Lycée Louis-Le-Grand, Paris
MP2I – Mathématiques
A. Troesch

Pour le 29/03/2024

DM n° 20 : DL - Polynômes

Corrigé du problème 1 – *Soit $\lambda \in \mathbb{R}$. On étudie les polynômes $P(X)$ à coefficients réels tels que :*

$$(X^2-1)P''(X) + 4XP'(X) = \lambda P(X). \tag{1}$$

Partie I – Propriétés des solutions de (1)

Soit $P(X)$ une solution non nulle de (1), de degré noté n.

1. Si $n = \deg(P) > 1$, alors $\deg(P') = n-1$ et $\deg(P'') = n-2$, et par conséquent, $(X^2-1)P''(X)$ et $4XP'(X)$ sont de degré n. Identifions les coefficients des termes de degré n. Soit $a_n \neq 0$ le coefficient du terme de degré n de P (donc le coefficient dominant).
   - Le terme de degré $n-2$ de P'' est obtenu en dérivant deux fois le monôme a_nX^n et est donc égal à $n(n-1)a_nX^{n-2}$. Ainsi, le coefficient du terme de degré n de $(X^2-1)P''(X)$ est $n(n-1)a_n$.
   - De même, le coefficient du terme de degré n de $4XP'(X)$ est $4na_n$.
   - Enfin, le coefficient du terme de degré n de λP est λa_n.

   Ainsi, l'identification des coefficients des termes de degré n donne l'équation :

   $$n(n-1)a_n + 4na_n = \lambda a_n.$$

   Comme $a_n \neq 0$ (n étant le degré de P), on obtient : $\boxed{\lambda = n(n-1) + 4n = n(n+3)}$.

   On vérifie facilement que cette égalité reste vraie pour $n = 0$ et $n = 1$.

2. D'après les règles de dérivation de fonctions composées :

   $$Q'(X) = -(-1)^nP'(-X) = (-1)^{n+1}P'(-X) \qquad \text{et} \qquad Q''(X) = (-1)^{n+2}P''(-X) = (-1)^nP''(-X).$$

   D'autre part, on peut composer l'équation (1) par $-X$, ce qui donne :

   $$(X^2-1)P''(-X) - 4XP'(-X) = \lambda P(-X).$$

   On en déduit que :

   $$\begin{aligned}(X^2-1)Q''(X) + 4XQ'(X) &= (-1)^n(X^2-1)P''(X) + 4X(-1)^{n+1}P'(-X)\\ &= (-1)^n\left((X^2-1)P''(X) - 4XP'(-X)\right)\\ &= (-1)^n\lambda P(-X) = \lambda Q(X).\end{aligned}$$

   Ainsi, $\boxed{Q \text{ est aussi solution de (1)}}$.

3. Soit $m = \deg(P-Q)$. Puisque P et Q vérifient l'équation (1), il est immédiat que $P-Q$ également. Par conséquent, d'après la question 1, si $m \neq -\infty$, l'entier positif ou nul m vérifie $\lambda = m(m+3) = n(n+3)$. Comme la fonction $x \mapsto x(x+3)$ est strictement positive sur $\mathbb{R}_+$, elle est injective, et on en déduit que $m = n$.

   Ceci contredit le fait évident que P et Q ont même coefficient de degré n. Ainsi, $\deg(P-Q) = -\infty$, donc $\boxed{P = Q}$.

   Il en résulte que $\boxed{P \text{ est de même parité que } n}$.

4. Pour $n = 0$, on obtient $\lambda = 0$, et la seule expression possible pour P_0 est $\boxed{P_0 = 1}$, qui vérifie bien l'équation (1), avec $\lambda = 0$.

   Si $n = 1$, alors $\lambda = 4$, et P_1 est de la forme $P_1 = X + a$, donc $P_1' = 1$ et $P'' = 0$. Ainsi, l'équation (1) se réécrit :

$$4X = 4X + 4a \qquad \text{soit:} \qquad a = 0.$$

   Ainsi, $\boxed{P_1 = X}$.

   Si $n = 2$, alors $\lambda = 10$, et P_2 est de la forme $P_2 = X^2 + aX + b$, donc $P_2' = 2X + a$ et $P_2'' = 2$. Ainsi l'équation est :

$$2(X^2 - 1) + 8X^2 + 4a = 10X^2 + 10aX + 10b \qquad \text{soit:} \qquad 10aX + 10b - 4a + 2 = 0.$$

   Ainsi, $a = 0$ et $b = -\frac{1}{5}$. On a donc : $\boxed{P_2 = X^2 - \frac{1}{5}}$.

5. Une première remarque, le polynôme ainsi défini ne comporte que des monômes de même parité que n, ce qui est conforme au résultat de la question 1c.

   Explicitons sur les coefficients le fait que P_n satisfait (1) :

$$\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (n-2k)(n-2k-1)a_{2k}X^{n-2k} - \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (n-2k)(n-2k-1)a_{2k}X^{n-2(k+1)} + 4\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (n-2k)a_{2k}X^{n-2k} = n(n+3)\sum_{k=0}^{E\left\lfloor \frac{n}{2} \right\rfloor} a_{2k}X^{n-2k},$$

$$\text{soit :} \quad \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (n-2k)(n-2k-1)a_{2k}X^{n-2k} - \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} (n-2k+2)(n-2k+1)a_{2k-2}X^{n-2k} + 4\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} (n-2k)a_{2k}X^{n-2k} = n(n+3)\sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} a_{2k}X^{n-2k},$$

$$\text{soit :} \quad \sum_{k=1}^{\lfloor \frac{n}{2} \rfloor} \Big(\big((n-2k)(n-2k-1) + 4(n-2k) - n(n+3)\big)a_{2k} - (n-2k+2)(n-2k+1)a_{2k-2} \Big) X^{n-2k} + n(n-1) + 4n - n(n+3) = 0.$$

   On a bien $n(n-1) + 4n - n(n+3) = 0$, et en identifiant les coefficients, on obtient le système suivant :

$$\forall k \in \left[\!\left[1, \left\lfloor \frac{n}{2} \right\rfloor\right]\!\right], \quad \big((n-2k)(n-2k+3) - n(n+3)\big)a_{2k} = (n-2k+2)(n-2k+1)a_{2(k-1)},$$

   et donc :

$$\boxed{\forall k \in \left[\!\left[1, \left\lfloor \frac{n}{2} \right\rfloor\right]\!\right] 2k(2k-2n-3)a_{2k} = (n-2k+2)(n-2k+1)a_{2(k-1)}}$$

   Pour tout $k \in \left[\!\left[1, \left\lfloor \frac{n}{2} \right\rfloor\right]\!\right]$, k est non nul, et $2k - 2n - 3$ est impair, donc non nul. Ainsi, ce système admet une unique solution (a_{2k}), donnée par l'unique solution de la relation de récurrence :

$$\boxed{a_0 = 1} \qquad \text{et} \qquad \forall k \in \left[\!\left[1, E\left(\frac{n}{2}\right)\right]\!\right], \quad \boxed{a_{2k} = \frac{(n-2k+2)(n-2k+1)}{2k(2k-2n-3)} \cdot a_{2(k-1)}.}$$

   Par exemple, $a_2 = -\dfrac{n(n-1)}{2(2n+1)} \cdot a_0 = -\dfrac{n(n-1)}{2(2n+1)}$. Pour $n = 2$, on retrouve bien $a_2 = -\frac{1}{5}$.

6. Si λ n'est pas de la forme $\lambda = n(n+3)$, il n'y a pas de solution.

   S'il existe n (forcément unique) tel que $\lambda = n(n+3)$, P_n est solution de (1), alors pour tout $\alpha \in \mathbb{C}$, αP est solution de (1). Ainsi, $\mathbb{C}P_n = \{\alpha P_n, \ \ \alpha \in \mathbb{C}\}$ est inclus dans l'ensemble des solutions.

