Partie I

1. Utilisons le développement limité usuel

$$\sqrt{1+x} = (1+x)^{1/2} = 1 + \sum_{k=1}^{p-1} a_k x^k + \underset{x\to 0}{o}(x^{p-1})$$

avec pour tout $k \in [\![1, p-1]\!]$:

$$\begin{aligned} a_k &= \frac{1}{k!}\frac{1}{2}\left(\frac{1}{2}-1\right)\dots\left(\frac{1}{2}-(k-1)\right) \\ &= \frac{1}{k!}\frac{1.(-1)(-3)\dots\big(-(2k-3)\big)}{2^k} \\ &= (-1)^{k-1}\frac{1}{k!}\frac{(2k)!}{2.4.6\dots(2k-2)(2k-1)(2k)2^k} \\ &= (-1)^{k-1}\frac{(2k)!}{2^{2k}(k!)^2(2k-1)} = \frac{(-1)^{k-1}}{2^{2k}(2k-1)}\binom{2k}{k} \end{aligned}$$

2. Il existe une fonction ε de limite nulle en 0 telle que

$$\sqrt{1+x} = P_p(x) + x^{p-1}\varepsilon(x)$$

En élevant au carré on a : $1 + x = P_p^2(x) + 2P_p(x)\varepsilon(x)\ x^{p-1} + \varepsilon(x)^2\ x^{2p-2}$ et donc

$$1 + x - P_p(x)^2 = x^{p-1}\left(2P_p(x)\varepsilon(x) + \varepsilon(x)^2 x^{p-1}\right)$$

Le terme dans la parenthèse de droite tendant vers 0 quand x tend vers 0 on a

$$1 + x - P_p(x)^2 = \underset{x\to 0}{o}(x^{p-1})$$

Posons $Q = 1+X-P_p^2$ qui est un polynôme comme différence de polynômes. On note $Q = \sum\limits_{k=0}^{d} q_k X^k$ où $d \geqslant \max(p-1, \deg(Q))$.
On peut alors obtenir le développement limité de Q en 0 :

$$Q(x) = \sum_{k=0}^{p-1} q_k x^k + \underset{x\to 0}{o}(x^{p-1})$$

Par unicité du développement limité d'ordre $p-1$ de $Q(x)$ quand $x \to 0$, on en déduit que $q_0 = q_1 = \ldots = q_{p-1} = 0$. Ainsi Q est divisible par X^p.

3. Comme $f^p = 0_{\mathscr{L}(E)} \neq f^{p-1}$, on en déduit que X^p annule f mais X^{p-1} ne l'annule pas.
Donc le polynôme minimal Π_f divise X^p mais ne divise pas X^{p-1}. Comme Π_f est unitaire et que les seuls diviseurs unitaires de X^p sont les X^k avec $k \leqslant p$, on en déduit que $\Pi_f = X^p$.

4. On a $g^2 = (P_p^2)(f) = (1 + X - (1 + X - P_p^2))(f) = \mathrm{id}_E + f - (1 + X - P_p^2)(f)$.
Or $1 + X - P_p^2$ est multiple du polynôme minimal X^p de f, donc il annule f.
Ainsi $g^2 = \mathrm{id}_E + f$.

5. On a $A^2 = \begin{pmatrix} -4 & 4 & 8 \\ -2 & 2 & 4 \\ -1 & 1 & 2 \end{pmatrix}$ et $A^3 = 0_{\mathscr{M}_3(\mathbb{R})}$.

   Par ce qui précède, on a $B^2 = I_3 + A$ en posant

$$B = P_3(A) = I_3 + \frac{1}{2}A + \frac{1}{2!}\frac{1}{2}\left(-\frac{1}{2}\right)A^2 = I_3 + \frac{1}{2}A - \frac{1}{8}A^2 = \begin{pmatrix} -1 & 4 & 0 \\ -\frac{5}{4} & \frac{13}{4} & \frac{1}{2} \\ -\frac{3}{8} & \frac{7}{8} & \frac{3}{4} \end{pmatrix}$$

Partie II

6. Comme f^{p-1} n'est pas l'endomorphisme nul, il existe $x_0 \in E$ tel que $f^{p-1}(x_0) \neq 0_E$.

   Soient $\lambda_0, \ldots, \lambda_{p-1}$ des réels tels que

$$0_E = \lambda_0 x_0 + \lambda_1 f(x_0) + \ldots + \lambda_{p-1} f^{p-1}(x_0) \quad (*)$$

   Appliquant f^{p-1} aux deux membres de cette relation, et remarquant que pour $q \geqslant p$ on a $f^q = 0_{\mathscr{L}(E)}$ car X^q est multiple du polynôme minimal X^p de f, on en déduit

$$\lambda_0 f^{p-1}(x_0) = 0_E$$

   et comme $f^{p-1}(x_0) \neq 0_E$, on en déduit que $\lambda_0 = 0_{\mathbb{R}}$.

   Appliquant maintenant f^{p-2} aux deux membres de $(*)$, on a

$$\lambda_0 f^{p-2}(x_0) + \lambda_1 f^{p-1}(x_0) = 0_E$$

   et comme λ_0 est nul, on en déduit que λ_1 l'est aussi.

