Écoles normales supérieures 2019

Épreuve de mathématiques D, MP, six heures

(corrigé)

Nous utiliserons abondamment, dans ce corrigé, le fait que si $\varphi : X \to Y$ est une bijection entre ensembles finis, et si ψ est une fonction définie sur Y et à valeurs dans un anneau, alors :

$$\sum_{y\in Y} \psi(y) = \sum_{x\in X} \psi(\varphi(x)).$$

I – Séries de Dirichlet et formules de sommation.

1. Soit $f \in \mathcal{F}_p^-(\mathbb{Z},\mathbb{C})$. Alors, pour tout $k \in \mathbb{Z}$, on a, du fait de la parité et p-périodicité de f :

$$f(k) = -f(-k) = -f(p-k). \tag{1}$$

En particulier, $f(0) = 0$ et $f(p) = 0$.
De plus, si p est impair, alors l'application $k \mapsto p-k$ induit une bijection de $[\![1, \frac{p-1}{2}]\!]$ dans $[\![\frac{p+1}{2}, p-1]\!]$ (sa réciproque est $k \mapsto p-k$), donc :

$$\mu_p(f) = \sum_{1\leqslant k\leqslant \frac{p-1}{2}} f(k) + \sum_{\frac{p+1}{2}\leqslant k\leqslant p-1} f(k) = \sum_{1\leqslant k\leqslant \frac{p-1}{2}} f(k) + \sum_{1\leqslant k\leqslant \frac{p-1}{2}} f(k-p) \overset{(1)}{=} 0.$$

Si p est pair (c'est-à-dire si $p = 2$), alors : $\mu_p(f) = f(1) + f(2) = f(1) + f(0)$, et d'après (1) on a $f(0) = -f(0)$ et $f(1) = -f(1)$, donc $f(0) = f(1) = 0$, donc $\mu_p(f) = 0$.
Ainsi, pour tout nombre premier p et toute fonction $f \in \mathcal{F}_p^-(\mathbb{Z},\mathbb{C})$, on a bien : $\mu_p(f) = 0$.

2. Nous devons normalement supposer g de classe C^1 ici (et non seulement dérivable), pour que les manipulations ci-dessous, où l'on intègre g', soient licites.

Soit $x \geqslant 1$. L'application S_h est constante par morceaux, égale à $S_h(n)$ sur $[n, n+1[$ pour tout $n \in \mathbb{N}^*$; on peut donc écrire :

$$\begin{aligned}
\int_1^x S_h(t)g'(t)\mathrm{d}t &= \sum_{1\leqslant n\leqslant [x]-1} \int_n^{n+1} S_h(t)g'(t)\mathrm{d}t + \int_{[x]}^x S_h(t)g'(t)\mathrm{d}t \\
&= \sum_{1\leqslant n\leqslant [x]-1} S_h(n)\int_n^{n+1} g'(t)\mathrm{d}t + S_h(x)\int_{[x]}^x g'(t)\mathrm{d}t \\
&= \sum_{1\leqslant n\leqslant [x]-1} S_h(n)(g(n+1)-g(n)) + S_h(x)g(x) - S_h(x)g([x]) \\
&= \sum_{1\leqslant n\leqslant [x]-1} S_h(n)g(n+1) - \sum_{1\leqslant n\leqslant x} S_h(n)g(n) + S_h(x)g(x) - S_h([x])g([x]).
\end{aligned}$$

Il suffit alors de faire le changement d'indice de sommation $n \mapsto n+1$ dans la première somme du membre de droite, et d'utiliser le fait que $S_h(n) - S_h(n-1) = h(n)$ pour tout $n \in \mathbb{N}^*$, pour reconnaître la formule de sommation attendue :

$$\int_1^x S_h(t)g'(t)\mathrm{d}t - S_h(x)g(x) = -\sum_{1\leqslant n\leqslant x} h(n)g(n).$$