   De plus, si P est un polynôme solution de (1) de coefficient dominant α, alors $\frac{P}{\alpha}$ est un polynôme unitaire solution de (1), et, d'après l'unicité d'une telle solution, $\frac{P}{\alpha} = P_n$, donc $P = \alpha P_n$.

   Ainsi, $\boxed{\text{l'ensemble des solutions est } \mathbb{C}P_n}$.

Partie II – Une relation de récurrence pour le calcul de P_n

On se propose d'établir que pour tout $n \geqslant 2$:

$$P_n(X) - XP_{n-1}(X) + \frac{n^2-1}{4n^2-1}P_{n-2}(X) = 0. \tag{2}$$

1. *On considère, pour tout $n \geqslant 2$, $R_n(X) = (X^2-1)P_n'(X) - nXP_n(X)$.*

   (a) On dérive l'égalité définissant R_n :

   $$R_n'(X) = 2XP_n'(X) + (X^2-1)P_n''(X) - nP_n(X) - nXP_n'(X).$$

   On remplace P_n'' par son expression en fonction de P_n et P_n' :

   $$R_n'(X) = (2-n)XP_n'(X) - nP_n(X) + n(n+3)P_n(X) - 4XP_n'(X),$$

   soit : $\boxed{R_n'(X) = (n+2)(nP_n(X) - XP_n'(X))}$.

   (b) On dérive l'égalité définissant R_n :

   $$R_n'(X) = 2XP_n'(X) + (X^2-1)P_n''(X) - nP_n(X) - nXP_n'(X).$$

   On remplace P_n'' par son expression en fonction de P_n et P_n' :

   $$R_n'(X) = (2-n)XP_n'(X) - nP_n(X) + n(n+3)P_n(X) - 4XP_n'(X) = (n+2)(nP_n(X) - XP_n'(X).$$

   (c) Dérivons $(X^2-1)R_n'$:

   $$\begin{aligned}(X^2-1)R_n'' + 2XR_n' &= (n+2)((n-1)P_n'(X) - XP_n''(X))(X^2-1) + 2(n+2)X(nP_n(X) - XP_n'(X)) \\ &= (n+2)\left(((n-1)(X^2-1) + 2X^2)P_n'(X) + (2n - n(n+3))XP_n(X)\right).\end{aligned}$$

   Cette dernière égalité est obtenue en utilisant l'équation (1).
   Ainsi :

   $$\begin{aligned}(X^2-1)R_n'' + 4XR_n' &= (n+2)\left((n-1)(X^2-1)P_n'(X) + (2n - n(n+3) + 2n)XP_n(X)\right) \\ &= (n+2)(n-1)((X^2-1)P_n'(X) - nXP_n(X)) \\ &= \boxed{(n+2)(n-1)R_n(X)}.\end{aligned}$$

   (d) Ainsi, R_n est solution de l'équation (1) de paramètre $\lambda = (n-1)(n+2)$. Par conséquent, R_n est égal à P_{n-1} à une constante multiplicative près. Comme P_n est unitaire, cette constante est égal au coefficient dominant de R_n, qu'on obtient à partir de la définition de R_n :
   On voit sans peine que les monômes de degré $n+1$ de R_n se compensent, et comme P_n est de même parité que n, R_n n'a pas non plus de monôme de degré n. Ainsi, il faut trouver son coefficient de degré $n-1$ (cela conforte le fait que R_n est dans $\mathbb{C}P_{n-1}$).
   Pour cela, on a besoin du coefficient de degré $n-2$ de P_n, à savoir $a_2 = -\dfrac{n(n-1)}{2(2n+1)}$. L'identification donne alors sans peine :

   $$\boxed{-\frac{n(n-1)(n-2)}{4n+2} - n + \frac{n^2(n-1)}{4n+2} = -\frac{n(n+2)}{2n+1}} \neq 0;$$

   On déduit au final que :

   $$\boxed{R_n = -\frac{n(n+2)}{2n+1}P_{n-1}}.$$

   En remplaçant R_n par son expression dans cette égalité, on obtient finalement :

   $$\boxed{(X^2-1)P_n'(X) - nXP_n(X) + \frac{n(n+2)}{2n+1}P_{n-1}(X) = 0}.$$

   Cette égalité est vraie pour tout $n \geqslant 1$.

2. Soit $n \geqslant 1$. Dérivons l'expression obtenue dans la question précédente :

$$\begin{aligned} 0 &= (X^2-1)P_n'' + 2XP_n' - nP_n - nXP_n' + \frac{n(n+2)}{2n+1}P_{n-1}'(X) \\ &= n(n+3)P_n - 4XP_n' + 2XP_n' - nP_n - nXP_n' \\ &= (n+2)\left(nP_n - XP_n' + \frac{n}{2n+1}P_{n-1}'\right) \end{aligned}$$

Ainsi, pour tout $n \in \mathbb{N}^*$,

$$\boxed{nP_n - XP_n' + \frac{n}{2n+1}P_{n-1}' = 0}.$$

Soit $n \geqslant 2$. En multipliant cette relation par X^2-1 et en utilisant la relation de la question précédente aux rangs n et $n-1$, on obtient :

$$\begin{aligned} 0 &= n(X^2-1)P_n - X(X^2-1)P_n' + \frac{n}{2n+1}(X^2-1)P_{n-1}' \\ &= n(X^2-1)P_n - nX^2P_n + X\frac{n(n+2)}{2n+1}P_{n-1} + \frac{n}{2n+1}\left((n-1)XP_{n-1} - \frac{(n-1)(n+1)}{2n-1}P_{n-2}\right) \\ &= -nP_n + XnP_{n-1} - \frac{n(n^2-1)}{4n^2-1}P_{n-2}. \end{aligned}$$

Ainsi, en divisant par $-n$, on obtient, pour tout $n \geqslant 2$:

$$\boxed{P_n - XP_{n-1} + \frac{n^2-1}{4n^2-1}P_{n-2} = 0}.$$

3. On donne sans commentaire :

```
def normalise(P):
    """ Supprime les zéros inutiles en hauts degrés: la liste s'arrête
    au monôme dominant """
    while len(P)>0 and P[-1] == 0:
        P.pop(-1)
    return(P)

def scal(a,P):
    """ Multiplication du polynôme P par le scalaire a """
    if a == 0:
        return []
    else:
        return [a * c for c in P]

def mul(P,Q):
    """ Multiplication de deux polynômes P et Q"""
    R = [0 for i in range(len(P)+len(Q)-1)]
    for i in range(len(P)):
        for j in range(len(Q)):
            R[i+j]+= P[i] * Q[j]
    return R

def somme(P,Q):
    """ Somme de 2 polynômes"""
    R = [0 for i in range(max(len(P),len(Q)))]
    for i,c in enumerate(P):
        R[i] += c
    for i,c in enumerate(Q):
```

```
        R[i] += c
    return normalise(R)

def Pn(n):
    """ Calcul de P_n """
    if n == 0:
        return [1]
    else:
        P = [1]
        Q = [0,1]
        for i in range(2,n+1):
            P,Q  = Q, somme(mul([0,1],Q), scal(-(n*n-1)/ (4*n*n - 1), P))
        return Q
```

Corrigé du problème 2 – (Développement asymptotique de la fonction Γ et formule de Stirling, d'après X 2015)

Partie I – Autour de la fonction Γ

1. La fonction $t \mapsto \mathrm{e}^{-\frac{t}{2}}$ est continue sur $[1, +\infty[$, et

$$\int_1^A \mathrm{e}^{-\frac{t}{2}}\,\mathrm{d}t = 2\mathrm{e} - 2\mathrm{e}^{-\frac{A}{2}} \longrightarrow 2\mathrm{e}.$$

Ainsi, $\boxed{\int_1^{+\infty} \mathrm{e}^{-\frac{t}{2}}\,\mathrm{d}t \text{ converge}}$.

