Feuille de TD n° 13

Applications linéaires, Factorisation de polynômes

16 décembre 2021

■ *Pour commencer . . .*

Exercice 1.
Soit $r \in \mathbb{Q}$ avec $r > 0$. Soit $n \geq 2$. On pose $P(X) = X^n - r$.

1. Factoriser $P(X)$ dans $\mathbb{C}[X]$.
2. On écrit $r = \frac{p}{q}$ avec $p, q > 0$ et $pgcd(p, q) = 1$.
   On suppose que la racine n-ème de r n'est pas un rationnel ($r^{\frac{1}{n}} \notin \mathbb{Q}$), et on suppose que n est un nombre premier.
   Montrer que pour tout $1 \leq k \leq n-1$, on a $(r^{\frac{1}{n}})^k \notin \mathbb{Q}$. (On pourra raisonner par l'absurde et utiliser des facteurs premiers.)
3. Soit $Q \in \mathbb{C}[X]$ tel que $Q \mid P$.
   Si $\deg(Q) = d$, combien vaut $|Q(0)|$?
4. On suppose encore n premier. Soient $Q, R \in \mathbb{Q}[X]$ tels que $P(X) = Q(X)R(X)$.
   Montrer que l'on a $(Q(0), R(0)) = (r, 1)$,$(r, -1)$,$(-1, r)$, ou $(1, -r)$.
   Combien vaur leur degré ?
5. En déduire que $\mathbb{Q}[X]$ possède des polynômes irréductibles de degré aussi grand que l'on veut.

---

1. On a $X^n - r = \Pi_{k=1}^{n}(X - r^{\frac{1}{n}} \exp(\frac{2ik\pi}{n})$.
2. Soit $1 \leq k \leq n-1$.
   Supposons par l'absurde que $(r^{\frac{1}{n}})^k \in \mathbb{Q}$.
   On a donc $p', q' \in \mathbb{Q}$, $p', q' > 0$, premiers entre eux, tels que $r^{\frac{k}{n}} = \frac{p'}{q'}$.
   Alors, on a $r^k = \frac{p^k}{q^k} = \frac{(p')^n}{(q')^n}$.
   Vu que p et q sont premiers entre eux, et p' et q' sont premiers entre eux, on en déduit par unicité de l'écriture d'un rationnel que $p^k = (p')^n$ et que $q^k = (q')^n$.
   On écrit $p = \Pi_{i=1}^{s} p_i^{a_i}$ et $q = \Pi_{j=1}^{m} q_j^{b_j}$. Regardons les facteurs premiers de p et de q.
   On a donc $v_{p_i}(p^k) = pv_{p_i}(p) = v_{p_i}((p')^n) = nv_{p_i}(p')$.
   Comme n est premier, et que n est premier avec k, on en déduit que n divise $v_{p_i}(p)$.
   De même, pour tout q_j facteur premier de q, on obtient $kv_{q_j}(q) = nv_{q_j}(q')$, et donc n divise $v_{q_j}(q)$ car n est premier et premier avec k.
   Mais alors, on a $p = (\Pi_{i=1}^{s} p_i^{a_i/n})^n$ et $q = (\Pi_{j=1}^{m} q_j^{b_j/m})^n$.
   Cela implique que $r = x^n$ pour un certain nombre rationnel x, ce qui est absurde.
   On en déduit donc que $r^{\frac{k}{n}}$ n'est pas un nombre rationnel.
3. Soit Q un diviseur de P de degré d dans $\mathbb{C}[X]$.
   Alors, Q se factorise comme le produit de d polynômes de la forme $(X - r^{\frac{1}{n}} \exp(\frac{2ik\pi}{n})$.
   $Q(0)$ est le coefficient constant de Q, c'est donc un produit de d nombres complexes de module $r^{\frac{1}{n}}$. On a donc $|Q(0)| = (r^{\frac{1}{n}})^d = r^{\frac{d}{n}}$.
4. D'après la question précédente, pour $d = \deg(Q)$ on a $\deg(R) = n - d$, et $|Q(0)| = r^{\frac{d}{n}}$, $|R(0)| = r^{\frac{n-d}{n}} = \frac{r}{r^{\frac{d}{n}}}$. D'après la question 2), comme n est premier, $r^{\frac{d}{n}}$ n'est pas rationnel si $1 \leq d \leq n-1$.
   Comme on a $d \in \{0, \ldots, n\}$ et comme $Q \in \mathbb{Q}[X]$, les seuls cas possibles sont $d = 0$ ou $d = n$.
   On a donc $|Q(0)| = 1$ (et $|R(0)| = r$) ou $|Q(0)| = r$ (et $|R(0)| = 1$), ce qui donne les 4 cas de l'énoncé.
5. D'après la question précédente, pour n un nombre premier et r un rationnel qui n'est pas une puissance n-ème d'un rationnel (par exemple $r = 2$), le polynôme $X^n - r$ ne possède que des diviseurs de degré 1 et de degré n dans $\mathbb{Q}[X]$.
   Ce polynôme est donc irréductible dans $\mathbb{Q}[X]$.