3. Soient $f, g \in \mathcal{F}(\mathbb{N}^*, \mathbb{C})$, et x, y des réels tels que $1 \leqslant y \leqslant x$. D'abord :

$$S_{f*g}(x) = \sum_{1\leqslant n\leqslant x} \sum_{dd'=n} f(d)g(d'). \tag{2}$$

Il y a une bijection évidente entre :

$$\left\{(n,d,d') \in (\mathbb{N}^*)^3 \mid 1 \leqslant n \leqslant x,\ dd' = n\right\},$$

et :

$$\left\{(d,d') \in (\mathbb{N}^*)^2 \mid 1 \leqslant d \leqslant x,\ 1 \leqslant d' \leqslant \frac{x}{d}\right\},$$

donnée par : $(n,d,d') \mapsto (d,d')$, et de réciproque : $(d,d') \mapsto (dd',d,d')$. On en déduit :

$$\sum_{1\leqslant n\leqslant x} \sum_{dd'=n} f(d)g(d') = \sum_{1\leqslant d'\leqslant x} \sum_{1\leqslant d\leqslant \frac{x}{d'}} f(d)g(d') = \sum_{1\leqslant d'\leqslant x} g(d') \sum_{1\leqslant d\leqslant \frac{x}{d'}} f(d) = \sum_{1\leqslant d'\leqslant x} g(d') S_f\left(\frac{x}{d'}\right). \tag{3}$$

En combinant (2) et (3), on obtient :

$$S_{f*g}(x) = \sum_{1\leqslant d'\leqslant x} g(d') S_f\left(\frac{x}{d'}\right)$$

(les rôles de f et g sont bien sûr symétriques). Ensuite, d'après ce qu'on vient d'obtenir :

$$S_{f*g}(x) - \sum_{1\leqslant n\leqslant y} g(n) S_f\left(\frac{x}{n}\right) = \sum_{y<n\leqslant x} S_f\left(\frac{x}{n}\right) g(n) = \sum_{y<n\leqslant x} \sum_{1\leqslant m\leqslant \frac{x}{n}} f(m)g(n). \tag{4}$$

Or :

$$\left\{(n,m) \in (\mathbb{N}^*)^2 \mid y < n \leqslant x,\ 1 \leqslant m \leqslant \frac{x}{n}\right\} = \left\{(n,m) \in (\mathbb{N}^*)^2 \mid y < n \leqslant \frac{x}{m},\ 1 \leqslant m \leqslant \frac{x}{y}\right\},$$

donc :

$$\begin{aligned}\sum_{y<n\leqslant x} \sum_{1\leqslant m\leqslant \frac{x}{n}} f(m)g(n) = \sum_{1\leqslant m\leqslant \frac{x}{y}} \sum_{y<n\leqslant \frac{x}{m}} f(m)g(n) &= \sum_{1\leqslant m\leqslant \frac{x}{y}} f(m) \sum_{y<n\leqslant \frac{x}{m}} g(n) \\ &= \sum_{1\leqslant m\leqslant \frac{x}{y}} f(m)\left(S_g\left(\frac{x}{m}\right) - S_g(y)\right).\end{aligned} \tag{5}$$

En combinant (4) et (5), on obtient :

$$S_{f*g}(x) - \sum_{1\leqslant n\leqslant y} g(n) S_f\left(\frac{x}{n}\right) + S_f\left(\frac{x}{y}\right) S(y) = \sum_{1\leqslant m\leqslant \frac{x}{y}} f(m) S_g\left(\frac{x}{m}\right),$$

d'où le résultat.

Remarque. Cette formule de l'hyperbole est attribuée à Dirichlet.

4. (a) On a : $\dfrac{f(n)}{n^s} = \underset{n\to+\infty}{O}\left(\dfrac{1}{n^s}\right)$ parce que f est bornée. Or la série de Riemann $\displaystyle\sum_{n\geqslant 1} \frac{1}{n^s}$ converge parce que $s > 1$, donc la série $\displaystyle\sum_{n\geqslant 1} \frac{f(n)}{n^s}$ converge absolument par comparaison.