2. Pour tout x fixé dans $\mathbb{R}$, la fonction $t \mapsto t^{x-1}\mathrm{e}^{-t}$ est continue sur $]0, 1]$, et

$$t^{x-1}\mathrm{e}^{-t} \underset{0}{\sim} t^{x-1}.$$

Or, pour tout $a \in]0, 1[$, si $x \neq 0$

$$\int_a^1 t^{x-1}\,\mathrm{d}t = \frac{1}{x}(1 - a^x).$$

Cette expression admet une limite finie lorsque $a \to 0^+$ si et seulement si $x > 0$.
Le cas $x = 0$ se traite de façon particulière, puisque dans ce cas,

$$\int_a^1 t^{x-1}\,\mathrm{d}t = -\ln(a) \underset{a\to 0^+}{\longrightarrow} +\infty.$$

Ainsi, l'intégrale $\displaystyle\int_0^1 t^{x-1}\,\mathrm{d}t$ converge si et seulement si $x > 0$, et en utilisant la comparaison par équivalents rappelée dans l'énoncé (qui peut s'utiliser dans les deux sens, donc permet aussi de comparer les divergences, par contraposition), les fonctions étant positives, on en déduit que $\boxed{\int_0^1 t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t \text{ converge si et seulement si } x > 0.}$

3. Au voisinage de $+\infty$, on a, d'après les croissances comparées, $t^{x-1}\mathrm{e}^{-t^2} = o(\mathrm{e}^{-\frac{t}{2}})$. En effet

$$\mathrm{e}^{\frac{t}{2}} t^{x-1}\mathrm{e}^{-t^2} = \mathrm{e}^{-t^2+\frac{t}{2}+(x-1)\ln(t)} \underset{t\to+\infty}{\longrightarrow} 0,$$

le terme prépondérant dans l'exposant étant le terme $-t^2$.

La positivité des fonctions et la question 1 permettent alors d'obtenir la $\boxed{\text{convergence de } \int_1^{+\infty} t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t}$, pour tout $x \in \mathbb{R}$, par comparaison (avec o).
Ainsi, Γ est définie en tout point en lequel les deux intégrales sur les intervalles $[0, 1]$ et $[1, +\infty[$ sont convergentes, donc $\boxed{D_\Gamma = \mathbb{R}_+^*.}$

4. En l'absence de théorème précis sur les IPP sur les intégrales impropres, on restreint l'intervalle d'intégration. Soit $0 < a < b$. Les fonctions étant toutes de classe $\mathcal{C}^1$, on peut faire une intégration par parties :

$$\int_a^b t^x \mathrm{e}^{-t}\,\mathrm{d}t = \Big[-t^x\mathrm{e}^{-t}\Big]_a^b + \int_a^b xt^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t.$$

Puisque $x > 0$, $a^x \to 0$ lorsque $a \to 0$, et par croissances comparées, $b^x\mathrm{e}^{-b} \to 0$ lorsque $b \to +\infty$. Ainsi, lorsqu'on fait tendre a vers 0 et b vers $+\infty$, on obtient :

$$\boxed{\Gamma(x+1) = x\Gamma(x)}.$$

Montrons par récurrence que pour tout $n \in \mathbb{N}$, $\Gamma(n+1) = n!$.

- Pour commencer, $\Gamma(1) = \displaystyle\int_0^{+\infty} \mathrm{e}^{-t}\,\mathrm{d}t = 1 - \lim_{b\to+\infty} \mathrm{e}^{-b} = 1 = 0!$.
- Soit $n \in \mathbb{N}$. On suppose que $\Gamma(n+1) = n!$. La relation obtenue en début de question amène alors

$$\Gamma(n+2) = (n+1)\Gamma(n+1) = (n+1)\cdot n! = (n+1)!.$$

- Ainsi, d'après le principe de récurrence, pour tout $n \in \mathbb{N}$, $\boxed{\Gamma(n+1) = n!}$.

5. On se ramène à l'intégrale de Gauss par le changement de variables $t = u^2$, de classe $\mathcal{C}^1$. On le fait une une intégrale non impropre. On se donne $0 < a < b$. On a alors

$$\int_a^b t^{-\frac{1}{2}}\mathrm{e}^{-t}\,\mathrm{d}t = \int_{\sqrt{a}}^{\sqrt{b}} \frac{1}{u}\mathrm{e}^{-u^2} 2u\,\mathrm{d}u = 2\int_{\sqrt{a}}^{\sqrt{b}} \mathrm{e}^{-u^2}\,\mathrm{d}u.$$

En faisant tendre a vers 0 et b vers $+\infty$, il vient donc

$$\Gamma\left(\frac{1}{2}\right) = 2\int_0^{+\infty} \mathrm{e}^{-u^2}\,\mathrm{d}u \qquad \text{donc:} \qquad \boxed{\Gamma\left(\tfrac{1}{2}\right) = \sqrt{\pi}}.$$

Partie II – Généralisation de la formule de Stirling

1. Soit $y > 0$, on a d'après les résultats de la partie précédente, $y\Gamma(y) = \Gamma(y+1)$, donc

$$\boxed{\Gamma(y) = y^{-1}\int_0^{+\infty} \mathrm{e}^{-t}t^y\,\mathrm{d}t.}$$

Posons pour commencer le changement de variable $t = ys$. On le fait directement sur l'intégrale impropre (vérifier que c'est bien ce que cela donne lorsqu'on le fait sur l'intégrale restreinte, et qu'on fait tendre les bornes ; c'est essentiellement le théorème de la bijection qui nous dit que cela va marcher) :

$$\Gamma(y) = y^{-1}\int_0^{+\infty} \mathrm{e}^{-sy}s^y y^y y\mathrm{d}s = y^y\int_0^{+\infty} \mathrm{e}^{-y(s-\ln(s))}\mathrm{d}s.$$

On effectue ensuite le changement de variables $u = s - 1$, qui amène :

$$\Gamma(y) = y^y\int_{-1}^{+\infty} \mathrm{e}^{-y((u+1)-\ln(u+1))}\,\mathrm{d}u = \boxed{\mathrm{e}^{-y}y^y\int_{-1}^{+\infty} \mathrm{e}^{-y\varphi(u)}\,\mathrm{d}u}.$$

2. Étudions la fonction φ. Elle est dérivable sur $]-1,+\infty[$, et

$$\forall u \in]-1,+\infty[,\quad \varphi'(u) = 1 - \frac{1}{1+u} = \frac{u}{1+u}.$$

Comme $1+u > 0$, $\varphi'(u)$ est du signe de u. Ainsi, φ est strictement décroissante sur $]-1,0]$ et strictement croissante sur $[0,+\infty[$. De plus $\lim\limits_{u\to-1^+} \varphi(u) = +\infty$, $\varphi(0) = 0$ et $\lim\limits_{u\to+\infty} \varphi(u) = +\infty$, et φ est continue. Ainsi, le théorème de la bijection appliqué sur les deux intervalles $]-1,0[$ et $]0,+\infty[$ nous assure que φ se restreint en une $\boxed{\text{bijection décroissante } \varphi_- \text{ de }]-1,0[\text{ sur }]0,+\infty[}$ et en une $\boxed{\text{bijection croissante de }]0,+\infty[\text{ sur }]0,+\infty[.}$

3. (a) Les hypothèses sur f amènent $f(0) = 0$. La formule de Taylor nous donne alors l'existence d'un développement limité en 0 à l'ordre n, sans terme constant :

$$f(x) = a_1 x + \cdots + a_n x^n + o(x^n).$$

La fonction $\tilde{f} : x \mapsto f(x) - a_1 x + \cdots + a_n x^n + o(x^n)$ est alors aussi de classe $\mathcal{C}^n$ et vérifie $\tilde{f}(x) = o(x^n)$. En vertu de la formule de Taylor et de l'unicité du DL, ceci signfie que les dérivées successives de $\tilde{f}$ en 0 sont nulles jusqu'à l'ordre n. Par ailleurs, le développement de Taylor de f étant de valuation 1, $\frac{f(x)}{x}$ et $\frac{\tilde{f}(x)}{x}$ diffèrent d'un polynôme : l'une est alors de classe $\mathcal{C}^{n-1}$ si et seulement l'autre l'est aussi. On peut donc sans perte de généralité remplacer f par $\tilde{f}$, c'est-à-dire supposer que les dérivées successives de f sont nulles en 0.

