Devoir à la maison n°7
CORRECTION

Problème 1. Valeur prise par une fonction au voisinage de $+\infty$

On fixe dans tout l'exercice une fonction $f : \mathbb{R} \to \mathbb{R}$ quelconque. On considère l'ensemble :

$$X_f = \{y \in \mathbb{R} \mid \forall\, A \in \mathbb{R}, \exists\, x \geqslant A, f(x) = y\}$$

1. Pour tout $y \in f([0,T])$, $\exists\, x_0 \in [0,T]$ tel que $f(x) = y$.
   Puis, par parité, la suite $u_n = f(x_0 + nT)$ est constante ($u_{n+1} = u_n$),
   donc pour tout $n \in \mathbb{N}$, $f(x_0 + nT) = f(x_0) = y$.
   Et donc pour tout $A \in \mathbb{R}$, $\exists\, n = \lfloor \frac{A}{T} \rfloor + 1$ tel que $x_0 + nT > A$ car $nT > A$ et $f(x_0 + nT) = y$.
   Donc $y \in X_f$. On a l'inclusion $f([0,T] \subset X_f$.
   Réciproquement, comme f est T-périodique, $f([0,T]) = f(\mathbb{R})$.
   Et donc si $y \notin f([0,T])$, $y \notin f(\mathbb{R})$ donc nécessairement, pour tout $x \in \mathbb{R}$, $f(x) \neq y$ et $y \notin X_f$.

   $$\boxed{\text{Par double inclusion : } X_f = f([0,T])\big(= f(\mathbb{R})\big)}$$

2. Si X_f est non vide et que $y \in X_f$.
   Alors nécessairement il existe $x \in \mathbb{R}$ tel que $f(x) = y$.
   Et en prenant $A > x$, il existe $x' > A$ tel que $y = f(x')$.
   Or f est injective, donc $f(x) = f(x')(= y)$ implique $x = x'$ et pour tout $x < A < x'$.
   On a donc une contradiction et donc

   $$\boxed{\text{l'ensemble } X_f \text{ est vide.}}$$

3. Soit $y \in \mathbb{R}$.
   Comme $f \to \infty$, on peut affirmer

   $$\forall\, M > 0, \exists\, A > 0 \text{ tel que } x > A \longrightarrow f(x) > M$$

   En prenant $M = y + 1$, à partir d'un rang $A > 0$, pour tout $x > A$, $f(x) > M$ donc $f(x) > y$.
   Ainsi $y \notin X_f$.

   $$\boxed{\forall\, y \in \mathbb{R}, y \notin X_f \text{ i.e. } X_f = \emptyset}$$

4. On suppose que la fonction f admet en $+\infty$ une limite réelle ℓ.
   (a) Soit $y \in X_f$.
   Pour tout $\epsilon > 0$, il existe $A > 0$ tel que pour $x \geqslant A$, $|f(x) - \ell| < \epsilon$.
   Or comme $y \in X_f$, il existe $x \geqslant A$ tel que $f(x) = y$.
   On a donc pour tout $\epsilon > 0$, $\exists\, A > 0$, $\exists\, x > A$ tel que $|f(x) - \ell| < \epsilon$ et $f(x) = y$.
   Ainsi pour tout $\epsilon > 0$, $\exists\, A > 0$, $\exists\, x > A$ tel que $|f(x) - \ell| < \epsilon$ et $|y - \ell| < \epsilon$.
   A et x ne servent plus :

   $$\forall\, \epsilon > 0, |f(x) - \ell| < \epsilon \Longrightarrow f(x) = \ell$$

   $$\boxed{X_f \subset \{\ell\}}$$

   Remarques !
   On n'a bien démontré qu'une inclusion et non une égalité ! !

