_M$.

Remarque 6.9. Le polynôme caractéristique est une fonction continue de la matrice, mais c'est faux pour le polynôme minimal, par exemple pour

$$M_p = \begin{pmatrix} \frac{1}{p} & 0 \\ 0 & \frac{2}{p} \end{pmatrix}$$

On a $M_p \xrightarrow{p \rightarrow +\infty} 0$ et $\Pi_{M_p} = (X - \frac{1}{p})(X - \frac{2}{p}) \xrightarrow{p \rightarrow +\infty} X^2 \neq X = \Pi_{M_\infty}$ donc $\lim_{p \rightarrow +\infty} \Pi_{M_p} \neq \Pi_{\lim_{p \rightarrow +\infty} M_p}$.

Solution 6.49. On note $A_h = \{|\varphi(x) - \varphi(y)| \mid (x, y) \in I^2 \text{ et } |x - y| \leq h\}$.

1. ω_φ est bien défini car $|\varphi(x) - \varphi(y)| \leq 2\|\varphi\|_\infty$. Si $0 < h \leq h'$, alors $A_h \subset A_{h'}$ donc $\sup(A_h) \leq \sup(A_{h'})$ donc $\omega_\varphi(h) \leq \omega_\varphi(h')$.
2. Soit $(h, h') \in (\mathbb{R}_+^*)^2$, soit $(x, y) \in I^2$ tel que $|x - y| \leq h + h'$ (où on peut supposer que $x \leq y$).
 - Si $y \in [x, x + h]$, alors $|x - y| \leq h$ donc $|\varphi(x) - \varphi(y)| \leq \omega_\varphi(h) \leq \omega_\varphi(h) + \omega_\varphi(h')$
 - Si $y \in [x + h, x + h + h']$, $|\varphi(x) - \varphi(y)| \leq |\varphi(x) - \varphi(x + h)| + |\varphi(x + h) - \varphi(y)| \leq \omega_\varphi(h) + \omega_\varphi(h')$ car $|x - (x + h)| \leq h$ et $|x + h - y| \leq h'$.
 Donc $\omega_\varphi(h + h') \leq \omega_\varphi(h) + \omega_\varphi(h')$.
3. Par récurrence sur $n \in \mathbb{N}$, on a $\omega_\varphi(nh) = n\omega_\varphi(h)$. Si $\lambda \in \mathbb{R}_+^*$, on a $\lambda h \leq ([\lambda] + 1)h$ et par croissance et ce qui précède, on a

$$\omega_\varphi(\lambda h) \leq ([\lambda] + 1)\omega_\varphi(h) \leq (\lambda + 1)\omega_\varphi(h)$$

4. Soit $\varepsilon > 0$. φ étant uniformément continue, il existe $\alpha > 0$ tel que pour tout $(x, y) \in I^2$, si $|x - y| < \alpha$ on a $|\varphi(x) - \varphi(y)| \leq \varepsilon$ et on a pour $h \leq \alpha$, $\omega_\varphi(h) \leq \varepsilon$ d'où $\lim_{h \rightarrow 0} \omega_\varphi(h) = 0$.
 Soit alors $h_0 > 0$ fixé et $h > 0$,
 — si $h_0 \leq h$, on a $0 \leq \omega_\varphi(h) - \omega_\varphi(h_0) \leq \omega_\varphi(h - h_0)$.
 — si $h \leq h_0$, on a $0 \leq \omega_\varphi(h_0) - \omega_\varphi(h) \leq \omega_\varphi(h_0 - h)$.
 Dans tous les cas, on a $|\omega_\varphi(h) - \omega_\varphi(h_0)| \leq \omega_\varphi(|h_0 - h|)$. Donc on a bien $\lim_{h \rightarrow h_0} \omega_\varphi(h) = \omega_\varphi(h_0)$. Donc ω_φ est continue (et même uniformément).

Solution 6.50. G est borné car si $M \in G$, $\|M\| \leq \|I_n\| + \mu = 1 + \mu$. Montrons donc que si G_0 est un sous-groupe borné de $GL_n(\mathbb{C})$, alors les valeurs propres de ses éléments sont de module 1, et ceux-ci sont diagonalisables.

En effet, soit $M \in G$ et $\lambda \in \text{Sp}(M)$, soit X un vecteur propre associé. On a $\|MX\| = |\lambda| \|X\| \leq \|M\| \|X\|$ donc $|\lambda| \leq \|M\| \leq \sup_{M \in G} \|M\|$. Pour tout $k \in \mathbb{Z}$, $M^k \in G$ et $\lambda^k \in \text{Sp}(M^k)$, donc si $|\lambda| > 1$, on a $\lim_{k \rightarrow +\infty} |\lambda|^k = +\infty$, et si $|\lambda|^\lambda < 1$, on a $\lim_{k \rightarrow -\infty} |\lambda|^k = +\infty$. Comme G est borné, $|\lambda| = 1$.