La formule de Taylor appliquée à f, mais aussi à toutes ses dérivées jusqu'à l'ordre n, nous donne alors, au voisinage de 0 :

$$\forall k \in [\![0, n]\!], f^{(k)}(x) = o(x^{n-k})$$

Soit $g : x \mapsto \frac{f(x)}{x}$. On va utiliser le théorème de la classe $\mathcal{C}^n$ par prolongement pour montrer que g est de classe $\mathcal{C}^{n-1}$ au voisinage de 0 (dans sa version telle qu'elle est au programme, qui nous oblige à contrôler toutes les dérivées intermédiaires). Pour commencer, g est évidemment de classe $\mathcal{C}^{n-1}$ sur un voisinage de 0 privé de 0. Soit alors $\ell \in [\![0, n-1]\!]$. On a, d'après la formule de Leibniz, pour tout n non nul au voisinage de 0 :

$$g^{(\ell)}(x) = \sum_{i=0}^{\ell} \binom{i}{\ell} f^{(i)}(x) \frac{(-1)^{\ell-i}(\ell-i)!}{x^{\ell-i+1}}.$$

Comme $\ell - i + 1 \leqslant n - i$, l'hypothèse faite sur f amène la nullité de la limite de chacun des termes de la somme lorsque x tend vers 0. Ainsi, pour tout $\ell \in [\![0, n-1]\!]$, $g^{(\ell)}(x) \to 0$ lorsque $x \to 0$.

D'après le théorème de la classe $\mathcal{C}^n$ (ou ici plutôt $\mathcal{C}^{n-1}$) par prolongement, on en déduit que :

$\boxed{g \text{ est de classe } \mathcal{C}^{n-1} \text{ au voisinage de } 0}$.

(b) Soit $n \in \mathbb{N}$ et une fonction f de classe $\mathcal{C}^n$ au voisinage de 0 dont le développement limité à l'ordre $k-1$ (pour $k \in [\![1, n]\!]$) au voisinage de 0 est donné par

$$f(x) = a_0 + a_1 x + \cdots + a_k x^k + o(x^{k-1}).$$

On pose $f_0 : x \mapsto f(x) - (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1})$. On a alors $f_0(x) = a_k x^k + o(x^k)$, et f_0 est de classe $\mathcal{C}^n$ au voisinage de 0.

En particulier, puisque $k \geqslant 1$, $\frac{f_0(x)}{x} \to 0$ quand $x \to 0$. D'après la question précédente, cette fonction se prolonge donc en 0 en une fonction f_1 de classe $\mathcal{C}^{n-1}$. Mais, si $k \geqslant 2$, on a aussi $\frac{f_1(x)}{x} = \frac{f_0(x)}{x^2} \to 0$ quand $x \to 0$, donc $x \mapsto \frac{f_1(x)}{x}$ se prolonge en une fonction f_2 de classe $\mathcal{C}^{n-2}$ au voisinage de 0. L'hypothèse $f_0(x) = a_k x^k + o(x^k)$ nous permet de continuer de la sorte jusqu'à la construction de f_k définie comme prolongement de $\frac{f_{k-1}(x)}{x} = \frac{f_0(x)}{x^k}$ (de limite a_k). La fonction f_k est alors de classe $\mathcal{C}^{n-k}$. Or, f_k est la fonction g de l'énoncé.

Cela prouve que $\boxed{g : x \mapsto \dfrac{f(x) - (a_0 + a_1 x + \cdots + a_{k-1} x^{k-1})}{x^k} \text{ se prolonge en 0 en une fonction de classe } \mathcal{C}^{n-k}}$ sur un voisinage de 0.

(c) Comme φ est définie sur $]-1, +\infty[$ et prend ses valeurs dans $\mathbb{R}_+$, $\boxed{\sqrt{\varphi} \text{ est définie sur }]-1, +\infty[.}$

Comme la fonction racine est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}_+^*$, et φ est de classe $\mathcal{C}^\infty$ sur $]-1, +\infty]$, $\sqrt{\varphi}$ est de classe $\mathcal{C}^\infty$ en tout point de $]-1, +\infty[$ n'annulant pas φ, donc sur $]-1, +\infty[\backslash\{0\}$.

Par ailleurs, $\varphi(u) = u - \ln(1+u) = \frac{u^2}{2} + o(u^2)$, donc $\frac{\varphi(u)}{u^2} \to \frac{1}{2}$ lorsque $u \to 1$. Comme φ est de classe $\mathcal{C}^\infty$ au voisinage de 0, en appliquant la question précédente pour toute valeur de n, $u \mapsto \frac{\varphi(u)}{u^2}$ se prolonge en une fonction g de classe $\mathcal{C}^\infty$ au voisinage de 0. La fonction g ne s'annulant par en 0, $\sqrt{g}$ est aussi de classe $\mathcal{C}^\infty$. Ainsi, $\sqrt{\varphi}$ est obtenue en multipliant $\sqrt{g}$ par x sur $[0, +\infty[$, et par $-x$ sur $]-1, 0]$. Sur chacun de ces intervalles, $\sqrt{\varphi}$ est produit de fonctions de classe $\mathcal{C}^\infty$, donc $\boxed{\sqrt{\varphi} \text{ est de classe } \mathcal{C}^\infty \text{ sur }]-1, 0] \text{ et } [0, +\infty[}$.

4. (a) La fonction racine étant strictement croissante, elle ne change pas la monotonie, et les limites restent aussi les mêmes. Donc on peut adapter la question 2. On peut aussi inclure la borne 0 dans l'argument qu'on avait donné. Ainsi $\boxed{\sqrt{\varphi} \text{ induit des bijections de }]-1, 0] \text{ sur } [0, +\infty[\text{ et de } [0, +\infty[\text{ sur } [0, +\infty[}$. On note ψ_- et ψ_+ respectivement leurs réciproques.

(b) En tout $x \in]-1,+\infty[$ différent de 0, φ ne s'annule pas, et φ' non plus (voir étude de la question 2). Ainsi, la dérivée de $\sqrt{\varphi}$ étant $\frac{\varphi'}{2\sqrt{\varphi}}$, elle ne s'annule pas. Comme $\sqrt{\varphi}$ est de classe $\mathcal{C}^\infty$, on déduit du théorème de dérivation des réciproques que ψ_+ et ψ_- sont de classe $\mathcal{C}^\infty$ en tout y distinct de $\sqrt{\varphi(0)} = 0$.

Il reste donc à étudier la classe $\mathcal{C}^\infty$ en 0. Pour cela on remarque que $\varphi(u) \underset{0}{\sim} \dfrac{u^2}{2}$, donc $\sqrt{\varphi} \underset{0}{\sim} |u|$. Ainsi

$$\sqrt{\varphi(u)} \underset{u\to 0^+}{=} u + o(u).$$

On en déduit que $\sqrt{\varphi}$ est dérivable à droite en 0, de dérivée égale à 1, donc non nulle. L'argument précédente reste donc valable pour montrer que ψ_+ est de classe $\mathcal{C}^\infty$ en 0

De la même manière, la dérivée de $\sqrt{\varphi}$ à gauche en 0 est égale à -1, donc non nulle, et ψ_- est donc de classe $\mathcal{C}^\infty$ en 0.