Exercice 2.
1. Soient $P \in \mathbb{K}[X]$ et $a \in \mathbb{K} \neq 0$.
   Montrer que $P(X)$ est irréductible si et seulement si $P(aX + b)$ est irréductible.
2. Soit $r \in \mathbb{R}_+^*$. Factoriser $X^n - r$ dans $\mathbb{R}[X]$.
3. Soit $n \geq 1$. Est-ce que $(X^2 + X + 1)^2$ divise $(X+1)^n - X^n - 1$ dans $\mathbb{Q}[X]$?

---

1. Si $P(X) = Q(X)R(X)$, alors on a $P(aX + b) = Q(aX + b)R(aX + b)$. Donc, si P est réductible, alors $P(aX + b)$ est réductible.
   Réciproquement, posons $Q(X) = P(aX + b)$. On a alors $Q(\frac{1}{a}X - \frac{b}{a}) = P(X)$. Donc si Q est réductible, alors $P(X)$ est réductible.

2. Dans $\mathbb{C}[X]$ on a $X^n - r = \Pi_{k=1}^n (X - r^{\frac{1}{n}} \exp(\frac{2ik\pi}{n})$.
Si $n = 2m+1$, on a $X^n - r = (X - r^{\frac{1}{n}})\Pi_{k=1}^m (X - r^{\frac{1}{n}} \exp(\frac{2ik\pi}{n})(X - r^{\frac{1}{n}} \exp(\frac{2i(n-k)\pi}{n})$
$X^n - r = (X - r^{\frac{1}{n}})\Pi_{k=1}^m (X - r^{\frac{1}{n}} \exp(\frac{2ik\pi}{n})(X - r^{\frac{1}{n}} \exp(\frac{2i(-k)\pi}{n})$
$X^n - r = (X - r^{\frac{1}{n}})\Pi_{k=1}^m (X^2 - r^{\frac{1}{n}} 2\cos(\frac{2k\pi}{n})X + r^{\frac{2}{n}})$
Si $n = 2m$, on a $X^n - r = (X - r^{\frac{1}{n}})(X + r^{\frac{1}{n}})\Pi_{k=1}^{m-1} (X - r^{\frac{1}{n}} \exp(\frac{2ik\pi}{n})(X - r^{\frac{1}{n}} \exp(\frac{2i(n-k)\pi}{n})$
$X^n - r = (X - r^{\frac{1}{n}})(X + r^{\frac{1}{n}})\Pi_{k=1}^{m-1} (X - r^{\frac{1}{n}} \exp(\frac{2ik\pi}{n})(X - r^{\frac{1}{n}} \exp(\frac{2i(-k)\pi}{n})$
$X^n - r = (X - r^{\frac{1}{n}})(X + r^{\frac{1}{n}})\Pi_{k=1}^{m-1} (X^2 - r^{\frac{1}{n}} 2\cos(\frac{2k\pi}{n})X + r^{\frac{2}{n}})$