   (b) Premier cas $X_f = \emptyset$, donc $X_f \neq \{\ell\}$.
   Considérons $f : x \mapsto \frac{1}{x} + \ell$, alors $\lim_{+\infty} f = \ell$.
   Et pourtant $\ell \notin f(\mathbb{R})$, donc $\ell \notin X_f$. Second cas, $X_f = \{\ell\}$.
   Il suffit de considérer $f : x \mapsto \ell$, constante.

   $$\boxed{\text{L'inclusion réciproque peut être vraie ou fausse.}}$$

5. I est un intervalle de $\mathbb{R}$ si $\forall\ y_1 < y_2 \in I$, $[y_1, y_2] \subset I$.
   Soient $y_1 < y_2 \in X_f$.
   Soit $t \in [y_1, y_2]$.
   Soit $A > 0$, il existe $x_1, x_2 \geqslant A$ tel que $y_1 = f(x_1)$ et $y_2 = f(x_2)$.
   f est continue, on applique le théorème des valeurs intermédiaires :

$$\exists\ x \in [x_1, x_2] \text{ (ou } [x_2, x_1]) \mid t = f(x)$$

   et nécessairement $x \geqslant A$.
   Ainsi, $\forall\ t \in [y_1, y_2]$, $\forall\ A > 0$, $\exists\ x \geqslant A$ tel que $f(x) = t$
   $\forall\ t \in [y_1, y_2]$, $t \in X_f$ $\quad [y_1, y_2] \subset X_f$.

$$\boxed{X_f \text{ est un intervalle de } \mathbb{R}}$$

Problème 2. Etude d'une fonction

On considère la fonction numérique f de la variable réelle x définie par :

$$f(0) = 0 \qquad \text{et} \qquad \forall\ x \neq 0, f(x) = \frac{1}{x^2} \times \exp(-\frac{1}{x})$$

1. Représentation de la fonction f.
   (a) Par croissance comparée : $\lim_{t\to+\infty} t^2 e^{-t} = 0$, donc en composant avec $x = \frac{1}{t}$, $\lim\limits_{x\to 0^+} f(x) = 0$.
   et $\lim_{t\to-\infty} t^2 e^{-t} = +\infty$, donc en composant avec $x = \frac{1}{t}$, $\lim\limits_{x\to 0^-} f(x) = +\infty$.

$$\boxed{f \text{ n'est pas continue en } 0 \text{ (elle est au moins continue à droite)}}$$

   On a donc évidemment $\dfrac{f(x) - f(0)}{x - 0}$ qui n'admet pas de limite pour $x \to 0^-$.
   en revanche, comme $\lim_{t\to+\infty} t^3 e^{-t} = 0$, avec $x = \frac{1}{t}$:

$$\frac{f(x) - f(0)}{x - 0} = \frac{1}{x^3}\exp(-\frac{1}{x}) \underset{x\to 0^+}{\longrightarrow} 0$$

$$\boxed{f \text{ est dérivable à droite en } 0, \text{ avec } f'(0^+) = 0 \text{ - mais non dérivable à gauche}}$$

   (b) f est dérivable sur $\mathbb{R}^*$ (fonctions de référence) et pour tout $x \neq 0$

$$f'(x) = \left(\frac{1}{x^4} - \frac{2}{x^3}\right)\exp(-\frac{1}{x}) = \frac{1 - 2x}{x^4}\exp(-\frac{1}{x})$$

$$f'(x) \geqslant 0 \qquad \Longleftrightarrow \qquad x \leqslant \frac{1}{2}$$

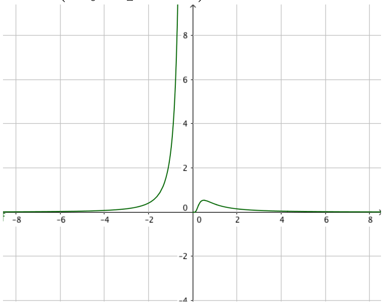
x	$-\infty$		0		$\frac{1}{2}$		$+\infty$
$f'(x)$		$+$	$\|\|$	$+$	0	$-$	
$f(x)$	0	$\nearrow +\infty$	$\|\|$	$0 \nearrow$	$4e^{-2}$	$\searrow$	0

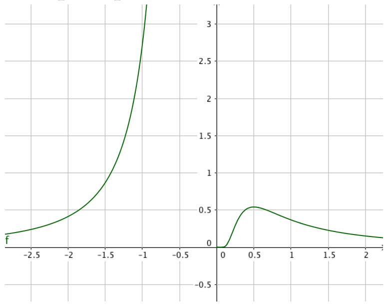
   car $f(\frac{1}{2}) = 4e^{-2} \approx 0,54$ $\lim\limits_{\pm\infty} f(x) = 0$ (aucune forme indéterminée).
   Par ailleurs, pour u au voisinage de 0, $e^u \underset{u\to 0}{\sim} 1$.
   donc par composition, pour $x \to \pm\infty$, $\frac{1}{x^2}e^{-\frac{1}{x}} \underset{x\to\mathcal{A}\infty}{\sim} \frac{1}{x^2} > 0$ $\quad$ ainsi en $\pm\infty$, $\mathcal{C}_f$ admet une asymptote horizontale d'équation $y = 0$ et $\mathcal{C}_f$ est situé « au dessus ».