On en déduit que $\boxed{\psi_- \text{ et } \psi_+ \text{ sont de classe } \mathcal{C}^\infty \text{ sur leur domaine.}}$

Par ailleurs, pour tout $x \in [0,+\infty[$,

$$\sqrt{\varphi(\psi_+(x))} = x = \psi_+(\sqrt{\varphi(x)}),$$

donc, en élevant la première égalité au carré, et en prenant $\sqrt{x}$ comme nouvelle variable, on obtient :

$$\forall x \in \mathbb{R}_+, \quad \varphi(\psi_+(\sqrt{x})) = x = \psi_+(\sqrt{\varphi(x)}).$$

Cette égalité montre que $x \mapsto \psi_+(\sqrt{x})$ est la réciproque de φ sur $[0,+\infty[$. Ainsi, ψ_+ et φ_+^{-1} sont reliés par la relation :

$$\forall x \in]0,+\infty[, \quad \boxed{\varphi_+^{-1}(x) = \psi_+(\sqrt{x})}.$$

On montre de même que pour tout $x \in]0,+\infty[$, $\boxed{\varphi_-^{-1}(x) = \psi_-(\sqrt{x})}$.

(c) Les fonctions ψ_+ et ψ_- étant de classe $\mathcal{C}^\infty$ à droite en 0, elles admettent, d'après la formule de Taylor-Young, des développements à tous ordres à droite en 0.

Nous allons déterminer des développements limités à l'ordre 3 de ψ_+ et ψ_- par identification, comme inverses de $\sqrt{\varphi}$. Nous commençons par faire le développement de φ au voisinage de 0 :

$$\varphi(x) = x - \ln(1+x) = \frac{x^2}{2} - \frac{x^3}{3} + \frac{x^4}{4} + o(u^4).$$

Ainsi, au voisinage à droite de 0 :

$$\begin{aligned}
\sqrt{\varphi(x)} &= \frac{x}{\sqrt{2}}\sqrt{1 - \frac{2x}{3} + \frac{x^2}{2} + o(x^2)} \\
&= \frac{x}{\sqrt{2}}\left(1 + \frac{1}{2}\left(-\frac{2x}{3} + \frac{x^2}{2}\right) - \frac{1}{8}\left(-\frac{2x}{3} + \frac{x^2}{2}\right)^2 + o(x^2)\right) \\
&= \frac{x}{\sqrt{2}}\left(1 - \frac{x}{3} + \frac{x^2}{4} - \frac{x^2}{18} + o(x^2)\right) \\
&= \frac{x}{\sqrt{2}}\left(1 - \frac{x}{3} + \frac{7}{36}x^2 + o(x^2)\right)
\end{aligned}$$

Comme $\varphi(0) = 0$, on a aussi $\psi_+(0) = 0$, donc le développement de ψ_+ à l'ordre 3 en 0 s'écrit sous la forme

$$\psi_+(x) = ax + bx^2 + cx^3 + o(x^3).$$

Exprimons le DL de $\psi_+ \circ \sqrt{\varphi}$ au voisinage à droite en 0 :

$$\begin{aligned}
\psi_+(\sqrt{\varphi(x)}) &= a\left(\frac{x}{\sqrt{2}}\left(1 - \frac{x}{3} + \frac{7}{36}x^2\right)\right) + b\left(\frac{x}{\sqrt{2}}\left(1 - \frac{x}{3} + \frac{7}{36}x^2\right)\right)^2 + c\left(\frac{x}{\sqrt{2}}\left(1 - \frac{x}{3} + \frac{7}{36}x^2\right)\right)^3 + o(x^3) \\
&= \frac{ax}{\sqrt{2}} + x^2\left(\frac{b}{2} - \frac{a}{3\sqrt{2}}\right) + x^3\left(\frac{7}{36}\frac{a}{\sqrt{2}} - \frac{b}{3} + \frac{c}{2\sqrt{2}}\right).
\end{aligned}$$

Cette composée étant égale à l'identité, son DL doit être égal à $x + o(x^3)$. Par unicité de DL, on peut donc identifier les coefficients et on obtient le système

$$\begin{cases} \frac{ax}{\sqrt{2}} & = 1 \\ \frac{b}{2} - \frac{a}{3\sqrt{2}} & = 0 \\ \frac{7}{36}\frac{a}{\sqrt{2}} - \frac{b}{3} + \frac{c}{2\sqrt{2}} & = 0 \end{cases}$$

La résolution de ce système amène $a = \sqrt{2}$, $b = \frac{2}{3}$ et $c = \frac{1}{9\sqrt{2}}$. Ainsi, au voisinage de 0 :

$$\boxed{\psi_+(x) = \sqrt{2} \cdot x + \frac{2}{3}x^2 + \frac{x^3}{9\sqrt{2}} + o(x^3)}.$$

On fait de même pour ψ_-. Le DL de φ au voisinage à gauche de 0 diffère du DL à droite uniquement par son signe (provenant de la racine qu'on applique à x^2. Ce signe modifie le signe les termes provenant du développement des deux termes d'exposant impair dans le DL de la composée. On obtient donc le système

$$\begin{cases} -\frac{ax}{\sqrt{2}} & = 1 \\ \frac{b}{2} + \frac{a}{3\sqrt{2}} & = 0 \\ -\frac{7}{36}\frac{a}{\sqrt{2}} - \frac{b}{3} - \frac{c}{2\sqrt{2}} & = 0 \end{cases}$$

qui amène $a = -\sqrt{2}$, $b = \frac{2}{3}$ et $c = -\frac{1}{9\sqrt{2}}$. Ainsi, au voisinage de 0 :

$$\boxed{\psi_-(x) = -\sqrt{2} \cdot x + \frac{2}{3}x^2 - \frac{x^3}{9\sqrt{2}} + o(x^3)}.$$

(d) On a alors au voisinage de 0 :

$$\boxed{\varphi_+^{-1}(x) = \psi_+(\sqrt{x}) = \sqrt{2x} + \frac{2x}{3} + \frac{x^{3/2}}{9\sqrt{2}} + o(x^{3/2})} \text{ et } \boxed{\varphi_-^{-1}(x) = \psi_-(\sqrt{x}) = -\sqrt{2x} + \frac{2x}{3} - \frac{x^{3/2}}{9\sqrt{2}} + o(x^{3/2})}.$$

On aimerait dériver ces développements asymptotiques, mais le seul théorème nous autorisant à le faire porte sur des développements limités, et pas sur des développements asymptotiques. On le fait donc sur les développements limités de ψ_+ et ψ_-. La dérivation est licite du fait que les fonctions sont de classe $\mathcal{C}^\infty$, donc les DL sont du ressort de la formule de Taylor. On a alors, au voisinage de 0 :

$$\psi'_+(x) = \sqrt{2} + \frac{4}{3}x + \frac{1}{3\sqrt{2}}x^2 + o(x^2) \qquad \text{et} \qquad \psi'_-(x) = -\sqrt{2} + \frac{4}{3}x - \frac{1}{3\sqrt{2}}x^2 + o(x^2).$$

Or, $(\varphi_+^{-1})'(x) = \frac{1}{2\sqrt{x}}\psi'_+(x)$, et de même pour $(\varphi_-^{-1})'$, d'où les développements attendus :

$$\boxed{(\varphi_+^{-1})'(x) = \frac{1}{\sqrt{2x}} + \frac{2}{3} + \frac{\sqrt{x}}{6\sqrt{2}} + o(\sqrt{x})} \qquad \text{et} \qquad \boxed{(\varphi_-^{-1})'(x) = -\frac{1}{\sqrt{2x}} + \frac{2}{3} - \frac{\sqrt{x}}{6\sqrt{2}} + o(\sqrt{x})}$$

5. (a) D'après la relation de Chasles,

$$\int_{-1}^{+\infty} \mathrm{e}^{-y\varphi(u)}\,\mathrm{d}u = \int_{-1}^{0} \mathrm{e}^{-y\varphi(u)}\,\mathrm{d}u + \int_{0}^{+\infty} \mathrm{e}^{-y\varphi(u)}\,\mathrm{d}u.$$