3. On commence d'abord dans $\mathbb{C}[X]$. Pour $j = \exp(\frac{2i\pi}{3})$, on a $X^2+X+1 = (X-j)(X-j^2)$.
On a ainsi $1 + j + j^2 = 0$, et on sait aussi que $j^3 = 1$.
Donc, $(X^2 + X + 1)^2$ divise $P(X) = (X + 1)^n - X^n - 1$ si et seulement si $P(j) = P'(j) = P(j^2) = P'(j^2) = 0$.
Comme P est à coefficients réels, d'après le cours on a $P(j) = 0$ implique $P(\bar{j}) = P(j^2) = 0$. Même chose pour P'.
On a $P'(X) = n(X + 1)^{n-1} - nX^{n-1}$.
Donc, $P'(j) = n((j + 1)^{n-1} - j^{n-1}) = n((-j^2)^{n-1} - j^{n-1})$.
Si $n = 3k + 2$, on a $P'(j) = n((-1)^{3k+1}j^2 - j) \neq 0$.
Si $n = 3k$, on a $P'(j) = n((-1)^{3k-1}j - j^2) \neq 0$.
Si $n = 3k + 1$, on a $P'(j) = n((-1)^k - 1)$. Dans ce cas, on a $P'(j) = 0$ si et seulement si k est pair.
Donc, $P'(j) = 0$ si et seulement si $n = 6k + 1$.
On sait donc que j et j^2 sont des racines de $P'(X)$ dans ce cas.
Maintenant, regardons la divisibilité pour P.
$P(j) = (j + 1)^{6k+1} - j^{6k+1} - 1 = (-j^2)^{6k+1} - j - 1 = -j^2 - j - 1 = 0$.
On en déduit donc que j et j' sont des racines de P dans ce cas.
On a donc $(X^2 + X + 1)^2 \mid P(X)$ dans $\mathbb{C}[X]$ ssi $n = 6k + 1$.
En effectuant la division euclidienne de P par $(X^2 + X + 1)$ dans $\mathbb{Q}[X]$, on en déduit que $(X^2 + X + 1)^2 \mid P$ dans $\mathbb{Q}[X]$ ssi $n = 6k + 1$.

Exercice 3. Soit $n \geq 1$. Dans $\mathbb{R}[X]$, on définit $P(X) = (X^2 - 1)^n$.

1. Montrer que pour tout $k \geq 0$, le polynôme $P^{(k)}$ est scindé (ou nul).
2. Quelle est la multiplicité de -1 et 1 dans $P^{(k)}$, pour $k \leq n$?
3. Montrer que pour tout $0 \leq k \leq n-1$, $P^{(k)}$ possède au moins $2+k$ racines distinctes, situées dans l'intervalle $[-1, 1]$.
4. En déduire que pour tout $0 \leq k \leq n-1$, $P^{(k)}$ possède exactement $2 + k$ racines distinctes, situées dans l'intervalle $[-1, 1]$.
5. En déduire que $P^{(n)}$ est scindé à racines simples, à racines dans $]-1, 1[$.

---

1. Le polynôme P est scindé et à coefficients réels. Donc, d'après le cours, P' est scindé (ou $P' = 0$).
On montre alors par récurrence sur $k \geq 0$ que $P^{(k)}$ est scindé ou $P^{(k)} = 0$.
2. -1 et 1 sont des racines de P de multiplicité n.
Donc, d'après le cours, pour $0 \leq k \leq n-1$, -1 et 1 sont des racines de $P^{(k)}$ de multiplicité $n - k$.

3. Démontrons donc le résiltat par récurrence sur $0 \leq k \leq n-1$.
Pour $k = 0$ c'est vrai.
Supposons le résultat vrai pour $0 \leq k < n-1$.
Alors, $P^{(k)}$ possède au moins $2 + k$ racines distinctes $a_1 < a_2 < \ldots < a_{2+k}$, qui sont toutes dans $[-1, 1]$.
Comme -1 et 1 sont des racines de $P^{(k)}$, on en déduit que $a_1 = -1$ et $a_{2+k} = 1$.
D'après le théorème de Rolle, il existe donc $b_1 < \ldots < b_{k+1}$ des réels, avec $b_i \in]a_i, a_{i+1}[$ tels que $P^{(k+1)}(b_i) = 0$.
D'après la question précédente, -1 et 1 sont aussi des racines de $P^{(k+1)}$. On a donc trouvé $k + 3 = (k + 1) + 2$ racines distinctes de $P^{[k+1)}$, dans $[-1, 1]$.
Cela termine la récurrence.
4. D'après les deux questions précédentes, $P^{(k)}$ possède -1 et 1 comme racines de multiplicité $n - k$, et il possède k autres racines dans $]-1, 1[$.
Or, $P^{(k)}$ est de degré $2n - k$. Comme $(n - k) + (n - k) + k = 2n - k$, on a trouvé toutes les racines de $P^{(k)}$ comptées avec multiplicité.
5. Pour $k = n - 1$, on a $P^{(n-1)}$, polynôme de degré $n + 1$, qui possède $k + 2 = n + 1$ racines distinctes dans $[-1, 1]$.
Donc $P^{(n-1)}$ est scindé à racines simples.
D'après le cours, son polynôme dérivé, qui vaut $P^{(n)}$, est lui aussi à racines simples, situées dans $]-1, 1[$.