On utilise ensuite la décomposition de Dunford pour M : $M = D + N$ avec $DN = ND$, D diagonalisable et N nilpotente. Grâce au binôme de Newton, pour $k \geq r$ $p^* r$ est l'indice de nilpotence de N , on a

$$M^k = \sum_{p=0}^k \binom{k}{p} N^p D^{k-p} = \underbrace{D^k}_{\text{borné}} + kND + \sum_{p=2}^{r-1} \underbrace{\binom{k}{p}}_{\substack{\sim \frac{k^p}{p!} \\ k \rightarrow +\infty}} N^p \underbrace{D^{k-p}}_{\text{borné car } \text{Sp}(D) \subset \mathbb{U}}$$

Donc

$$M^k \underset{k \rightarrow +\infty}{\sim} \underbrace{\frac{k^{r-1}}{(r-1)!} \underbrace{N^{r-1}}_{\neq 0} D^{k-r+1}}_{\text{non borné si } N \neq 0}$$

Donc $N = 0$ et $M = D$ est diagonalisable.

Revenons donc à l'exercice. Soit $M \in G$ et $\lambda = e^{i\theta} \in \text{Sp}(M)$ avec $\theta \in]-\pi, \pi]$. Si X est un vecteur propre associé à λ , on a

$$(\lambda - 1)\|X\| = \|(M - I_n)X\| \leq \mu \|X\|$$

donc $|\lambda - 1| = 2 \underbrace{\left| \sin\left(\frac{\theta}{2}\right) \right|}_{\geq 0} \leq \mu$. Donc $\theta \in [-\theta_0, \theta_0]$ où $\theta_0 = \arcsin(\frac{\mu}{2}) \in [0, \pi[$.

Si $\frac{\theta}{\pi} \notin \mathbb{Q}$, $e^{ik\pi} \in \text{Sp}(M^k)$, $|e^{ik\theta} - 1| \leq \mu$. Alors $\{k\theta + 2l\pi \mid (k, l) \in \mathbb{Z}^2\}$ est un sous-groupe de $(\mathbb{R}, +)$ non monogène et donc dense, et alors $(e^{ik\theta})_{k \in \mathbb{Z}}$ est dense dans \mathbb{U} , donc il existe $k_0 \in \mathbb{Z}$ tel que $|e^{ik_0\theta} + 1| = |2 - (1 - e^{ik_0\theta})| < 2 - \mu$, ce qui est impossible car $|2 - (1 - e^{ik_0\theta})| \geq 2 - |1 - e^{ik_0\theta}| \geq 2 - \mu$.

Ainsi, $\frac{\theta}{\pi} \in \mathbb{Q}$ et il existe $m \in \mathbb{N}^*$ tel que $\lambda = e^{i\theta} \in \mathbb{U}_m$. Ce n'est pas forcément le même m pour tout les M dans G . Notons alors pour

$$\lambda \in \bigcup_{M \in G} \text{Sp}(M) = \mathcal{A}$$

$\omega(\lambda)$ l'ordre (multiplicatif) de λ dans \mathbb{U} .

Si $\omega(\lambda) = m$, on a $\text{gr}(\lambda) = \mathbb{U}_m$ donc il existe $k \in \mathbb{Z}$ tel que $\lambda^k = e^{\frac{2i\pi}{m}} \in \mathcal{A}$ (car $\lambda^k \in \text{Sp}(M^k)$). Supposons que $\{\omega(\lambda) \mid \lambda \in \mathcal{A}\}$ non borné. Alors il existe $(m_k)_{k \in \mathbb{N}}$ tel que $m_k \xrightarrow[k \rightarrow +\infty]{} +\infty$ et $e^{\frac{2i\pi}{m_k}} \in \mathcal{A}$. Alors

$$\underbrace{e^{2i \lfloor \frac{m_k}{2} \rfloor \frac{\pi}{m_k}}}_{\xrightarrow[k \rightarrow +\infty]{} e^{i\pi} = -1} \in \mathcal{A}$$

ce qui est impossible car $|\lambda + 1| \geq 2 - \mu > 0$. On peut donc noter

$$m = \bigvee_{\lambda \in \mathcal{A}} \omega(\lambda)$$

et pour tout $M \in G$, pour tout $\lambda \in \text{Sp}(M)$, $\lambda^m = 1$. Or M est diagonalisable, donc $M^m = I_n$.

Solution 6.51. Si $M \in \mathcal{G}_q$, $P(X) = X^q - 1$ annule M donc M est diagonalisable à valeurs propres dans \mathbb{U}_q . Réciproquement, si M est diagonalisable et $\text{Sp}_{\mathbb{C}}(M) \subset \mathbb{U}_q$ alors il existe $P \in GL_n(\mathbb{C})$ avec

$$M = P \text{diag}(\lambda_1, \dots, \lambda_n) P^{-1}$$

et donc

$$M^q = P \text{diag}(\lambda_1^q, \dots, \lambda_n^q) P^{-1} = I_n$$

Si $M \in \mathcal{G}_q$ n'est pas une homothétie, il existe $\lambda \neq \mu \in \text{Sp}_{\mathbb{C}}(M)^2$ et $P \in GL_n(\mathbb{C})$ tel que

$$M = P \begin{pmatrix} \lambda & & \\ & \mu & \\ & & \ddots \end{pmatrix} P^{-1}$$

Soit $k \in \mathbb{N}^*$ tel que

$$M = P \begin{pmatrix} \lambda & \frac{1}{k} & & \\ & \mu & & \\ & & \ddots & \\ & & & \lambda \end{pmatrix} P^{-1} \xrightarrow[k \rightarrow +\infty]{} M$$

Or

$$\begin{pmatrix} \lambda & \frac{1}{k} \\ 0 & \lambda \end{pmatrix} \text{ est semblable } \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$$

car $\chi_A = (X - \lambda)(X - \mu)$ donc est diagonalisable. Donc $M_k \sim M$ et $M_k \in \mathcal{G}_q$ et M n'est pas isolé.