On fait dans la première intégrale le changement de variable bijectif décroissant de classe $\mathcal{C}^1$ donné par $t = \varphi(u)$, donc $u = \varphi_-^{-1}(t)$ et $\mathrm{d}u = (\varphi_-^{-1})'(t)\,\mathrm{d}t$, et dans la deuxième intégrale, on fait le changement de variable bijectif croissant $u = \varphi_-^{-1}(t)$. Dans les deux cas, le domaine de la nouvelle variable t est $[0, +\infty[$, mais prcouru en sens décroissante pour la première intégrale. Il faut donc un signe pour rééchanger les bornes, et on obtient :

$$\int_{-1}^{+\infty} \mathrm{e}^{-y\varphi(u)}\,\mathrm{d}u = -\int_{O}^{+\infty} \mathrm{e}^{-yt}(\varphi_-^{-1})'(t)\,\mathrm{d}t + \int_{O}^{+\infty} \mathrm{e}^{-yt}(\varphi_+^{-1})'(t)\,\mathrm{d}t,$$

et d'après II-1, il vient donc :

$$\boxed{\Gamma(y) = \mathrm{e}^{-y} y^y \int_0^{+\infty} \mathrm{e}^{-yt}((\varphi_+^{-1})'(t) - (\varphi_-^{-1})'(t))\ \mathrm{d}t}.$$

Tant que vous n'avez pas de théorèmes sur les intégrales impropres, il est plus sûr de faire le changement de variable sur une intégrale définie et faire tendre les bornes ensuite.

(b) On a au voisinage de 0 :

$$(\varphi_+^{-1})'(t) - (\varphi_-^{-1})'(t) = \frac{\sqrt{2}}{\sqrt{t}} + \frac{\sqrt{2t}}{6} + o(\sqrt{t}).$$

Or, le changement de variables $u = yt$ amène :

$$\int_0^{+\infty} \frac{\sqrt{2}}{\sqrt{x}} \mathrm{e}^{-yt}\ \mathrm{d}t = \frac{1}{y} \int_0^{+\infty} \frac{\sqrt{2y}}{\sqrt{u}} \mathrm{e}^{-u}\ \mathrm{d}u = \frac{\sqrt{2}}{\sqrt{y}} \Gamma\left(\frac{1}{2}\right) = \sqrt{\frac{2\pi}{y}},$$

et de même, en utilisant la question I-4 pour exprimer $\Gamma\left(\frac{3}{2}\right)$:

$$\int_0^{+\infty} \frac{\sqrt{2t}}{6} \mathrm{e}^{-yt}\ \mathrm{d}t = \frac{1}{y} \int_0^{+\infty} \frac{\sqrt{2}}{6} \sqrt{\frac{u}{y}} \mathrm{e}^{-u}\ \mathrm{d}u = \frac{\sqrt{2}}{6y\sqrt{y}} \Gamma\left(\frac{3}{2}\right) = \frac{\sqrt{2}}{12y\sqrt{y}} \Gamma\left(\frac{1}{2}\right) = \frac{\sqrt{2\pi}}{12y\sqrt{y}} \tag{3}$$

Posons alors pour tout $t \in \mathbb{R}_+$,

$$h(t) = (\varphi_+^{-1})'(t) - (\varphi_-^{-1})'(t) - \left(\frac{\sqrt{2}}{\sqrt{t}} + \frac{\sqrt{2t}}{6}\right) = o(\sqrt{t}).$$

Soit $\varepsilon > 0$. Il existe donc t_0 tel que pour tout $t \in [t, t_0]$, $|h(t)| \leqslant \dfrac{\varepsilon}{2\sqrt{\pi}t}$. On a alors :

$$\left| \int_0^{t_0} \mathrm{e}^{-yt} h(t)\ \mathrm{d}t \right| \leqslant \int_0^{t_0} |h(t)\mathrm{e}^{-yt}|\ \mathrm{d}t \leqslant \frac{\varepsilon}{2\sqrt{\pi}} \int_0^{+\infty} \sqrt{t}\mathrm{e}^{-yt} = \frac{\varepsilon}{2\sqrt{\pi} \cdot y\sqrt{y}} \Gamma\left(\frac{1}{2}\right) = \frac{\varepsilon}{2y\sqrt{y}}.$$

En effet, le dernier calcul de l'intégrale se ramène à (1). Il reste à contrôler la seconde moitié de l'intégrale. Pour cela, il faut pouvoir contrôler le comportement de h par rapport à l'exponentielle : il ne doit pas devenir trop gros par rapport à l'exponentielle. Pour cela on revient à la définition. Au voisinage de $+\infty$, on a

$$h(t) = (\varphi_+^{-1})'(t) - (\varphi_-^{-1})'(t) + O(\sqrt{t}).$$

Mais par ailleurs,

$$(\varphi_+^{-1})'(t) = \frac{1}{\varphi'(\varphi_+^{-1}(t))} = \frac{\varphi_+^{-1}(t) + 1}{\varphi_+^{-1}(t)}.$$

Comme $\varphi_+^{-1}(t) \to +\infty$ lorsque $t \to +\infty$, et comme sa dérivée est continue sur $[t_0, +\infty[$ on obtient que $(\varphi_+^{-1})'$ est bornée (il y a du théorème de compacité là-dessous pour contrôler ce qu'il se passe au niveau de la borne t_0). Il en est de même de $(\varphi_-^{-1})'$. ce sont donc des $O(1)$ donc aussi des $O(\sqrt{t})$ au voisinage de $+\infty$.
Ainsi, $h(t) = O(\sqrt{t})$ au voisinage de $+\infty$. Comme par ailleurs, elle est continue sur $[t_0, +\infty[$, $\frac{h(t)}{\sqrt{t}}$ est bornée sur $[t_0, +\infty[$ (encore le théorème de compacité : la limite contrôle ce qui se passe au voisinage de l'infini, le théorème de compacité ce qui se passe sur le reste du domaine, fermé borné). On peut donc trouver M tel que pour tout $t \in [t_0, +\infty[$, $|h(t)| \leqslant M\sqrt{t}$.
On a alors

$$\left| \int_{t_0}^{+\infty} h(t)\mathrm{e}^{-yt}\ \mathrm{d}t \right| \leqslant M \int_{t_0}^{+\infty} \sqrt{t}\mathrm{e}^{-yt}\ \mathrm{d}t \leqslant \frac{M}{y\sqrt{y}} \int_{yt_0}^{+\infty} \sqrt{u}\mathrm{e}^{-u}\ \mathrm{d}u.$$

Or, lorsque y tend vers $+\infty$, la borne inférieure de cette intégrale convergente tend vers $+\infty$, donc

$$\int_{yt_0}^{+\infty} \sqrt{u}\mathrm{e}^{-u}\ \mathrm{d}u \to 0.$$

Cela prouve que (à t_0 fixé) $\displaystyle\int_{t_0}^{+\infty} h(t)\mathrm{e}^{-yt}\ \mathrm{d}t = o\left(\frac{1}{y\sqrt{y}}\right)$. Il existe donc y_0 tel que pour tout $y \geqslant y_0$,

$$\left| \int_{t_0}^{+\infty} h(t)\mathrm{e}^{-yt}\ \mathrm{d}t \right| \leqslant \frac{\varepsilon}{2y\sqrt{y}}.$$

On a donc, pour tout $y \geqslant y_0$,

$$\left|\int_{t_0}^{+\infty} h(t)\mathrm{e}^{-yt}\,\mathrm{d}t\right| \leqslant \frac{\varepsilon}{y\sqrt{y}}.$$

Cela prouve bien que $\displaystyle\int_{t_0}^{+\infty} h(t)\mathrm{e}^{-yt}\,\mathrm{d}t = o\left(\frac{1}{y\sqrt{y}}\right)$ lorsque $y \to +\infty$.