   (b) Soit $s \in \mathbb{R}$ tel que les séries $\displaystyle\sum_{n\geqslant 1} \frac{f(n)}{n^s}$ et $\displaystyle\sum_{n\geqslant 1} \frac{g(n)}{n^s}$ convergent absolument. Alors leur produit de Cauchy converge absolument, et d'après le théorème de sommation par paquets on a :

$$\sum_{n=1}^{+\infty} \frac{f(n)}{n^s} \sum_{n=1}^{+\infty} \frac{g(n)}{n^s} = \sum_{n=1}^{+\infty} \sum_{\substack{0\leqslant k,\ell\leqslant n \\ k\ell=n}} \frac{f(k)}{k^s}\frac{g(\ell)}{\ell^s} = \sum_{n=1}^{+\infty} \frac{1}{n^s} \sum_{\substack{0\leqslant k,\ell\leqslant n \\ k\ell=n}} f(k)g(\ell) = \sum_{n=1}^{+\infty} \frac{(f*g)(n)}{n^s},$$

   d'où le résultat. On retiendra cette formule, qui nous servira plusieurs fois :

$$\sum_{n=1}^{+\infty} \frac{f(n)}{n^s} \sum_{n=1}^{+\infty} \frac{g(n)}{n^s} = \sum_{n=1}^{+\infty} \frac{(f*g)(n)}{n^s}. \tag{6}$$

   (c) Le produit infini n'est pas défini dans ce problème, nous allons préciser ce qu'on entend par là. Montrons :

$$\forall s > 1, \quad L(s,f) = \lim_{T\to+\infty} \prod_{\substack{\ell \text{ premier} \\ \ell\leqslant T}} \left(1 - \frac{f(\ell)}{\ell^s}\right)^{-1},$$

   en ajoutant une hypothèse pour que cette identité (appelée *produit eulérien)* soit vraie. Supposons par exemple que f est bornée par 1, de sorte que pour tout $s > 1$, la série $\displaystyle\sum_{n\geqslant 1} \frac{f(n)}{n^s}$ converge absolument d'après la question 4.(a). Cette hypothèse sera suffisante pour ce problème (voir question 17).

   Soit $s > 1$. Notons d'abord que si f est complètement multiplicative, alors pour tout entier naturel non nul n, dont on écrit : $n = \ell_1^{m_1} \times \cdots \times \ell_r^{m_r}$ la décomposition en facteurs premiers, alors : $f(n) = f(\ell_1)^{m_1} \cdots f(\ell_r)^{m_r}$.

De la sorte, lorsqu'on développe les termes $\left(1-\frac{f(\ell)}{\ell^s}\right)^{-1}$ en série géométrique (ce qui est possible pour tout $\ell \geqslant 2$ car $\left|\frac{f(\ell)}{\ell^s}\right| < 1$ d'après l'hypothèse sur f) :

$$\forall \ell \geqslant 2, \quad \left(1-\frac{f(\ell)}{\ell^s}\right)^{-1} = \sum_{m=0}^{+\infty} \frac{f(\ell)^m}{\ell^{ms}},$$

et quand on fait le produit indexé par les nombres premiers $\ell_1, \ldots, \ell_r$ inférieurs ou égaux à $T \geqslant 2$, on obtient :

$$\prod_{\substack{\ell \text{ premier} \\ \ell \leqslant T}} \left(1-\frac{f(\ell)}{\ell^s}\right)^{-1} = \prod_{\substack{\ell \text{ premier} \\ \ell \leqslant T}} \sum_{m=0}^{+\infty} \frac{f(\ell)^m}{\ell^{ms}} = \sum_{(m_1,\ldots,m_r)\in\mathbb{N}^r} \frac{f(\ell_1)^{m_1}\cdots f(\ell_r)^{m_r}}{(\ell_1^{m_1}\cdots\ell_r^{m_r})^s} = \sum_{n\in\mathcal{N}(T)} \frac{f(n)}{n^s},$$

où $\mathcal{N}(T)$ désigne l'ensemble des entiers naturels dont tous les diviseurs premiers sont inférieurs ou égaux à T ; l'agencement des termes est permis par la convergence absolue de ce produit (fini) de séries absolument convergentes. Alors, pour tout $T \geqslant 2$, on a :

$$\left|L(s,f) - \prod_{\substack{\ell \text{ premier} \\ \ell \leqslant T}} \left(1-\frac{f(\ell)}{\ell^s}\right)^{-1}\right| = \left|\sum_{n\notin\mathcal{N}(T)} \frac{f(n)}{n^s}\right| \leqslant \sum_{n\notin\mathcal{N}(T)} \frac{|f(n)|}{n^s} \leqslant \sum_{n>T} \frac{|f(n)|}{n^s}.$$