Montrons le petit lemme suivante : soit $\|\cdot\|$ une norme sur \mathbb{C}^n et $\|\|\cdot\|\|$ la norme subordonnée, soit $\lambda \in \mathbb{C}$ et $M \in \mathcal{M}_n(\mathbb{C})$ et $\varepsilon > 0$. Si $\|\|M - \lambda I_n\|\| \leq \varepsilon$ alors $\text{Sp}_{\mathbb{C}}(M) \subset \overline{B(\lambda, \varepsilon)}$. En effet, soit X un vecteur propre de M associé à $\mu \in \text{Sp}_{\mathbb{C}}(M)$. On a

$$\|(M - \lambda I_n)X\| = |\mu - \lambda| \|X\| \leq \|\|M - \lambda I_n\|\| \|X\| \leq \varepsilon \|X\|$$

donc $|\mu - \lambda| \leq \varepsilon$.

Pour $\varepsilon = \sin(\frac{\pi}{q}) > 0$ et $\lambda \in \mathbb{U}_q$; si $M \in B_{\|\cdot\|}(\lambda I_n, \varepsilon) \cap \mathcal{G}_q$ alors pour tout $\mu \in \text{Sp}_{\mathbb{C}}(M)$, on a $|\lambda - \mu| \leq \sin(\frac{\pi}{q})$ donc $\lambda = \mu$. Donc si $M = \lambda I_n$ alors M est isolé (avec $\lambda \in \mathbb{U}_q$). Donc les matrices scalaires sont isolées.

7 Fonction d'une variable réelle

Solution 7.1. Tout d'abord, $\deg(L_n) = n$ et son coefficient dominant est $\frac{(2n)!}{2^n(n!)^2}$.

1. Soit $f \in \mathcal{C}^0([0, 1], \mathbb{R})$. -1 et 1 sont racines d'ordre n de P_n donc pour tout $k \in \{0, \dots, n-1\}$ $P_n^{(k)}(-1) = P_n^{(k)}(1) = 0$. Ainsi, on a par intégrations par parties successives :

$$(f|L_n) = (-1)^n \int_{-1}^1 f^{(n)}(t) P_n(t) dt$$

Notamment, si $P \in \mathbb{R}_{n-1}[X]$, $P^{(n)} = 0$ et $(P|L_n) = 0$. En particulier, pour tout $m < n$, $\deg(L_m) \leq n-1$ et $(L_m|L_n) = 0$ donc $(L_n)_{n \in \mathbb{N}}$ est orthogonale. Notons dès maintenant que l'on peut calculer la norme de L_n grâce aux intégrales de Wallis :

$$\begin{aligned} \|L_n\|_2^2 &= (L_n|L_n) \\ &= (-1)^n \int_{-1}^1 L_n^{(n)}(t^2 - 1)^n dt \\ &= \frac{(2n)!}{2^{2n}(n!)^2} \int_{-1}^1 (1 - t^2)^n dt \end{aligned}$$

On pose $t = \cos(\theta)$ d'où $dt = -\sin(\theta)d\theta$, d'où

$$\begin{aligned} \int_{-1}^1 (1 - t^2)^n dt &= \int_0^\pi \sin(\theta)^{2n+1} d\theta \\ &= 2I_{2n+1} \text{ [Wallis]} \end{aligned}$$

On a classiquement $I_{n+2} = \frac{n+1}{n+2} I_n$. D'où

$$\begin{aligned} I_{2n+1} &= \frac{2n}{2n+1} \times \frac{2n-2}{2n-1} \times \dots \times \frac{2}{3} \times \underbrace{I_1}_{=1} = 1 \\ &= \frac{2^{2n}(n!)^2}{(2n+1)!} \end{aligned}$$

d'où

$$\|L_n\|_2^2 = \frac{(2n)!}{2^{2n}(n!)^2} \times 2 \times \frac{2^{2n}(n!)^2}{(2n+1)!} = \frac{2}{2n+1}$$

2. On utilise la formule de Leibniz en écrivant $X^2 - 1 = (X+1)(X-1)$.
3. On montre le résultat par récurrence sur $k \in \{0, \dots, n\}$ en invoquant le théorème de Rolle. On trouve donc que $L_n = P_n^{(n)}$ s'annule au moins n fois sur $] -1, 1[$. Or $\deg(L_n) = n$, donc ces zéros sont simples et ce sont les seuls.