Il ne reste plus qu'à mettre tous ces morceaux épars ensemble, en utilisant la question 5(a) :

$$\Gamma(y) = \mathrm{e}^{-y}y^y\left(\sqrt{\frac{2\pi}{y}} + \frac{\sqrt{2\pi}}{12y\sqrt{y}} + o\left(\frac{1}{y\sqrt{y}}\right)\right).$$

En mettant en facteur, il vient, lorsque $y \to +\infty$:

$$\boxed{\Gamma(y) = \mathrm{e}^{-y}y^y\left(\frac{2\pi}{y}\right)^{\frac{1}{2}}\left(1 + \frac{1}{12y} + o\left(\frac{1}{y}\right)\right).}$$

6. Lorsqu'on prend $y = n$, il vient

$$(n-1)! = \left(\frac{n}{\mathrm{e}}\right)^n \frac{\sqrt{2\pi}}{\sqrt{n}}\left(1 + \frac{1}{12n} + o\left(\frac{1}{n}\right)\right),$$

et si on multiplie par n, on obtient :

$$n! = \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n\left(1 + \frac{1}{12n} + o\left(\frac{1}{n}\right)\right).$$

En particulier, en gardant la partie principale de ce développement asymptotique, il reste la formule de Stirling :

$$\boxed{n! \underset{+\infty}{\sim} \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n}.$$

Corrigé du problème 3 – Polynômes irréductibles sur $\mathbb{F}_p$.

Soit p un nombre premier, et soit $n \in \mathbb{N}^*$ un entier fixé. On note pour tout $k \in \mathbb{N}^*$, $A(k)$ l'ensemble des polynômes irréductibles unitaires de degré k de $\mathbb{F}_p[X]$, et $I(k) = \mathrm{Card}(A(k))$. Le but de l'exercice est de donner une formule pour le calcul de $I(n)$.

1. Soit d un diviseur de n et $P \in A(d)$.

   (a) La relation de congruence est clairement reflexive, symétrique, et transitive (la propriété de divisibilité étant stable par somme). Ainsi, la congruence modulo P est une relation d'équivalence.

   (b) On montre que la relation de congruence est compatible avec $+$ et $\times$ de $\mathbb{F}_p[X]$. Soient Q_1, Q_2, R_1, R_2 tels que $Q_1 \equiv Q_2\ [P]$ et $R_1 \equiv R_2 \mod P$.

   - On a :
   $$(Q_2 + R_2) - (Q_1 + R_1) = (Q_2 - Q_1) + (R_2 - R_1),$$
   et, P divisant $Q_2 - Q_1$ et $R_2 - R_1$, P divise aussi $(Q_2 + R_2) - (Q_1 + R_1)$. Ainsi, $Q_1 + R_1 \equiv Q_2 + R_2\ [P]$.
   - De même,
   $$Q_2R_2 - Q_1R_1 = Q_2(R_2 - R_1) + R_1(Q_2 - Q_1),$$
   donc P divise $Q_2R_2 - Q_1R_1$, puis $Q_1R_1 \equiv Q_2R_2\ [P]$.

   Ainsi, les lois $+$ et $\times$ passent au quotient, définissant deux lois, qu'on notera de la même façon, sur l'espace quotient $\mathbb{K}$. Les propriétés liées à la structure d'anneau de $\mathbb{F}_p[X]$ restent vérifiées par passage au quotient, ainsi, $\mathbb{K}$ est muni d'une structure d'anneau commutatif. Il reste à vérifier que tout élément non nul est inversible.

   Soit donc $h \in \mathbb{K}$, non nul, représenté par un polynôme H de $\mathbb{F}_p[X]$. Comme P est irréductible et unitaire, $H \wedge P = 1$ ou $H \wedge P = P$. Puisque $h \neq 0$, H n'est pas divisible par P, donc $H \wedge P = 1$. D'après le théorème de Bézout, il existe donc deux polynômes U et V tels que

   $$HU + PV = 1.$$

En notant u la classe d'équivalence de U modulo P, il vient donc, par passage au quotient, la relation suivante dans $\mathbb{K}$:

$$h \cdot u = 1_{\mathbb{K}}.$$

Nous avons bien montré que tout élément non nul de l'anneau commutatif $\mathbb{K}$ est inversible, $\mathbb{K}$ est un corps.

Par ailleurs, d'après le théorème de la division euclidienne, $h \in \mathbb{K}$ admet un représentant dans $\mathbb{F}_p[X]$ de degré au plus $d-1$. Il y a un nombre fini de polynômes de degré au plus $d-1$ (plus exactement p^d, puisque chacun des n coefficients peut prendre p valeurs différentes). Ainsi $\boxed{\mathbb{K} \text{ est un corps fini.}}$

(c) χ étant la classe de X, les lois de $\mathbb{K}$ étant obtenues de celles de $\mathbb{F}_p[X]$ par passage au quotient, $P(\chi)$ est la classe de $P(X)$, c'est-à-dire 0. Ainsi, $P(\chi) = 0_{\mathbb{K}}$, donc $\boxed{P \text{ admet au moins la racine } \chi \text{ dans } \mathbb{K}}$.

(d)
- Puisque $\mathbb{K}$ est un corps, $(\mathbb{K}, +)$ est un groupe abélien.
- Puisque $\mathbb{F}_p$ est un sous-corps de $\mathbb{K}$, la restriction du produit de $\mathbb{K}$ à $\mathbb{F}_p \times \mathbb{K}$ défini une loi de composition interne. La structure de corps de $\mathbb{K}$ nous assure alors que celle loi est distributive sur la somme de $\mathbb{K}$, ainsi que sur la somme de $\mathbb{F}_p$, qu'elle respecte le neutre de $\mathbb{F}_p$ (qui est aussi le neutre de $\mathbb{K}$), et qu'elle vérifie la propriété d'associativité externe, obtenue par restriction de l'associativité de $\times$ dans $\mathbb{K}$.

Ainsi, $\boxed{\mathbb{K} \text{ est un espace vectoriel sur } \mathbb{F}_p}$.

Comme on l'a dit plus haut, tout élément de $\mathbb{K}$ admet un représentant de degré au plus $d-1$. Ainsi, $(1, \chi, \ldots, \chi^{d-1})$ est une famille génératrice de $\mathbb{K}$ en tant que $\mathbb{F}_p$-ev. Par ailleurs, le seul polynôme de degré au plus $d-1$ divisible par P de degré d est le polynôme nul. On en déduit sans peine la liberté de la famille $(1, \chi, \ldots, \chi^{d-1})$. Il s'agit donc d'une base, de cardinal d.

Ainsi, $\boxed{\mathbb{K} \text{ est un espace vectoriel de dimension } d \text{ sur } \mathbb{F}_p}$.

Tout vecteur étant alors déterminé de façon unique par le choix de d coordonnées dans $\mathbb{F}_p$ (après choix d'une base), $\boxed{\text{Card}(\mathbb{K}) = p^d}$ (cela se formalise en disant que $\mathbb{K}$ est alors isomorphe à $\mathbb{F}_p^d$).

2. $(\mathbb{K}^*, \times)$ est un groupe de cardinal $p^d - 1$. Donc, d'après le théorème de Lagrange, pour tout $x \in \mathbb{K}^*$, $x^{p^d-1} = 1$, donc $x^{p^d} = x$. Cette relation étant trivialement vraie pour $x = 0$ aussi, il vient :

$$\forall x \in \mathbb{K}, \quad \boxed{x^{p^d} = x}.$$

Vous aurez reconnu une généralisation du petit théorème de Fermat.

En notant $d_1 = \frac{n}{d}$, on obtient alors $\chi^{p^n} = (((\chi^{p^d})^{p^d}) \cdots)^{p^d} = \chi$, obtenu en élevant d_1 fois à la puissance p^d. Ainsi, χ est racine commune de P et $X^{p^n} - X$, donc que $P \wedge X^{p^n} - X \neq 1$. Or, les polynômes P et $X^{p^n} - X$ étant à coefficients dans $\mathbb{F}_p$, l'algorithme d'Euclide pour le calcul du PGCD permet d'affirmer que $P \wedge X^{p^n} - X$ est aussi à coefficients dans $\mathbb{F}_p$. Comme il divise P (dans $\mathbb{F}_p[X]$), et est différent de 1, l'irréductibilité de P amène $P \wedge X^{p^n} - X = P$, donc $\boxed{P \text{ divise } X^{p^d} - X}$.