Remarques !

Le tableau de variations donne déjà ces informations, le calcul de l'équivalent n'est pas nécessaire

(c) Vu de loin (asymptotes) et de plus près





2. Dérivées successives de la fonction f et polynômes associés.

(a) f est le produit de deux fonctions de classe $\mathcal{C}^\infty$ sur $]0,+\infty[$,

$$\boxed{\text{donc } f \text{ est de classe } \mathcal{C}^\infty \text{ sur }]0,+\infty[.}$$

(b) On va démontrer ce résultat par récurrence, mais considérons d'abord la suite (P_n) de polynômes définie par récurrence par $P_0 = 1$ et $\forall\ n \in \mathbb{N}$, $P_{n+1} = X^2 P_n' + [1-2(n+1)X]P_n$.
Il s'agit bien d'une suite de polynômes : P_0 est un polynôme et si P_n est un polynôme, il en est de même de P_{n+1}.

Puis notons, pour tout entier $n \in \mathbb{N}$, $\mathcal{P}_n$: « $\forall\ x > 0,\ f^{(n)}(x) = \dfrac{P_n(x)}{x^{2n+2}} \times e^{-\frac{1}{x}}$ ».

— Pour tout $x > 0$, $f^{(0)}(x) = f(x) = \dfrac{1}{x^2} e^{-\frac{1}{x}} = \dfrac{P_0}{x^{2\times 0+2}} e^{-\frac{1}{x}}$.
Ainsi $\mathcal{P}_0$ est vraie.

— Soit $n \in \mathbb{N}$. Supposons que $\mathcal{P}_n$ est vraie.
Pour tout $x > 0$, (en exploitant $\mathcal{P}_n$) :

$$f^{(n+1)}(x) = [f^{(n)}]'(x) = \left(\frac{P_n(x)}{x^{2n+2}} \times \frac{1}{x^2} + \frac{x^{2n+2} \times P_n'(x) - (2n+2)x^{2n+1} \times P_n(x)}{x^{2(2n+2)}}\right) e^{-\frac{1}{x}}$$

$$= \left(\frac{P_n(x) + x^2 P_n'(x) - (2n+2)xP_n(x)}{x^{2n+4}}\right) e^{-\frac{1}{x}} = \frac{P_{n+1}(x)}{x^{2(n+1)+2}} e^{-\frac{1}{x}}$$

Donc $\mathcal{P}_{n+1}$ est vérifiée.

$$\boxed{\begin{array}{c}\text{Pour tout } n \in \mathbb{N}, \text{ tout } x \in]0,+\infty[,\ f^{(n)}(x) = \dfrac{P_n(x)}{x^{2n+2}} \times e^{-\frac{1}{x}} \\ \text{avec pour tout } n \in \mathbb{N},\ P_{n+1} = X^2 P_n' + [1-2(n+1)X]P_n \text{ et } P_0 = 1.\end{array}}$$

(c) On a vu $P_0 = 1$.
Puis $P_1 = X^2 P_0' + (1-2X)P_0 = 1 - 2X$
Puis $P_2 = X^2 P_1' + (1-4X)P_1 = -2X^2 + 1 - 6X + 8X^2 - 2X^2 = 1 - 6X + 6X^2$
Puis $P_3 = X^2 P_2' + (1-6X)P_2 = (-6X^2 + 12X^3) + (1 - 12X + 42X^2 - 36X^3)$
$= 1 - 12X + 36X^2 - 24X^3$.
Et enfin $P_4 = X^2 P_3' + (1-8X)P_3$
$= (-12X^2 + 72X^3 - 72X^4) + (1 - 20X + 132X^2 - 312X^3 + 192X^4)$
$= 1 - 20X + 120X^2 - 240X^3 + 120X^4$

$$\boxed{\begin{array}{c}P_0 = 1, \quad P_1 = 1 - 2X, \quad P_2 = 1 - 6X + 6X^2 \\ P_3 = 1 - 12X + 36X^2 - 24X^3 \quad P_4 = 1 - 20X + 120X^2 - 240X^3 + 120X^4\end{array}}$$