Nous avons là le reste d'une série convergente, d'après la question 4.(a), donc il tend vers 0 quand $T \to +\infty$. Donc, d'après le théorème des gendarmes :

$$\lim_{T\to+\infty} \prod_{\substack{\ell \text{ premier} \\ \ell \leqslant T}} \left(1-\frac{f(\ell)}{\ell^s}\right)^{-1} = L(s,f),$$

d'où le résultat.

5. (a) Soit $s > \alpha$. Pour tout $x \geqslant 1$, la sommation d'Abel avec $g : n \mapsto \dfrac{1}{n^s}$ et $h = f$ implique :

$$\sum_{1\leqslant n\leqslant x} \frac{f(n)}{n^s} = \frac{S_f(x)}{x^s} + s\int_1^x \frac{S_h(t)}{t^{s+1}}\mathrm{d}t. \tag{7}$$

Par hypothèse, pour tout $x \geqslant 1$ on a : $|S_f(x)| \leqslant Mx^\alpha$. Donc pour tout $x \geqslant 1$, on a :

$$0 \leqslant \frac{|S_f(x)|}{x^s} \leqslant \frac{M}{x^{s-\alpha}} \underset{x\to+\infty}{\longrightarrow} 0.$$

De plus, l'application $t \mapsto \dfrac{S_h(t)}{t^{s+1}}$ est continue par morceaux sur $[1,+\infty[$, et au voisinage de $+\infty$ on a, par hypothèse sur S_h :

$$\frac{S_h(t)}{t^{s+1}} \underset{t\to+\infty}{=} O\left(\frac{1}{t^{s-\alpha+1}}\right).$$

L'intégrale de Riemann $\displaystyle\int_1^{+\infty} \frac{\mathrm{d}t}{t^{s-\alpha+1}}$ converge parce que $s-\alpha+1>1$ par hypothèse sur s. Donc, par comparaison, l'intégrale $\displaystyle\int_1^{+\infty} \frac{S_h(t)}{t^{s+1}}\mathrm{d}t$ converge absolument donc converge.

Quand $x\to+\infty$, la relation (7) donne donc l'existence (et finitude) de $\displaystyle\lim_{x\to+\infty}\sum_{1\leqslant n\leqslant x}\frac{f(n)}{n^s}$, et :

$$L(s,f)=s\int_1^{+\infty}\frac{S_f(t)}{t^{s+1}}\mathrm{d}t,$$

d'où le résultat.

(b) Pour tout $s>\alpha$, l'application $t\mapsto S_f(t)t^{-s-1}$ est évidemment continue par morceaux sur $[1,+\infty[$ (l'application S_f est constante sur tout intervalle de la forme $[n,n+1[$ où $n\in\mathbb{N}^*$, et se prolonge bien sûr par continuité à l'extrémité), et pour tout $t\in[1,+\infty[$ l'application $s\mapsto S_f(t)t^{-s-1}$ est continue sur $]\alpha,+\infty[$ par continuité des fonctions puissances.
De plus, pour tout compact K de $]\alpha,+\infty[$, il existe $a>\alpha$ tel que $K\subseteq[a,+\infty[$ (puisque K est fermé), et pour tout $(x,t)\in K\times[1,+\infty[$ on a :

$$\left|S_f(t)t^{-s-1}\right|\leqslant Mt^{\alpha-s-1}\leqslant Mt^{\alpha-a-1}\quad\text{(HYPOTHÈSE DE DOMINATION)},$$

et l'application $t\mapsto t^{\alpha-a-1}$ est continue et intégrable sur $[1,+\infty[$ parce que $\alpha-a-1<-1$ par hypothèse sur a.
Les hypothèses du théorème de continuité des intégrales à paramètres sont vérifiées sur tout compact de $]\alpha,+\infty[$, donc $s\mapsto\displaystyle\int_1^{+\infty}S_f(t)t^{-s-1}\mathrm{d}t$ est continue sur $]\alpha,+\infty[$. Par conséquent, l'application $s\mapsto L(s,f)$ est également continue sur $]\alpha,+\infty[$.