Exercice 4. Soit $P \in \mathbb{R}[X]$.

1. Montrer que P est à coefficients rationnels si et seulement si $P(\mathbb{Q}) \subset \mathbb{Q}$. (On pourra utiliser les polynômes d'interpolation de Lagrange)
2. Montrer que le résultat est faux si on remplace "rationnel" par "entiers" (et $\mathbb{Q}$ par $\mathbb{Z}$). (On pourra chercher un contre-exemple en utilisant le petit théorème de Fermat)

---

1. Soit $P \in \mathbb{R}[X]$.
Si $P \in \mathbb{Q}[X]$ on a bien évidemment $P(\mathbb{Q}) \subset \mathbb{Q}$.
Réciproquement, supposons que $P(\mathbb{Q}) \subset \mathbb{Q}$.
Si $P = 0$ c'est bon. Sinon, on a $\deg(P) = n \geq 0$.
On prend alors $L_0, \ldots, L_n$ les polynômes d'interpolation de Lagrange associés aux entiers $0, 1, \ldots, n$.

D'après leur définition, ces polynômes sont à coefficients rationnels.
D'après le cours, on a : $P(X) = \sum_{k=0}^{n} P(k)L_k(X)$.
Ainsi, comme $P(k) \in \mathbb{Q}$, on obtient $P \in \mathbb{Q}[X]$.

2. Soit p un nombre premier. On pose $P(X) = \frac{1}{p}X^p - \frac{1}{p}X$.
   D'après le petit théorème de Fermat, pour tout entier n, on a $n^{p-1} \equiv 1 \mathrm{mod}\ (p)$ si $pgcd(n,p) = 1$. Si $pgcd(n,p) \neq 1$, on a $p \mid n$ et donc $n \equiv 0 \mathrm{mod}\ (p)$.
   Cela se généralise en $n^p \equiv n \mathrm{mod}\ (p)$, pour tout $n \in \mathbb{Z}$.
   Donc, $p \mid n^p - n$ pour tout entier n.
   Donc, $\frac{n^p - n}{p} \in \mathbb{Z}$, $\forall n \in \mathbb{Z}$.
   On obtient donc que $P(\mathbb{Z}) \subset \mathbb{Z}$. Et pourtant le polynôme P n'est pas à coefficients entiers.

Exercice 5. Soit $P \in \mathbb{K}[X]$. Soient $a, b \in \mathbb{K}$ avec $a \neq b$.

1. Déterminer le reste de la division euclidienne de P par $(X-a)(X-b)$.
2. Soient $n \geq 1$ et $t \in \mathbb{R}$.
   Déterminer le reste dans la division euclidienne, dans $\mathbb{R}[X]$, de $P(X) = (X\cos(t) + \sin(t))^n$ par $X^2 + 1$.
3. Calculer la valeur de $P(X) = 2X^5 - 4X^4 - 2X^3 + 3X^2 - 5X - 4$ en $1 + \sqrt{2}$. (On pourra utiliser la question 1) ainsi qu'une division euclidienne)

---

1. On a $P(X) = Q(X)(X-a) + P(a)$. On a $Q(X) = Q_2(X)(X-b) + Q(b)$.
   Donc, $P(X) = Q_2(X)(X-a)(X-b) + Q(b)(X-a) + P(a)$. On a bien obtenu une division euclidienne.
   Maintenant, on a $P(b) = Q(b)(b-a) + P(a)$, donc $Q(b) = \frac{P(b)-P(a)}{b-a}$.
   Donc, le reste vaut $\frac{P(b)-P(a)}{b-a}(X-a) + P(a)$.