(d) *On note $[T]_h$, le coefficient situé devant X^h dans le polynôme T.*
Les premiers exemples montre que $\deg(P_n) = n$, que $[P_n]_0 = 1$ et $[P_n]_n = (-1)^n(n+1)!$.
Montrons ce résultat par récurrence.
Notons, pour tout entier $n \in \mathbb{N}$, $\mathcal{Q}_n$: « $\deg(P_n) = n$, $[P_n]_0 = 1$ et $[P_n]_n = (-1)^n(n+1)!$ ».

— $\mathcal{Q}_0$ est vraie (ainsi que $\mathcal{Q}_1$, $\mathcal{Q}_2$, $\mathcal{Q}_3$ et $\mathcal{Q}_4$).

— Soit $n \in \mathbb{N}$. Supposons que $\mathcal{Q}_n$ est vraie.
On peut donc affirmer que $P_n = 1 + a_1 X + \cdots + a_{n-1}X^{n-1} + (-1)^n(n+1)!X^n$.
Alors

$$\begin{aligned}P_{n+1} &= X^2 P_n' + (1-2(n+1)X)P_n \\ &= X^2(a_1 + \cdots + (n-1)a_{n-1}X^{n-2} + (-1)^n(n+1)! \times nX^{n-1}) \\ &\quad +(1 + (a_1 - 2(n+1))X + \cdots + (a_{n-1} - 2(n+1)a_{n-2})X^{n-1} - 2(n+1)(-1)^n(n+1)!X^{n+1} \\ &= 1 + (a_1 - 2(n+1))X + \cdots + (a_{k+1} - 2(n+1)a_k + ka_k)X^{k+1} \\ &\quad + \cdots + (a_n - 2(n+1)a_{n-1} + (n-1)a_{n-1})X^n + (-2(n+1)(-1)^n(n+1)! + (-1)^n n(n+1)!)X^{n+1}\end{aligned}$$

On vérifie bien que P_{n+1} est de degré $n+1$, son coefficient constant est $[P_{n+1}] = 1$ et le coefficient de plus haut degré est

$$[P_{n+1}]_{n+1} = -2(n+1)(-1)^n(n+1)!+(-1)^n n(n+1)! = (-1)^n(-2n-2+n)(n+1)! = (-1)^{n+1}(n+2)!$$

Ainsi $\mathcal{Q}_{n+1}$ est vérifiée

$$\boxed{\text{Bilan : } \forall\, n \in \mathbb{N},\ \deg(P_n) = n+1,\ [P_n]_0 = 1 \text{ et } [P_n]_{n+1} = (-1)^n n!}$$

Remarques !

On n'est pas obligé de calculer explicitement les coefficients de P_n et se contenter de voir que $\deg P_n = n$, donc $\deg P_n' = n-1$ donc $\deg(X^2P_n') = n+1$ ainsi que $\deg((1-2(n+1)X)P_n = n+1$.

Donc $\deg(P_{n+1}) \leqslant n+1$.

Puis on calcule $[P_{n+1}]_{n+1}$ pour s'assurer qu'il est non nul.

$[P_{n+1}]_{n+1} = n[P_n]_n - 2(n+1)[P_n]_n = -(n+2)[P_n]_n \ldots$

(e) Et donc on a l'équivalent :

$$f^{(n)}(x) \underset{x\to 0}{\sim} \frac{1}{x^{2n+2}} e^{-\frac{1}{x}} \underset{x\to 0}{\longrightarrow} 0$$

$$\boxed{\text{Pour tout } n \in \mathbb{N},\ f^{(n)} \text{ admet une limite à droite nulle en } 0}$$

Soit $n \in \mathbb{N}$. Le théorème de prolongement de la fonction qui la rend de classe $\mathcal{C}^1$, s'applique n fois.
Donc $f_{|[0,+\infty[}$ est de classe $\mathcal{C}^n$, ceci pour tout entier n.

$$\boxed{\text{la fonction } f_{|[0,+\infty[} \text{ est de classe } \mathcal{C}^\infty.}$$

3. Nouvelles relations entre les polynômes P_n.
On considère la fonction $g : \mathbb{R} \to \mathbb{R},\ x \to x^2 f(x)$.