   Par récurrence **forte**, on montre que tous les λ_k sont nuls : pour tout $k \in [\![0, p-1]\!]$, supposant que $\lambda_0 = \ldots = \lambda_{k-1} = 0$ et appliquant f^{p-1-k} aux deux membres de $(*)$, on en déduit que $\lambda_k = 0$.

   Comme une famille libre de E comporte au plus $\dim(E) = n$ termes, on en déduit que $p \leqslant n$. Donc X^n est multiple de X^p, polynôme minimal de f et par conséquent annule f.

7. S'il existe $g \in \mathscr{L}(E)$ tel que $g^2 = f$, alors $g^{2p-2} = f^{p-1} \neq 0_{\mathscr{L}(E)}$. Par contre, $g^{2p} = f^p = 0_{\mathscr{L}(E)}$. L'endomorphisme g est donc nilpotent et donc $g^n = 0_{\mathscr{L}(E)}$. Comme g^{2p-2} n'est pas nul, $2p-2 < n$ c'est-à-dire $2p - 1 \leqslant n$.

8. On a

$$g(x_1) = g(f(x_0)) = f(g(x_0)) = f\left(\sum_{i=0}^{n-1} a_i f^i(x_0)\right) = \sum_{i=0}^{n-1} a_i f^{i+1}(x_0) = \sum_{i=1}^{n-1} a_{i-1} x_i$$

   car $f^n = 0$.

   Pour tout $k \in [\![0, n-1]\!]$, comme f^k commute avec g (récurrence immédiate), on a :

$$g(x_k) = g(f^k(x_0)) = f^k(g(x_0)) = \sum_{i=0}^{n-1} a_i f^{i+k}(x_0) = \sum_{i=k}^{n-1} a_{i-k} x_i$$

   car $f^q = 0$ pour tout $q \geqslant n$.

   Posons $T = a_0 + a_1 X + \ldots + a_{p-1} X^{p-1}$ et $h = T(f)$.

   Comme h commute avec f et que $h(x_0) = \sum_{k=0}^{n-1} a_k f^k(x_0) = g(x_0)$, on en déduit que h prend les mêmes valeurs que g en chacun des x_k.

   Par unicité de l'endomorphisme transformant une base donnée en une famille donnée, $h = g$. Donc g est un polynôme en h.

9. Si $g^2 = \mathrm{id}_E + f$, alors $f = g^2 - \mathrm{id}_E$. Donc f est un polynôme en g et par conséquent commute avec g. Par la question précédente, g est un polynôme en f.

10. a) Comme $(P^2 - Q^2)(f) = g - h = 0$, $P^2 - Q^2$ est un polynôme annulateur de f, et par conséquent est divisible par le polynôme minimal X^n de f.

    b) On a
$$(P+Q)(P-Q) = P^2 - Q^2 = X^n R$$
    où R est un polynôme.

    Si $P+Q$ n'est pas divisible par X^n, alors $P-Q$ est divisible par X car par unicité de la décomposition en irréductibles, l'exposant de X dans un produit est la somme de ses exposants dans les facteurs du produit, et ici, l'exposant dans le produit est au moins n et l'exposant dans $P+Q$ est strictement inférieur à n donc l'exposant dans $P-Q$ est strictement positif.

    Si de plus $P-Q$ n'est pas divisible par X^n, alors de même $P+Q$ est divisible par X.

    Alors $P = \frac{1}{2}[(P+Q)+(P-Q)]$ est aussi divisible par X.

    Donc g s'écrit $g = (UX)(f) = U(f) \circ f$ avec $U \in \mathbb{R}[X]$. Or f n'est pas injective, car sinon f^n le serait, or $f^n = 0_{\mathscr{L}(E)}$ et E n'est pas réduit à $\{0_E\}$. Donc g n'est pas injective non plus.

    Or $g^2 = \mathrm{id} + f$ et $f^n = 0$ donc $(g^2 - \mathrm{id})^n = 0$ donc g est annulé par $(X^2-1)^n$. Comme g n'est pas injective, 0 est valeur propre de g donc racine de tout polynôme annulateur de g. Ainsi 0 est racine de $(X^2-1)^n$, ce qui est contradictoire.

    On en déduit que $P+Q$ ou $P-Q$ est divisible par X^n, donc annule f. Ainsi $g+h$ ou $g-h$ est l'endomorphisme nul. Donc $h = \pm g$.

    c) Par la question 4), il existe au moins un endomorphisme g tel que $g^2 = \mathrm{id} + f$. Alors on a aussi $(-g)^2 = \mathrm{id} + f$. Réciproquement, si $h^2 = \mathrm{id} + f$ alors $h = \pm g$ par la question précédente.

    Comme $g \neq 0$ (car sinon $g^2 = 0$ donc $f = -\mathrm{id}$, ce qui est faux puisque $(-\mathrm{id})^n = \pm\mathrm{id} \neq 0_{\mathscr{L}(E)}$), on a $g \neq -g$. Donc il existe exactement deux endomorphismes dont le carré est $\mathrm{id} + f$.

    Remarquant qu'un endomorphisme u vérifie $u^2 = \alpha\mathrm{id} + f$ si et seulement si $(\frac{1}{\sqrt{\alpha}}u)^2 = \mathrm{id} + \frac{1}{\alpha}f$ et que $\frac{1}{\alpha}f$ est également nilpotent d'indice n, on en déduit que cette équation a également exactement deux solutions dans $\mathscr{L}(E)$.