2. Comme $P(X)$ et X^2+1 sont à coefficients réels, leur division euclidienne dans $\mathbb{C}[X]$ est identique à leur division euclidienne dans $\mathbb{R}[X]$. (la div. eucl. dans $\mathbb{R}$ peut être vue dans $\mathbb{C}$, et il y a unicité).
   On effectue donc tous les calculs dans $\mathbb{C}[X]$.
   On a alors $X^2 + 1 = (X-i)(X+i)$.
   Donc, le reste de $P(X)$ dans la division euclidienne par X^+1, dans $\mathbb{C}[X]$, vaut :
   $R(X) = \frac{P(i)-P(-i)}{i-(-i)}(X-(-i)) + P(-i) = -i\frac{P(i)-P(-i)}{2}(X+i) + P(-i)$.
   $R(X) = -i\frac{P(i)-P(-i)}{2}X + P(-i) + i(-i)\frac{P(i)-P(-i)}{2} = -i\frac{P(i)-P(-i)}{2}X + \frac{P(i)+P(-i)}{2}$.
   Comme $P \in \mathbb{R}[X]$, on a $P(-i) = \overline{P(i)}$, donc :
   $R(X) = Im(P(i))X + Re(P(i))$. On a $P(i) = (i\cos(t) + \sin(t))^n = \exp(it - \frac{i\pi}{2})^n = \exp(ni(t - \frac{\pi}{2})$,
   donc $R(X) = \sin(n(t-\frac{\pi}{2})X + \cos(n(t-\frac{\pi}{2}))$.

3. On pose $x = 1 + \sqrt{2}$. Alors, on a $(x-1)^2 = 2$, donc x est une racine de $(X-1)^2 - 2 = X^2 - 2X - 1$.
   On effectue la division euclidienne de P par $X^2 - 2X - 1$. Après calculs, le reste vaut $X - 1$.
   Les racines de $X^2 - 2X - 1$ sont $a = 1 + \sqrt{2}$ et $b = 1 - \sqrt{2}$.
   On a donc : $X - 1 = \frac{P(b)-P(a)}{b-a}(X-a) + P(a) = \frac{P(b)-P(a)}{b-a}X + P(a) - a\frac{P(b)-P(a)}{b-a}$
   $X - 1 = \frac{P(b)-P(a)}{b-a}X + \frac{bP(a)-aP(b)}{b-a}$
   $(b-a)(X-1) = (P(b)-P(a))X + (bP(a) - aP(b))$
   $-2\sqrt{2}(X-1) = (P(b)-P(a))X + (P(a)-P(b)) - \sqrt{2}(P(a)+P(b))$.
   Avec les coefficients, on en déduit que $P(b) - P(a) = -2\sqrt{2}$, et que $-1 = -2\sqrt{2} - \sqrt{2}(P(a)+P(b))$.
   Donc, $P(a) - P(b) = 2\sqrt{2}$ et $P(a) + P(b) = -2 + \frac{1}{\sqrt{2}} = -2 + \frac{\sqrt{2}}{2}$.
   On obtient ainsi : $P(a) = \sqrt{2} - 1 + \frac{\sqrt{2}}{4} = -1 + \frac{5}{4}\sqrt{2}$.

Exercice 6. [Bonus] Résoudre dans $\mathbb{C}[X]$ l'équation $P(X^2) + P(X)P(X+1) = 0$.

Soit $P \in \mathbb{C}[X]$ solution de l'équation.
Si $P = a_0$, on obtient $a_0 + a_0^2 = 0$, donc $a_0 = 0$ ou $a_0 = 1$.
Supposons maintenant que $\deg(P) \geq 1$.
On est dans $\mathbb{C}[X]$, donc le polynôme P est scindé.
L'équation se réécrit : $P(X^2) = -P(X)P(X+1)$.
Pour $P(X) = a\Pi_{i=1}^{r}(X - z_i)^{a_i}$, on a $P(X^2) = \Pi_{i=1}^{r}(X^2 - z_i)^{a_i}$.
Pour $z_1, \ldots, z_r$ les racines de P, les racines de $P(X^2)$ sont exactement les racines carrées des z_i.
Si z_i possède deux racines carrées complexes $\pm w_i$, alors w_i et $-w_i$ sont de multiplicité a_i dans $P(X^2)$.
Si $z_1 = 0$, alors 0 est de multiplicité $2a_i$ dans $P(X^2)$.
Les racines de $P(X+1)$ sont les $z_i - 1$. On va étudier plus en détail les racines de P.
Soit $z \in \mathbb{C}$ une racine de P.
On a donc $P(z^2) + 0 = 0$. Donc, z^2 est une racine de P.
On en déduit par récurrence sur n que z^{2^n} sont des racines de P, pour tout $n \geq 2$.
Comme P est un polynôme non-constant, il a un nombre fini de racines.
Il existe donc deux entiers $n < m$ tels que $z^{2^n} = z^{2^m}$.
Si $|z| > 1$, c'est impossible (ils sont tous de module différent).
De même, si $|z| < 1$ et $z \neq 0$, c'est impossible.
On doit donc avoir $z = 0$ ou $|z| = 1$.
Donc, les racines de $P(X^2)$ sont elles-aussi nulles ou de module 1.
D'après ce que l'on a dit précédemment, pour z_i une racine de P, $z_i - 1$ est une racine de