(a) Pour tout $x \neq 0$,

$$g'(x) = 2xf(x) + x^2 f'(x) = \left(\frac{2}{x} + \frac{1-2x}{x^2}\right) e^{-\frac{1}{x}} = \frac{1}{x^2} e^{-\frac{1}{x}} = f(x)$$

Puis en dérivant n fois cette relation : pour tout $n \in \mathbb{N}$, tout $x \neq 0$, $g^{(n+1)}(x) = f^{(n)}(x)$. On se contente du résultat sur $\mathbb{R}_+$ (en prolongeant en 0) :

$$\boxed{\text{pour tout } n \in \mathbb{N},\ g^{(n+1)}_{|\mathbb{R}_+} = f^{(n)}_{|\mathbb{R}_+}.}$$

(b) On applique la formule de Leibniz, car par produit, g est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}_+$. On note $t_2 : x \mapsto x^2$. Pour tout $n \in \mathbb{N}$, $x > 0$,

$$\begin{aligned} g^{(n+1)}(x) &= \sum_{k=0}^{n+1} \binom{n+1}{k} t_2^{(k)}(x) f^{(n+1-k)}(x) \\ f^n(x) &= x^2 f^{(n+1)}(x) + 2(n+1)xf^{(n)}(x) + (n+1)nf^{(n-1)}(x) \\ \frac{P_n(x)}{x^{2n+2}} &= \frac{P_{n+1}(x) + 2(n+1)xP_n(x) + n(n+1)x^2 P_{n-1}(x)}{x^{2n+2}} \end{aligned}$$

Par unicité d'écriture,

$$\boxed{\forall\, x \in]0,+\infty[,\ P_{n+1}(x) = [1-2(n+1)x]P_n(x) - n(n+1)x^2 P_{n-1}(x)}$$

(c) En liant les deux relations connues sur la famille de polynômes (P_n) :

$$P_{n+1} = X^2 P_n' + (1-2(n+1)X)P_n = [1-2(n+1)X]P_n(x) - n(n+1)X^2 P_{n-1}(X)$$

Remarques !

On peut « identifier » x et X. x est normalement une variable réelle et X le formalisme de la multiplication.

En fait le polynôme en X possède une infinité de racines : tous les $x \in \mathbb{R}_+$, cela signifie donc que le polynôme est identiquement nul et que l'on peut écrire la relation au niveau du polynôme (en X).

$$\boxed{\forall\ x \in]0,+\infty[, P_n'(x) = -n(n+1)P_{n-1}(x) \text{ ou encore } P_n'(X) = -n(n+1)P_{n-1}(X)}$$

Remarques !

Cela permet de vérifier les calculs fait précédemment :

Ainsi $P_3 = 1 - 12X + 36X^2 - 24X^3$, *donc* $P_3'(X) = -12 + 72X - 72X^2 = -12(1 - 6X + 6X^2) = -12P_2$

et $P_4 = 1 - 20X + 120X^2 - 240X^3 + 120X^4$ *donc* $P_4'(X) = -20 + 240X - 720X^2 + 480X^3 = -20P_3$

4. Etude des racines du polynôme P_n.
On notera $p_n : \mathbb{R} \to \mathbb{R}$ la fonction polynomiale associée au polynôme P_n.
   (a) Soit $n \in \mathbb{N}$ et $n \geqslant 2$. Soit $x > 0$
   Supposons que $p_n(x) = p_{n-1}(x) = 0$.
   Comme $p_n(x) = [1 - 2nx]p_{n-1}(x) - n(n-1)x^2 p_{n-2}(x)$, et $x \neq 0$: $p_{n-2}(x) = 0$.
   Et ainsi, par récurrence rétrograde (ou raisonnement par l'absurde...) $p_0(x) = 0$.
   Or $p_0 = 1$. Ce qui est impossible.

$$\boxed{\text{pour tout } n \in \mathbb{N}^* \text{ et tout } x > 0,\ p_n(x) \neq 0 \text{ ou } p_{n-1}(x) \neq 0}$$