4. (L_0, \dots, L_n) est une base de $\mathbb{R}_n[X]$ (étagée en degré). Donc il existe $(\alpha_{n,0}, \dots, \alpha_{n,k}) \in \mathbb{R}^{k+1}$ tel que $XL_{n-1} = \sum_{k=0}^n \alpha_{n,k} L_k$. Si $k \leq n-3$, on a

$$(XL_{n-1}L_k) = \alpha_{n,k} \|L_k\|_2^2 = (L_{n-1}XL_k) = 0$$

car $\deg(XL_k) = k+1 \leq n-2$. Donc

$$XL_{n-1} = \alpha_{n,n-2}L_{n-2} + \alpha_{n,n-1}L_{n-1} + \alpha_{n,n}L_n$$

Pour calculer les coefficients, on fait tout simplement les produits scalaires :

$$(XL_{n-1}|L_{n-1}) = \int_{-1}^1 tL_{n-1}(t)^2 dt$$

Or P_n est paire, donc L_n est de la parité de n et donc L_n^2 est paire puis XL_n^2 est impaire.

Donc $\alpha_{n,n-1} = 0$.

$$\begin{aligned} (XL_{n-1}|L_{n-2}) &= \alpha_{n,n-2} \underbrace{\|L_{n-2}\|_2^2}_{= \frac{2}{2n-3}} \\ &= (-1)^n \int_{-1}^1 P_{n-1}(t) \underbrace{(XL_{n-2})^{(n-1)}(t)}_{\frac{(2n-4)!(n-1)}{2^{n-2}(n-2)!}} \end{aligned}$$

Par ailleurs,

$$\begin{aligned} (-1)^{n-1} \int_{-1}^1 P_{n-1}(t) dt &= \frac{1}{2^{n-1}(n-1)!} \underbrace{\int_{-1}^1 (1-t^2)^{n-1} dt}_{2I_{2n-1}} \\ &= \frac{1}{2^{n-1}(n-1)!} \times 2 \times \frac{2^{2n-2}(n-1)!}{(2n-1)!} \\ &= \frac{2^n(n-1)!}{(2n-1)!} \end{aligned}$$

donc $\frac{\alpha_{n,n-2}}{\alpha_{n,n}} = \frac{n-1}{n}$. D'où le résultat.

Solution 7.2. On forme

$$\begin{aligned} g: [a, b] &\rightarrow \mathbb{R} \\ x &\mapsto \underbrace{\Delta f(x_0, \dots, x_{n-1}, x)}_{\varphi(x)} - \underbrace{\prod_{i=0}^{n-1} (x - x_i) A}_{P(x)} \end{aligned}$$

On a $g(x_n) = 0$. On suppose les $(x_i)_{1 \leq i \leq n}$ distincts, et on pose

$$A = \frac{V(x_0, \dots, x_n)}{\prod_{i=0}^{n-1} (x_n - x_i)}$$

g est de classe \mathcal{C}^n et pour tout $i \in \{0, \dots, n\}$, on a $g(x_i) = 0$. Donc il existe $\xi \in]a, b[$ tel que $g^{(n)}(\xi) = 0$ (théorème de Rolle appliqué n fois. $\deg(P) = n$ et son coefficient dominant est A donc $P^{(n)}(\xi) = An! = \varphi^{(n)}(\xi)$).

On développe maintenant $\varphi(x)$ par rapport à la dernière colonne :

$$\varphi(x) = f(x) \times V_n(x_0, \dots, x_{n-1}) + Q(X)$$

avec $\deg(Q) \leq n-1$ et $V_n(x_0, \dots, x_{n-1}) = \prod_{0 \leq j < i \leq n-1} (x_i - x_j)$ (déterminant de Vandermonde). On a donc

$$\varphi^{(n)}(x) = f^{(n)}(x) \prod_{0 \leq j < i \leq n-1} (x_j - x_i)$$

et en reportant, on a

$$\frac{f^{(n)}(\xi)}{n!} = \frac{A}{\prod_{0 \leq i < j \leq n-1} (x_j - x_i)} = \Delta f(x_0, \dots, x_n)$$

Solution 7.3. On utilise le développement de Taylor avec reste intégral.

$$f(0) = f\left(\frac{1}{2}\right) - \frac{1}{2}f'\left(\frac{1}{2}\right) + \int_{\frac{1}{2}}^0 -tf''(t)dt$$

et de même

$$f(1) = f\left(\frac{1}{2}\right) - \frac{1}{2}f'\left(\frac{1}{2}\right) + \int_{\frac{1}{2}}^1 (1-t)f''(t)dt$$

D'où

$$\begin{aligned} A(f) &= f(0) - f\left(\frac{1}{2}\right) + f(1) - f\left(\frac{1}{2}\right) \\ &= \int_0^{\frac{1}{2}} tf''(t)dt + \int_{\frac{1}{2}}^1 (1-t)f''(t)dt \\ &\leq \int_0^{\frac{1}{2}} tdt + \int_{\frac{1}{2}}^1 (1-t)dt \\ &= \frac{1}{4} \end{aligned}$$

Et c'est atteint pour $f(t) = \frac{t^2}{4}$.