(c) D'après la question 1, on a $\mu_p(f)=0$, et f est p-périodique, donc pour tout entier $x\geqslant 1$ multiple de p on a $S_f(x)=0$. On en déduit, pour tout réel $x\geqslant 1$:

$$|S_f(x)|=\left|\sum_{p\left[\frac{x}{p}\right]\leqslant n\leqslant x}f(n)\right|\leqslant\sum_{p\left[\frac{x}{p}\right]\leqslant n\leqslant x}|f(n)|=\sum_{0\leqslant n\leqslant x-p\left[\frac{x}{p}\right]}|f(n)|\leqslant\sum_{0\leqslant n\leqslant p}|f(n)|.$$

Si l'on note $M=\displaystyle\sum_{0\leqslant n\leqslant p}|f(n)|$, alors pour tout réel $x\geqslant 1$ on a : $|S_f(x)|\leqslant M$. Donc, d'après les questions précédentes (avec $\alpha=0$), pour tout $s>0$ la série $\displaystyle\sum_{n\geqslant 1}\frac{f(n)}{n^s}$ converge et l'application $s\mapsto L(s,f)$ est continue sur $]0,+\infty[$.

(d) Petite étrangeté de l'énoncé : nous avons déjà besoin de la convergence de la série $\displaystyle\sum_{n\geqslant 1}\frac{1}{n^s}$ pour traiter la question 4.(a).

Pour tout $x \geqslant 1$, on a : $|S_1(x)| = [x] \leqslant x$. Donc, en appliquant la question 5.(a), on obtient la convergence de la série $\displaystyle\sum_{n\geqslant 1} \frac{1}{n^s}$ pour tout $s > 1$, et l'égalité :

$$\forall s > 1, \quad \zeta(s) = s\int_1^{+\infty} \frac{[t]}{t^{s+1}}\mathrm{d}t.$$

Ensuite, on écrit : $[t] = t + ([t] - t)$, de sorte que :

$$\forall s > 1, \quad \zeta(s) = s\int_1^{+\infty} \frac{\mathrm{d}t}{t^s} + s\int_1^{+\infty} \frac{[t]-t}{t^{s+1}}\mathrm{d}t = \frac{s}{s-1} + s\int_1^{+\infty} \frac{[t]-t}{t^{s+1}}\mathrm{d}t.$$

En reprenant le raisonnement de la question 5.(b), où l'on remplace $S_f(t)$ par $[t] - t$ (qui est de valeur absolue bornée par 1), on montre que l'application $s \mapsto s\displaystyle\int_1^{+\infty} \frac{[t]-t}{t^{s+1}}\mathrm{d}t$ est continue sur $]0, +\infty[$, donc en particulier elle est de limite finie en 1. Par conséquent :

$$\forall s > 1, \quad \zeta(s) = \frac{s}{s-1} + s\int_1^{+\infty} \frac{[t]-t}{t^{s+1}}\mathrm{d}t \underset{s\to 1}{\sim} \frac{1}{s-1},$$

et on en déduit :

$$\lim_{s\to 1}(s-1)\zeta(s) = 1.$$

II – Caractères modulo p.

6. (a) Petite imprécision de l'énoncé : les fonctions arithmétiques ont été définies sur $\mathbb{N}^*$, alors qu'un caractère est défini sur $\mathbb{Z}$. Heureusement, c'est presque sans impact sur le traitement de cette question.