   (b) Soit $n \in \mathbb{N}$ et $x > 0$ tel que $p_n(x) = 0$.
   Alors $p_{n-1}(x) \neq 0$ d'après la question précédente. Puis $p_n'(x) = -n(n+1)p_{n-1}(x) \neq 0$.
   On a donc au voisinage de x, l'équivalent :

$$p_n(x+h) \underset{h \to 0}{\sim} p_n'(x) \times h$$

   Et donc $p_n(x+h)$ change de signe pour $h < 0$ ou $h > 0$.

$$\boxed{\text{Ainsi pour } n \in \mathbb{N} \text{ et } x \in]0,+\infty[, \text{ si } p_n(x) = 0, \text{ alors } p_n'(x) \neq 0 \text{ et } p_n \text{ change de signe en } x.}$$

   (c) Soit $n \in \mathbb{N}$. La fonction polynomiale p_n a au plus un nombre fini de points d'annulation sur $]0,+\infty[$.
   Notons k ce nombre et plaçons-nous dans le cas où $k \geqslant 2$; notons $x_1 < ... < x_k$ ces points d'annulation.
      i. $p_n(0) = 1$, donc comme p_n change de signe à chaque annulation (en notant $x_0 = 0$) :

$$\boxed{\forall\ i \in \mathbb{N}, p_n \text{ est du signe de } (-1)^i \text{ sur l'intervalle }]x_i, x_{i+1}[}$$

      ii. La suite $(p_n'(x_i))_i$ change de signe pour chaque i. Il suffit donc de se contenter de l'etude en un point.
      On se concentre en x_1. p_n est positive sur $[x_0, x_1[$, s'annule en x_1, donc est décroissante en x_1.
      Par conséquent : $p_n'(x_1) < 0$, donc du signe de $(-1)^1$.

$$\boxed{p_n'(x_i) \text{ est du signe de } (-1)^i.}$$

      iii. On a vu que $p_{n+1}(x) = [1 - 2(n+1)x]p_n(x) - n(n+1)x^2 p_{n-1}(x)$ et $p_n'(X) = -n(n+1)p_{n-1}(x)$.
      donc $p_{n+1}(x_i) = 0 + x_i^2 p_n'(x_i)$ car $p_n(x_i) = 0$

$$\boxed{\text{En chacun des } x_i,\ p_{n+1} \text{ est du signe de } (-1)^i.}$$

      iv. On a l'équivalent : $p_{n+1}(x) \underset{x \to +\infty}{\sim} (-1)^{n+1}(n+2)!x^{n+1} \longrightarrow (-1)^{n+1}\infty$

$$\boxed{p_{n+1}(x) \underset{x \to +\infty}{\longrightarrow} (-1)^{n+1}\infty}$$

      v. Supposons ici $k = n$.
      Soit $i \in [\![1, n-1]\!]$. Comme $p_{n+1}(x_i)$ et $p_{n+1}(x_{i+1})$ sont de signe contraire,
      d'après le théorème des valeurs intermédiaires : $\exists\ y_i \in]x_i, x_{i+1}[$ tel que $p_{n+1}(y_i) = 0$.
      De même $p_{n+1}(0) = 1$ et $p_{n+1}(x_1)$ est du signe de $(-1)^1 = -1$.
      On peut appliquer le TVI sur $]0, x_1[$, ce qui donne une nouvelle racine y_0.

Enfin, $p_{n+1}(x_n)$ est du signe de $(-1)^n$ alors que celui de $\lim_{+\infty} p_{n+1}$ est celui de $(-1)^{n+1}$.
au voisinage de $+\infty$, il existe a tel que $p_{n+1}(a)$ est du signe de $(-1)^{n+1}$.
Donc, en appliquant le TVI, on trouve une nouvelle racine de p_{n+1} au dela de x_n.

$$\boxed{\text{On a donc trouvé (au moins) } n+1 \text{ points d'annulation de la fonction } p_{n+1}}$$

(d) P_0 admet 0 racine et $P_1 = 1 - 2X$ admet une racine dans $]0, +\infty[$ ($x_1 = \frac{1}{2}$).
Supposons que P_n admet au moins n racines dans $]0, +\infty[$.
On se trouve dans le cas précédent avec $k = n$ et donc : p_{n+1} admet $n+1$ racines.
On a ainsi démontré par récurrence :

$$\boxed{\text{pour tout } n \in \mathbb{N}, \text{ le polynôme } P_n \text{ possède au moins } n \text{ racines dans }]0, +\infty[.}$$