Solution 7.4. Pour tout $(x, h) \in \mathbb{R}^2$, $f(x+h) - f(x-h) = 2hf'(x)$ donc

$$f'(x) = \frac{1}{2}(f(x+1) - f(x-1)) \quad (7.1)$$

donc f' est \mathcal{C}^1 et donc f est \mathcal{C}^2 . On fixe alors x et on dérive deux fois (7.1) en fonction de h . On a alors

$$f''(x+h) = f''(x-h)$$

pour tout $(x, h) \in \mathbb{R}^2$ donc f'' est constante et f est polynômiale de degré 2.

Réciproquement, si $f(x) = ax^2 + bx + c$, on a bien la relation de l'énoncé.

Solution 7.5.

1. Soit $a > 0$,

$$\begin{aligned} \tau_a : \mathbb{R} &\rightarrow]a, +\infty[\\ x &\mapsto \frac{f(x)-f(a)}{x-a} \end{aligned}$$

est croissante. Donc il existe $l = \lim_{x \rightarrow +\infty} \tau_a(x) \in \overline{\mathbb{R}}$. On écrit alors

$$\frac{f(x)}{x} = \frac{f(x) - f(a)}{x - a} \times \frac{x - a}{x} + \frac{f(a)}{x} \xrightarrow{x \rightarrow +\infty} l$$

2. S'il existe $a < b \in (\mathbb{R}_+^*)^2$ tel que $f(a) < f(b)$, alors $\tau_a(b) > 0$. Comme τ_a est croissante, $l \geq \tau_a(b) > 0$. Par contraposée, si $l \geq 0$, f est décroissante.

3. Posons pour tout $x \in \mathbb{R}_+^*$, $\varphi(x) = f(x) - lx$. Pour $x < y$, on a

$$\frac{\varphi(y) - \varphi(x)}{y - x} = \frac{f(y) - f(x)}{y - x} - l \leq 0$$

Donc φ est décroissante et $\lim_{x \rightarrow +\infty} \varphi(x) \in \overline{\mathbb{R}}$ existe.

Solution 7.6.

1. On forme

$$\begin{aligned} g : [0, 1] &\rightarrow \mathbb{R} \\ x &\mapsto \frac{1}{\frac{1}{p} + x} \end{aligned}$$

Alors

$$\sum_{k=0}^{np} \frac{1}{n+k} = \frac{1}{np} \sum_{k=0}^{np} \frac{1}{\frac{1}{p} + \frac{k}{np}} \xrightarrow{n \rightarrow +\infty} \int_0^1 \frac{dx}{\frac{1}{p} + x} = \ln(p+1) = l_p$$

2. On note $f(x) = f(0) + xf'(0) + x\varepsilon(x)$ avec $\varepsilon(x) \xrightarrow{\varepsilon \rightarrow 0} 0$.

Soit $\varepsilon_0 > 0$. Il existe $\alpha_0 > 0$ tel que si $0 < x < \alpha_0$, alors $|\varepsilon(x)| \leq \varepsilon_0$, et il existe $N_0 \in \mathbb{N}$ tel que pour tout $n \geq N_0$, $\frac{1}{n} \leq \alpha_0$. Alors pour tout $n \geq N_0$, pour tout $k \in \{0, \dots, np\}$,

$$\frac{1}{k+n} \Rightarrow \left| \varepsilon\left(\frac{1}{k+n}\right) \right| \leq \frac{\varepsilon_0}{p}$$

et

$$\left| \sum_{k=0}^{np} \frac{\varepsilon\left(\frac{1}{k+n}\right)}{k+n} \right| \leq \sum_{k=0}^{np} \frac{\frac{\varepsilon_0}{p}}{k+n} \leq \frac{\varepsilon_0}{p} \frac{np+1}{n+1} \leq \varepsilon_0$$

On a donc

$$v_n = \sum_{k=0}^{np} \frac{1}{n+k} f'(0) + \sum_{k=0}^{np} \frac{\varepsilon\left(\frac{1}{n+k}\right)}{n+k} \xrightarrow{n \rightarrow +\infty} \ln(p+1) f'(0)$$

3. On peut penser à $f: x \mapsto \sqrt{x}$ continue et $f(0) = 0$. De plus,

$$\sum_{k=0}^{np} \frac{1}{\sqrt{n+k}} \geq \frac{np+1}{\sqrt{n(p+1)}} \xrightarrow{n \rightarrow +\infty} +\infty$$

donc v_n diverge.