$P(X+1)$, donc une racine de $P(X^2)$. Donc $z_i - 1$ doit être encore nul ou de module 1.
Les seuls nombres complexes qui vérifient cela sont : 1, 0, $w = \frac{1+i\sqrt{3}}{2}$,$\overline{w} = \frac{1-i\sqrt{3}}{2}$.
On a $1-1=0$, $0-1=-1$, $w-1 = j = \exp(\frac{2i\pi}{3})$, $\overline{w}-1 = j^2$.
On a $w = \exp(\frac{i\pi}{3})$, donc les racines carrées de w sont $\pm\exp(\frac{i\pi}{6})$.
Ces nombres complexes ne sont pas des racines de $P(X)$, ni des racines de $P(X+1)$, donc ils ne peuvent pas être des racines de $P(X^2)$. Ainsi, la multiplicité de w dans $P(X)$ vaut 0.
De même, la multiplicité de $\overline{w}$ dans $P(X)$ vaut 0.
On a donc $P(X) = aX^{a_1}(X-1)^{a_2}$, et
$P(X+1) = a(X+1)^{a_1}(X)^{a_2}$, et
$P(X^2) = aX^{2a_1}(X-1)^{a_2}(X+1)^{a_2}$.
Le coefficient dominant de P vérifie $a = -a^2$, donc $a = -1$ (car il est non-nul).
On doit aussi avoir $a_1 = a_2$.
On vérifie que pour $P(X) = -X^{a_1}(X-1)^{a_1}$, on a bien $P(X^2) = -P(X)P(X+1)$.

■ *Un peu de Géométrie . . .*

Exercice 7. On considère les sous-espaces vectoriels de $\mathbb{R}^4$

$$F = \left\{(x,y,z,t) \in \mathbb{R}^4, |\ \ x+y=0,\ z+t=0\right\}$$

$$\text{et} \quad G = \text{Vect}\left\{(1,1,0,0),(1,1,1,1)\right\}.$$

1. Montrer que F et G sont supplémentaires.
2. Déterminer la matrice du projecteur p sur F parallèlement à G dans la base canonique.
3. Calculer la matrice de la symétrie s par rapport à F parallèlement à G dans la base canonique.

---

1. Soit $x \in F \cap G$. Il existe λ et μ tels que $x = (\lambda+\mu, \lambda+\mu, \mu, \mu)$. De plus, x appartient à F. Donc $2\lambda + 2\mu = 0$ et $2\lambda + 4\mu = 0$. Donc $\lambda = \mu = 0$. D'où $x = 0$.
   Maintenant F est de dimension 2 car $((1,-1,0,0),(0,0,1,-1))$ en est une base et G est aussi de dimension 2 car engendré par deux vecteurs indépendants. Donc $\dim(F \oplus G) = 4$, donc $F \oplus G = \mathbb{R}^4$.
2. On considère la famille de vecteurs

$$\mathcal{B} = ((1,-1,0,0),(0,0,1,-1),(1,1,0,0),(0,0,1,1)).$$

Cette famille est une base de $\mathbb{R}^4$. De plus, $(1,-1,0,0)$, $(0,0,1,-1) \in F$ et $(1,1,0,0)$, $(0,0,1,1) \in G$. Donc la matrice de p dans la base $\mathcal{B}$ est

$$\text{Mat}_{\mathcal{B}}(\text{p}) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Donc la matrice de la projection sur F parallèlement à G dans la base canonique est égale à :

$$P\text{Mat}_{\mathcal{B}}(\text{p})\text{P}^{-1}$$

où $P = \begin{pmatrix} 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & -1 & 0 & 1 \end{pmatrix}$. La matrice P^{-1} est alors égale à $\frac{1}{2}\begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$.
Donc la matrice de p dans la base canonique est :

$$\begin{aligned} P\text{Mat}_{\mathcal{B}}(\text{p})\text{P}^{-1} &= \begin{pmatrix} 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & -1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 1 & 0 & 1 & 0 \\ -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & -1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \\ &= \frac{1}{2}\begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix} \end{aligned}$$