Un polynôme de degré n possède au plus n racines. On peut donc affirmer que

$$\boxed{P_n \text{ possède exactement } n \text{ racines dans }]0, +\infty[}$$

Problème 3. Groupes à 2, 3, 4 éléments

Soit G un ensemble fini. Si $\star$ est une loi de composition interne (LCI) sur l'ensemble G, on appellera table de la loi $\star$ le tableau $T, \star$ ci-dessous, où on lit dans la ligne x et la colonne y le « produit » $x \star y$ (dans cet ordre). On recherche les lois de composition interne $\star$ sur G telles que $(G, \star)$ est un groupe, c'est-à-dire :

(i) la loi $\star$ est associative,

(ii) la loi $\star$ admet un élément neutre dans G,

(iii) tout élément $g \in G$ possède un symétrique dans G (que l'on notera g^{-1}) pour la loi $\star$.

On suppose que $\star$ est une telle loi. On notera désormais e l'élément neutre de G pour la loi $\star$. On le fera toujours apparaître en première position dans la table $T, \star$.

1. (a) Soit $x \in G$ fixé. Notons x^{-1}, son inverse.
Pour tout $y \in G$,

$$f_{x^{-1}} \circ f_x(y) = x^{-1} \star (x \star y) = (x^{-1} \star x) \star y = e \star y = y$$

$$f_x \circ f_{x^{-1}}(y) = x \star (x^{-1} \star y) = (x \star x^{-1}) \star y = e \star y = y$$

$$\boxed{f_x : G \to G,\ y \mapsto x \star y \text{ est bijective d'inverse } f_{x^{-1}}}$$

Cela signifie que f_x est surjective, donc toutes les valeurs de G sont sur la ligne de x,
elle ne s'y trouve qu'une et une seule fois, car f_x est injective.

$$\boxed{\text{Sur les lignes de la table de } \star \text{ on trouve exactement tous les éléments de } G \text{ une et une seule fois}}$$

Remarques !
A noter que
— *avec l'affirmation : $f_{x^{-1}} \circ f_x = id_G$, on affirme que f_x est injective.*
En effet si $f_x(y) = f_x(y')$, alors $f_{x^{-1}} \circ f_x(y) = f_{x^{-1}} \circ f_x(y')$ et donc $y = y'$.
Cela permet de conclure que tous les éléments sur la lignes de x sont distincts (ce qui est suffisant)
— *avec l'affirmation : $f_x \circ f_{x^{-1}} = id_G$, on affirme que f_x est surjective.*
En effet si $y \in G$, $\exists\ a \in G$ ($a = f_{x^{-1}}(y)$), tel que $y = f_x(a)$.
Cela permet de conclure que tous les éléments de G sont sur la lignes de x(ce qui est suffisant)

(b) Soit $x \in G$ fixé. Notons x^{-1}, son inverse.
Pour tout $y \in G$,

$$h_{x^{-1}} \circ h_x(y) = (y \star x) \star x^{-1} = y \star (x \star x^{-1}) = y \star e = y$$

$$h_x \circ h_{x^{-1}}(y) = (y \star x^{-1}) \star x = y \star (x^{-1} \star x) = y \star e = y$$

$$\boxed{f_x : G \to G,\ y \mapsto x \star y \text{ est bijective d'inverse } f_{x^{-1}}}$$

Cela signifie que h_x est surjective, donc toutes les valeurs de G sont sur la colonne de x,
elle ne s'y trouve qu'une et une seule fois, car h_x est injective.

$$\boxed{\text{Sur les colonnes de la table de } \star \text{ on trouve exactement tous les éléments de } G \text{ une et une seule fois}}$$

2. (a) On suppose ici que G est de cardinal 2. On note $G = \{e, a\}$.
Comme $e \star e = e$, $e \star a = a$ et $a \star e = a$. On obtient trois cases sur quatre. La dernière est nécessairement un e.