4. On écrit $f(x) = f(0) + xf'(0) + \frac{x^2}{2!} f''(0) + x^2 \varepsilon(x)$ avec $\varepsilon(x) \xrightarrow{\varepsilon \rightarrow +\infty} 0$. Ainsi,

$$v_n = \sum_{k=0}^{np} \frac{f''(0)}{2(n+k)^2} + \sum_{k=0}^{np} \frac{\varepsilon\left(\frac{1}{k+n}\right)}{(k+n)^2}$$

Soit $\varepsilon > 0$, il existe $N \in \mathbb{N}$ tel que pour tout $n \geq N$, pour tout $k \in \{0, \dots, np\}$,

$|\varepsilon\left(\frac{1}{n+k}\right)| \leq \varepsilon$ et donc

$$\left| \sum_{k=0}^{np} \frac{\varepsilon\left(\frac{1}{n+k}\right)}{(n+k)^2} \right| \leq \sum_{k=0}^{np} \frac{\varepsilon}{(n+k)^2}$$

donc

$$\sum_{k=0}^{np} \frac{\varepsilon\left(\frac{1}{n+k}\right)}{(n+k)^2} = O\left(\sum_{k=0}^{np} \frac{f''(0)}{2} \times \frac{1}{(n+k)^2}\right)$$

puis

$$v_n \underset{n \rightarrow +\infty}{\sim} \sum_{k=0}^{np} \frac{f''(0)}{2(n+k)^2}$$

Or

$$\begin{aligned}\sum_{k=0}^{np} \frac{1}{(n+k)^2} &= \frac{1}{(np)^2} \sum_{k=0}^{np} \frac{1}{\left(\frac{1}{p} + \frac{k}{np}\right)^2} \\ &= \frac{1}{np} \times \frac{1}{np} \underbrace{\sum_{k=0}^{np} \frac{1}{\left(\frac{1}{p} + \frac{k}{np}\right)^2}}_{\xrightarrow{n \rightarrow +\infty} \int_0^1 \frac{dx}{\left(\frac{1}{p} + x\right)^2}}\end{aligned}$$

donc

$$v_n \underset{n \rightarrow +\infty}{\sim} \frac{f''(0)p}{n(p+1)}$$

Solution 7.7. Supposons que f' ne tend pas vers 0 en $+\infty$: il existe $\varepsilon_0 > 0, \forall A > 0, \exists x_A \geq A, |f'(x_A)| \geq \varepsilon_0 > 0$. Par continuité uniforme, il existe $\alpha_0 \geq 0, \forall (x, y) \in (\mathbb{R}_+)^2$, si $|x - y| \leq \alpha_0$ alors $|f'(x) - f'(y)| \leq \frac{\varepsilon_0}{2}$. Alors pour tout $t \in [x_A - \alpha, x_A + \alpha]$, on a

$$|f'(t)| \geq |f'(x_A)| - |f'(x_A) - f'(t)| \geq \varepsilon_0 - \frac{\varepsilon_0}{2} \geq \frac{\varepsilon_0}{2}$$

et pour $A = n$, pour tout $n \in \mathbb{N}, \exists x_n \geq n, \forall t \in [x_n - \alpha, x_n + \alpha], |f'(t)| \geq \frac{\varepsilon_0}{2}$. D'après le théorème des valeurs intermédiaires, f' est de signe constant sur $[x_n - \alpha, x_n + \alpha]$. Quitte à changer f en $-f$, on peut supposer qu'il existe une infinité de $n \in \mathbb{N}$ tels que $f' > 0$ sur les $[x_n - \alpha, x_n + \alpha]$. Alors

$$f(x_n + \alpha_0) - f(x_n - \alpha_0) = \int_{x_n - \alpha_0}^{x_n + \alpha_0} f'(t) dt \geq \varepsilon_0 \alpha_0 > 0$$

mais comme $\lim_{x \rightarrow +\infty} f(x) \in \mathbb{R}$, on a

$$\lim_{n \rightarrow +\infty} f(x_n + \alpha_0) - f(x_n - \alpha_0) = 0$$

d'où la contradiction.

Si $f \in \mathcal{C}^1(\mathbb{R}_+, \mathbb{C})$, on applique ce qui précède à $\Im(f)$ et $\Re(f)$.

Si f' n'est pas uniformément continue, ce n'est plus valable, par exemple

$$f(x) = \frac{\sin(x^2)}{x} \xrightarrow{x \rightarrow +\infty} 0$$

car $|f(x)| \leq \frac{1}{x}$ et

$$f'(x) = \underbrace{-\frac{1}{x^2} \sin(x^2)}_{\xrightarrow{x \rightarrow +\infty} 0} + \underbrace{\frac{2x \cos(x^2)}{x}}_{\text{n'a pas de limite en } +\infty}$$

Solution 7.8. Soit $x \in \mathbb{R}$ et $h \neq 0$, on a

$$\frac{f(x+h) - f(x)}{h} = g(x + \frac{h}{2}) \xrightarrow{h \rightarrow 0} g(x)$$

par continuité de g . Donc f est dérivable et $f' = g$. Par ailleurs, pour $y = \frac{1}{2}$, on a

$$f'(x) = f(x + \frac{1}{2}) - f(x - \frac{1}{2})$$

par récurrence f est \mathcal{C}^∞ .

En outre, en fixant x et en dérivant la relation de départ deux fois par rapport à y , on a

$$f''(x+y) - f''(x-y) = 0$$

Donc f'' est constante donc f est un polynôme de degré plus petit que 2.

Réciproquement, on vérifie que ces fonctions marchent (avec $f' = g$).

Solution 7.9. On a

$$S_n = \sum_{k=1}^{n-1} \frac{1}{2} (f(k) + f(k+1)) - \int_k^{k+1} f(t) dt$$

On note $F(x) = \int_1^x f(t) dt$ de classe \mathcal{C}^2 .