3. Nous établissons la réciproque :

(a) On itère l'argument de la question 1 : à chaque étape, si $P = X^{p^n} - 1$ n'est pas scindé dans le corps $\mathbb{K}$ construit, on en considère un facteur irréductible Q de degré au moins 2, et on construit un corps $\mathbb{K}'$ de la même manière que dans la question 1, contenant $\mathbb{K}$ comme sous-corps, et dans lequel Q aura une racine. Dans ce corps $\mathbb{K}'$, le polynôme P a au moins une racine de plus que dans $\mathbb{K}$. On itère ce procédé jusqu'à ce que P soit scindé. On est assuré de la terminaison de cet algorithme du fait que P, dans n'importe quel sur-corps de $\mathbb{F}_p$ ne pourra jamais avoir plus de p^n racines. Le nombre de racines augmentant strictement à chaque étape, il y aura au maximum p^n étapes.

Ainsi, $\boxed{\text{il existe un corps } \mathbb{K}' \text{ contenant } \mathbb{F}_p, \text{ tel que } X^{p^n} - X \text{ soit scindé sur } \mathbb{K}'.}$

Ce procédé permet toujours de construire un « corps de décomposition » d'un polynôme P (corps dans lequel il sera scindé). La première étape donne un « corps de rupture » (corps dans lequel P admet une racine au moins)

Puisque $\mathbb{K}'$ contient $\mathbb{F}_p$, $\mathbb{K}'$ est de caractéristique p. Ainsi, $P' = p^n X^{p^n-1} - 1 = -1 \neq 0$. Donc une racine de P ne peut pas être racine de P', ce qui assure que $\boxed{\text{les racines de } P \text{ sont simples.}}$

(b) • $0 \in \mathbb{F}_{p^n}$

- Pour tout $(\omega_1, \omega_2) \in \mathbb{F}_{p^n}$,
$$(\omega_1 - \omega_2)^{p^n} = \omega_1^{p^n} - \omega_2^{p^n} = \omega_1 - \omega_2,$$
car dans un corps de caractéristique p, $(x+y)^p = x^p + y^p$, et, en distinguant les cas p pair et p impair, on obtient facilement $(x-y)^p = x^p - y^p$, puis, par itération, $(x-y)^{p^n} = x^{p^n} - y^{p^n}$. Ainsi, $\omega_1 - \omega_2 \in \mathbb{F}_{p^n}$.
- Pour tout $(\omega_1, \omega_2) \in \mathbb{F}_{p^n}$,
$$(\omega_1 \omega_2^{-1})^{p^n} = (\omega_1^{p^n})(\omega_2^{p^n})^{-1} = \omega_1 \omega_2^{-1}.$$
Donc $\omega_1 \omega_2^{-1} \in \mathbb{F}_{p^n}$.

On en déduit que $\boxed{\mathbb{F}_{p^n} \text{ est un sous-corps de } \mathbb{K}'}$.

Puisque pour tout $x \in \mathbb{F}_p$, on a $x^p = x$, on a, par itération, $x^{p^n} = x$, d'où $x \in \mathbb{F}_{p^n}$. Ainsi, $\boxed{\mathbb{F}_p \subset \mathbb{F}_{p^n}}$.

Enfin, les racines de $X^{p^n} - X$ étant toutes simples, et ce polynôme étant scindé sur $\mathbb{K}'$, elles sont au nombre de p^n, donc $\boxed{\text{Card}(\mathbb{F}_{p^n}) = p^n.}$

(c) P admet une racine x dans $\mathbb{F}_{p^n}$. Considérons $\varphi : \mathbb{F}_p[X] \mapsto \mathbb{F}_{p^n}$, le morphisme d'anneaux, bien et uniquement défini par $\varphi(k) = k$ si $k \in \mathbb{F}_p$ et $\varphi(X) = x$. Si Q est divisible par P, disons $Q = PR$, on a alors $\varphi(Q) = P(x)R(x) = 0$. Ainsi, φ passe au quotient, définissant un morphisme d'anneaux $\tilde{\varphi}$ de $\mathbb{K}$ vers $\mathbb{F}_{p^n}$, tel que $\tilde{\varphi}(\chi) = x$. C'est alors un morphisme de corps (par définition), et, comme tout morphisme de corps, il est injectif. En effet si $P \neq 0$, $\tilde{\varphi}(y) = 0$ implique
$$\tilde{\varphi}(1) = \tilde{\varphi}(y)\tilde{\varphi}(y^{-1}) = 0,$$
ce qui contredit $\tilde{\varphi}(1) = 1$. Ainsi, $\text{Ker}(\tilde{\varphi}) = \{0\}$, d'où l'injectivité.

Par conséquent, $\tilde{\varphi}$ induit un isomophisme de corps de $\mathbb{K}$ sur son image dans $\mathbb{F}_{p^n}$. En identifiant le corps $\mathbb{K}$ à son image, $\boxed{\text{on peut donc considérer } \mathbb{K} \text{ comme sous-corps de } \mathbb{F}_{p^n}}$.

(d) Comme dans 1(d), $\mathbb{F}_{p^n}$ est alors un espace vectoriel sur $\mathbb{K}$, de dimension finie. Comme $\mathbb{K}$ est de cardinal p^k, il existe donc un entier $k = \dim_{\mathbb{K}}(\mathbb{F}_{p^n})$ tel que
$$p^n = (p^d)^k = p^{kd}, \qquad \text{donc:} \qquad n = kd.$$
On en déduit que $\boxed{d \mid n.}$

4. Tout polynôme irréductible de degré $d \mid n$ divise $X^{p^n} - 1$ (question 2), et ceci une seule fois car les racines de ce dernier sont simples. Récirproquement, tout facteur irréductible de $X^{p^n} - 1$ est de degré $d \mid n$. Ainsi,
$$X^{p^n} - 1 = \prod_{d|n} \prod_{P \in A(d)} P.$$
En identifiant les degrés, il vient alors :
$$p^n = \sum_{d|n} \sum_{P \in A(d)} d = \sum_{d|n} dI(d).$$
On obtient la dernière identité par la formule d'inversion de Möbius, qu'on redémontre rapidement dans ce cas particulier :
$$\begin{aligned} \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d &= \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{d'|d} d' I(d') \\ &= \frac{1}{n} \sum_{d'|n} d' I(d') \sum_{d, d'|d} \mu\left(\frac{n}{d}\right). \end{aligned}$$
Le changement de variable $d'' = \frac{n}{d}$ dans la seconde somme amène
$$\frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d = \frac{1}{n} \sum_{d'|n} d' I(d') \sum_{d''|\frac{n}{d'}} \mu\left(d''\right).$$

Or, étant donné $k \in [\![2, n]\!]$, de décomposition $p_1^{\alpha_1}, \ldots, p_\ell^{\alpha_\ell}$,

$$\sum_{d|k} \mu(d) = \sum_{(\varepsilon_1,\ldots,\varepsilon_k)\in\{0,1\}^\ell} (-1)^{\varepsilon_1+\cdots+\varepsilon_k} = \left(\sum_{\varepsilon_1=0}^{1} (-1)^{\varepsilon_1}\right) \cdots \left(\sum_{\varepsilon_\ell=0}^{1} (-1)^{\varepsilon_\ell}\right) = 0.$$

Pour $k = 1$, on obtient en revanche $\sum_{d|k} \mu(d) = \mu(1) = (-1)^0 = 1$ Ainsi, reprenant le calcul précédent, la plupart des termes sont nuls, et il reste :

$$\boxed{\frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d = I(n).}$$