$\star$	e	a
e	e	a
a	a	e

(b) On suppose ici que G est de cardinal 3. On note $G = \{e, a, b\}$.

i. $a \star e = a$, donc $a \star a \neq a$ (injectivité de f_a).
si $a \star a = e$, alors $a \star b = b$, par surjectivité de f_a et donc $a \star b = e \star b$, donc $a = e$. Faux.

$$\boxed{\text{Donc nécessairement } a \star a = b}$$

ii. De même $b \star b = a$. La table existe et est unique :

$\star$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Remarques !
Tout groupe a trois éléments est nécessairement de cette forme.
C'est le cas de $(\frac{\mathbb{Z}}{3\mathbb{Z}}, +) = (\{0, 1, 2\}, +)$ *(reste modulo 3 avec addition).*
Ici $e = 0$, $a = 1$ *et* $b = 2$ *(par exemple).*
C'est aussi le cas de $(\{1, j, j^2\}, \times)$. *Ici* $e = 1$, $a = j$ *et* $b = j^2$

3. On suppose ici que G est de cardinal 4. On va distinguer deux « familles » de loi de groupe sur G.

(a) On suppose ici que, pour tout $x \in G$, $x \star x = e$.
On note $G = \{e, a, b, c\}$. On s'occupe de la ligne de a. On sait déjà que $a \star e = a$ et $a \star a = e$.
Si $a \star b = b$, alors $a = e$, faux. Donc $a \star b = c$ et ainsi $a \star c = b$.
De même pour les autres lignes, on trouve un unique tableau qui fonctionne bien :

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Remarques !
Un avatar est le produit cartésien du groupe à 2 éléments $(\{(0,0), (0,1), (1,0), (1,1)\}, +)$ *(modulo 2).*
Ici $e = (0,0)$, $a = (0,1)$, $b = (1,0)$ *et* $c = (1,1)$.
Ce groupe s'appelle le groupe de Klein (Felix Klein). Sur wikipédia, on peut lire : « Dans Les Structures élémentaires de la parenté, l'ethnologue Claude Lévi-Strauss, aidé du mathématicien André Weil, dégage le concept de structure élémentaire de parenté en utilisant la notion de groupe de Klein1. Dans La Structure des mythes, Lévi-Strauss réutilisera les groupes de Klein pour établir la « formule canonique du mythe ». »

(b) On suppose ici qu'il existe $a \in G$ tel que $a \star a \neq e$. On pose $b = a \star a$.

i. On ne peut avoir $a \star a = a$, sinon en multipliant par a^{-1},on aurait $a = e$.

$$\boxed{\text{donc } b \neq a}$$

ii. On sait que $a \star e = a$, $a \star a = b$. On ne peut avoir $a \star c = c$, sinon $a = e$.
Donc $a \star c = e$ et $a \star b = c$.
Comme l'inverse de a est c ($a \star c = e$),
nécessairement : $c \star e = c$, $c \star a = e$, $c \star b = c \star (a \star a) = a$ et $c \star c = b$.
Finalement, on trouve une et une seule table :

$\star$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Remarques !

Une incarnation de ce groupe : $(\{1, i, -1, -i\}, \times)$. *Ici* $e = 1$, $a = i$, $b = -1$ *et* $c = -i$.

Une autre $(\frac{\mathbb{Z}}{4\mathbb{Z}}, +) = (\{0, 1, 2, 3\}, +)$ *(reste modulo 4 avec +). Ici* $e = 0$, $a = 1$, $b = 2$ *et* $c = 3$.

Encore une : $\left(\left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)^*, \times\right) = (\{1, 2, 3, 4\}, +)$ *(reste modulo 5 avec* $\times$*)*

Ici $e = 1$, $a = 2$ $(a \times a = 4)$, $b = 4$ $(b \times b = 4 \times 4 = 1)$ *et* $c = 3$ $(c \times c = 9 = 4)$

(c) La question n'est pas facile, il existe le premier cas.
Pour le second cas, nous avons arbitrairement considéré $a \times a = b$ (on sait que nécessairement $a \times a \neq e$ (1er cas) et $a \times a \neq a$). On aurait pu avoir $a \times a = c$; mais dans ce cas, on aurait trouvé le même groupe (avec une permutation bijective du nom des lettres b et c : $b \leftrightarrow c$). On considère habituellement qu'il n'y a donc qu'un seul tel groupe.

$$\boxed{\text{Il existe donc seulement deux lois } \star \text{ sur } G \text{ de cardinal 4 telles que } (G, \star) \text{ soit un groupe}}$$