On a

$$F(b) = F(a) + F'(a)(b-a) + \int_a^b F''(t)(b-t) dt$$

Pour $a = k$ et $b = k + \frac{1}{2}$, on a

$$F(k + \frac{1}{2}) = F(k) + \frac{1}{2} F'(k) + \int_k^{k+\frac{1}{2}} (k + \frac{1}{2} - t) f'(t) dt = F(k) + \frac{1}{2} F'(k) + \int_0^{\frac{1}{2}} u f'(k + \frac{1}{2} - u) du$$

et pour $a = k+1, b = k + \frac{1}{2}$,

$$F(k + \frac{1}{2}) = F(k+1) - \frac{1}{2} F'(k+1) + \int_{k+1}^{k+\frac{1}{2}} (k + \frac{1}{2} - t) f'(t) dt = F(k+1) - \frac{1}{2} F'(k+1) + \int_0^{\frac{1}{2}} u f'(k + \frac{1}{2} + u) du$$

On a donc

$$\frac{1}{2} (f(k) - f(k+1)) - \int_k^{k+1} f(t) dt = \int_0^{\frac{1}{2}} u (f'(k + \frac{1}{2} + u) - f'(k + \frac{1}{2} - u)) du$$

d'où

$$S_n = \int_0^{\frac{1}{2}} u \underbrace{\sum_{k=1}^{n-1} f'(k + \frac{1}{2} + u) - f'(k + \frac{1}{2} - u)}_{\geq 0 \text{ car } u \geq 0 \text{ et } f' \text{ croissante}} du$$

et $f'(k + \frac{1}{2} + u) - f'(k + \frac{1}{2} - u) \leq f'(k + 1) - f'(k)$ d'où

$$S_n \leq \underbrace{\int_0^{\frac{1}{2}} u du}_{=\frac{1}{8}} (f'(n) - f'(1))$$

Solution 7.10.

1. D'après l'inégalité de Taylor-Lagrange, on a

$$\begin{cases} \|A\| \leq \frac{h^2}{2} M_2 \\ \|B\| \leq \frac{h^2}{2} M_2 \end{cases}$$

On a $B - A - f(x - h) + f(x + h) = 2hf'(x)$ d'où

$$\|f'(x)\| \leq \frac{hM_2}{2} + \frac{M_0}{h}$$

Donc f' est bornée sur \mathbb{R} . On a ensuite un majorant qui dépend de h que l'on peut optimiser, et on trouve la borne demandée.

2. L'inégalité de Taylor-Lagrange donne à nouveau

$$\forall k \in \{1, \dots, n-1\}, \|A_k\| \leq \frac{k^n}{n!} M_n$$

On forme alors

$$\begin{pmatrix} A_1 - f(x+1) \\ \vdots \\ A_k - f(x+k) \\ \vdots \\ A_n - f(x+n) \end{pmatrix} = \underbrace{\begin{pmatrix} -1 & -1 & \dots & \frac{-1}{(n-1)!} \\ \vdots & \vdots & & \vdots \\ -1 & -k & \dots & \frac{-k^{n-1}}{(n-1)!} \\ \vdots & \vdots & & \vdots \\ -1 & -n & \dots & \frac{-n^{n-1}}{(n-1)!} \end{pmatrix}}_{=M} \begin{pmatrix} f(x) \\ \vdots \\ f^{(k)}(x) \\ \vdots \\ f^{(n-1)}(x) \end{pmatrix}$$

On a

$$\det(M) = \frac{(-1)^n}{1! \times 2! \times \dots \times (n-1)!} V(1, \dots, n)$$

où V est le déterminant de Vandermonde. Donc $\det(M) \neq 0$. On peut former les $f^{(j)}(x)$ en fonction des $(A_i - f(x+i))_{1 \leq i \leq n}$: il existe $(\alpha_1, \dots, \alpha_n) \in \mathbb{R}^n$ tel que pour tout $x \in \mathbb{R}$, $f^{(j)}(x) = \sum_{i=1}^n \alpha_i (A_i - f(x+i))$. Donc

$$\|f^{(j)}(x)\| \leq \sum_{i=1}^n |\alpha_i| \left(\frac{n}{n!} M_n + M_0 \right)$$

Donc $f^{(j)}$ est bornée pour tout $j \in \{1, \dots, n-1\}$.

Solution 7.11.

1.

$$l_{\sigma, \gamma} = \sum_{i=0}^{n-1} \left\| \int_{a_i}^{a_{i+1}} \gamma'(t) dt \right\| \leq \sum_{i=0}^{n-1} \int_{a_i}^{a_{i+1}} \|\gamma'(t)\| dt = \int_a^b \|\gamma'(t)\| dt$$

2. On a

$$\begin{aligned} \left| l_{\sigma, \gamma} - \sum_{i=0}^{n-1} \|\gamma'(a_i)\| (a_{i+1} - a_i) \right| &= \left| \sum_{i=0}^{n-1} \|\gamma(a_{i+1}) - \gamma(a_i)\| - \underbrace{\| (a_{i+1} - a_i) \gamma'(a_i) \|}_{>0} \right| \\ &\leq \sum_{i=0}^{n-1} \|\gamma(a_{i+1}) - \gamma(a_i) - (a_{i+1} - a_i) \gamma'(a_i)\| \\ &\leq \sum_{i=0}^{n-1} \int_{a_i}^{a_{i+1}} \|\gamma'(t) - \gamma'(a_i)\| dt \end{aligned}$$

3. $\|\gamma'\|$ est continue donc

$$\int_a^b \|\gamma'(t)\| dt = \lim_{\delta(\sigma) \rightarrow 0} \sum_{i=0}^{n-1} \|\gamma'(a_i)\| (a_{i+1} - a_i)$$

Donc α_0 existe.