3. On a $s = 2p - Id$. La matrice de la symétrie s dans la base canonique est donc :

$$\begin{pmatrix} 1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}.$$

Exercice 8. Soit $u = (1,1,1) \in \mathbb{R}^3$ et (e_1, e_2, e_3) la base canonique de $\mathbb{R}^3$. Soit $f : \mathbb{R}^3 \to \mathbb{R}^3$ l'endomorphisme défini par :

$$\forall (x,y,z) \in \mathbb{R}^3,\ \ f(x,y,z) = xe_1 + ye_2 + ze_3 - \frac{x+y+z}{3}\,u.$$

1. Écrire la matrice A de f dans la base canonique de $\mathbb{R}^3$.
2. Déterminer une base du noyau et une base de l'image de f.
   Montrer que $\text{Ker}\, f \oplus \text{Im}\, f = \mathbb{R}^3$.

3. Montrer que l'ensemble des vecteurs $v \in \mathbb{R}^3$ tels que $f(v) = v$ est un sous-espace vectoriel de $\mathbb{R}^3$ et en déterminer une base.
4. Montrer que f est un projecteur. Sur quel sous-espace vectoriel, parallèlement à quel sous-espace vectoriel ?
5. Trouver une matrice P inversible telle que

$$P^{-1}AP = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

---

1. La matrice A de f dans la base (e_1, e_2, e_3) est

$$A = \frac{1}{3}\begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & -1 \\ -1 & -1 & 2 \end{pmatrix}.$$

2. Puisque f est l'endomorphisme canoniquement associé à A, on a $\operatorname{Ker}(f) = \left\{X \in \mathbb{R}^3 \mid AX = 0\right\}$. On résout donc

$$\left\{\begin{array}{rrrcl} 2x & -y & -z & = & 0 \\ -x & +2y & -z & = & 0 \\ -x & -y & +2z & = & 0 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rrrcl} 2x & -y & -z & = & 0 \\ -3x & +3y & +0 & = & 0 \\ 3x & -3y & +0 & = & 0 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcl} x & = & z \\ x & = & y \end{array}\right.$$

   Donc $\operatorname{Ker}(f) = \mathbb{R}(1,1,1)$.
   L'image de f est engendrée par les colonnes C_1, C_2 et C_3 de A. Or $C_3 = -C_1 - C_2$ et (C_1, C_2) est une famille libre. Donc $\operatorname{Im} f = \operatorname{vect}((2,-1,-1), (-1,2,-1))$.
   Soit $(x,y,z) \in \operatorname{Im}(f) \cap \operatorname{Ker}(f)$. Il existe λ et μ tels que $(x,y,z) = (2\lambda - \mu, -\lambda + 2\mu, -\lambda - \mu)$, et on a $2\lambda - \mu = 2\mu - \lambda = \lambda - \mu$. Donc $\lambda = \mu = 0$. Donc $\operatorname{Im} f$ et $\operatorname{Ker}(f)$ sont en somme directe. Par un argument de dimension, ils sont supplémentaires.
3. Soit $F = \left\{v \in \mathbb{R}^3 \mid f(v) = v\right\} = \operatorname{Ker}(f - \operatorname{Id}_{\mathbb{R}^3})$, donc F est un sous-espace vectoriel de $\mathbb{R}^3$.
   Le vecteur (x,y,z) appartient à F si et seulement si $x + y + z = 0$. On a donc $\operatorname{Ker}(f - \operatorname{Id}_{\mathbb{R}^3}) = \operatorname{vect}((2,-1,-1), (-1,2,-1)) = \operatorname{Im} f$.
4. Nous avons montré que le noyau et l'image de f sont deux sous-espaces vectoriels supplémentaires de $\mathbb{R}^3$. De plus, nous venons de remarquer que pour tout $x \in \operatorname{Im}(f)$, $f(x) = x$. Donc f est une projecteur sur $\operatorname{Vect}((2,-1,-1),\ (-1,2,-1))$ et parallèlement à $\operatorname{Vect}(1,1,1)$.
5. Dans la base $((1,1,1),\ (2,-1,-1),\ (-1,2,-1))$ la matrice de f est

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Donc par changement de base, on a :

$$P^{-1}AP = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

où $P = \begin{pmatrix} 1 & 2 & -1 \\ 1 & -1 & 2 \\ 1 & -1 & -1 \end{pmatrix}$.