γ' est continue sur $[a, b]$ donc uniformément continue sur $[a, b]$, et il existe $\alpha_1 > 0$ tel que pour tout $(x, y) \in [a, b]^2$, on a

$$|x - y| \leq \alpha \Rightarrow \|\gamma'(x) - \gamma'(y)\| \leq \frac{\varepsilon}{2(b-a)}$$

Alors si $\delta(\sigma) \leq \alpha_1$, pour tout $i \in \{0, \dots, n-1\}$, pour tout $t \in [a_i, a_{i+1}]$, on a

$$|t - a_i| \leq (a_{i+1} - a_i) \leq \alpha_1$$

d'où

$$\|\gamma'(a_i) - \gamma'(t)\| \leq \frac{\varepsilon}{2(b-a)}$$

et d'après la question 2, on a donc

$$\left| l_{\sigma, \gamma} - \sum_{i=0}^{n-1} \|\gamma'(a_i)\| (a_{i+1} - a_i) \right| \leq \frac{\varepsilon}{2}$$

Finalement, si $\text{@}d(\sigma) \leq \min(\alpha_0, \alpha_1)$, on a

$$\left| l_{\sigma, \gamma} - \int_a^b \|\gamma'(t)\| dt \right| \leq \varepsilon$$

Donc

$$l(\gamma) = \int_a^b \|\gamma'(t)\| dt$$

4. On a

$$\gamma'(t) = \begin{pmatrix} -R \sin(t) \\ R \cos(t) \end{pmatrix}$$

donc $\|\gamma'(t)\| = R$ et $l(\gamma) = 2\pi R$.

Solution 7.12.

1. Pour tout $t \in I$, on a

$$\gamma(t) = |\gamma(t)| e^{i\theta_1(t)} = |\gamma(t)| e^{i\theta_2(t)}$$

donc

$$e^{i(\theta_1(t) - \theta_2(t))} = 1$$

Ainsi, pour tout $t \in I$, il existe $k(t) \in \mathbb{Z}$ telle que $\theta_2(t) - \theta_1(t) = 2k(t)\pi$. On a

$$k(t) = \frac{\theta_2(t) - \theta_1(t)}{2\pi}$$

qui est continue et à valeurs entières, donc constante égale à k_0 d'après le théorème des valeurs intermédiaires.

2. Si $\gamma(t) = x(t) + iy(t)$,

$$|\gamma(t)| = \sqrt{x(t)^2 + y(t)^2}$$

Comme $\sqrt{\cdot}$ est \mathcal{C}^∞ sur \mathbb{R}_+^* , par composition, f est \mathcal{C}^k . On a alors

$$f(t) = e^{i\theta(t)} \Rightarrow f'(t) = i\theta'(t)e^{i\theta(t)} = i\theta'(t)f(t)$$

Donc

$$\theta(t) = -i \frac{f'(t)}{f(t)}$$

De plus, on a

$$\theta(t) = \theta(t_0) - i \int_{t_0}^t \frac{f'(u)}{f(u)} du$$

pour $t_0 \in I$.

3. On fixe $t_0 \in I$. Soit θ_0 un argument de $\gamma(t_0)$, on pose

$$\theta(t) = \theta_0 - i \int_{t_0}^t \frac{f'(u)}{f(u)} du$$

Comme $\frac{f'}{f}$ est \mathcal{C}^{k-1} , θ est bien \mathcal{C}^k . On forme $g(t) = e^{i\theta(t)}$ qui est de classe \mathcal{C}^k . On a

$$g'(t) = i\theta'(t)g(t) = \frac{f'(t)}{f(t)}g(t)$$

donc $\left(\frac{g}{f}\right)' = 0$, donc $\frac{g}{f}$ est constante sur I et $g(t_0) = e^{i\theta_0} = f(t_0)$ donc $g = f$ sur I .

Ainsi, pour tout $t \in I$, on a $|f(t)| = |e^{i\theta(t)}| = 1$ et si $\theta(t) = a(t) + i(t)$, on a donc

$$e^{i\theta(t)} = e^{-b(t)}e^{ia(t)}$$

donc $b(t) = 0$ et $\theta(t) \in \mathbb{R}$.

- 8 Suites et séries de fonctions
- 9 Séries entières
- 10 Intégration
- 11 Espaces préhilbertiens
- 12 Espaces euclidiens
- 13 Calcul différentiel
- 14 Équation différentielles linéaires