Soient m et n deux entiers relatifs. Nous voulons montrer : $\chi(mn) = \chi(m)\chi(n)$. Si m ou n n'est pas premier avec p, alors cette égalité est une évidence : si par exemple m n'est pas premier avec p, alors mn non plus. Par définition d'un caractère modulo p, on a donc $\chi(mn) = 0$ et $\chi(m) = 0$, donc les deux membres de l'égalité voulue coïncident ; de même si n n'est pas premier avec p.
Si m et n sont premiers à p, alors l'égalité est évidente en utilisant le fait que χ relève un morphisme de $((\mathbb{Z}/p\mathbb{Z})^\times, \times)$ dans $(\mathbb{U}, \times)$, qui est multiplicatif par définition d'un morphisme. D'où le résultat.

(b) Si χ est un caractère, alors :

$$\forall n \in \mathbb{Z}, \quad \chi(-n) = \chi(-1)\chi(n) \tag{8}$$

d'après la question précédente.
Si χ est impair, alors (8) implique $\chi(-1)\chi(n) = -\chi(n)$ pour tout $n \in \mathbb{Z}$. En particulier, pour $n = 1$, cela donne : $\chi(-1) = -1$. Réciproquement, si $\chi(-1) = -1$, alors (8) donne

directement : $\forall n \in \mathbb{Z}$, $\chi(-n) = -\chi(n)$, donc χ est impair.

Remarque. Si $\chi(-1) \neq -1$, alors $\chi(-1) = 1$. En effet, si l'on prend $n = -1$ dans (8) :

$$(\chi(-1))^2 = \chi(1) = 1. \tag{9}$$

(c) Soient k et n deux entiers supérieurs ou égaux à 1. Alors :

$$(\chi * (\chi\tau_k))(n) = \sum_{d|n} \chi\left(\frac{n}{d}\right) \chi(d)\tau_k(d),$$

mais d'après la question 6.(a), un caractère est complètement multiplicatif, donc :

$$\sum_{d|n} \chi\left(\frac{n}{d}\right) \chi(d)\tau_k(d) = \sum_{d|n} \chi(n)\tau_k(d) = \chi(n) \sum_{d|n} \tau_k(d) = \chi(n)(1 * \tau_k)(n),$$

et le produit de convolution est associatif, comme nous l'avons admis dans l'énoncé, donc : $1 * \tau_k = \tau_{k+1}$. En conclusion, nous avons montré :

$$(\chi * (\chi\tau_k))(n) = \chi(n)\tau_{k+1}(n),$$

comme attendu.

7. (a) Montrons que xy est d'ordre st sous l'hypothèse que s et t sont premiers entre eux, x d'ordre s et y d'ordre t : soit d l'ordre de xy. Comme H est commutatif, on a $(xy)^k = x^k y^k$ pour tout $k \in \mathbb{Z}$. Or $x^{st} = 1_H$ car x est d'ordre s, et de même $y^{st} = 1_H$, donc : $(xy)^{st} = 1_H$. On en déduit que d divise st.
De plus, $(xy)^d = x^d y^d = 1_H$, donc : $x^d = y^{-d}$, puis : $x^{dt} = y^{-dt} = 1_H$, donc l'ordre de x divise dt, c'est-à-dire : s divise dt. Or s et t sont premiers entre eux, donc s divise d. On montre de même que t divise d et donc, comme s et t sont premiers entre eux : st divise d.
Puisque d et st sont associés et positifs, on en déduit : $d = st$. Ainsi xy est bien d'ordre st.

(b) Il y a une inattention dans l'énoncé : il s'agit de démontrer, *sans hypothèse sur s et t*, que si $x \in H$ et $y \in H$ sont d'ordres respectifs s et t, alors il existe un élément de H d'ordre $\mathrm{ppcm}(s,t)$.

Pour cela, on décompose s et t en nombres premiers :

$$s = \prod_{p \text{ premier}} p^{\alpha_p}, \quad t = \prod_{p \text{ premier}} p^{\beta_p},$$

où les α_p sont presque tous nuls (et de même pour les β_p). Avec ces notations, on a :

$$\mathrm{ppcm}(s,t) = \prod_{p \text{ premier}} p^{\max(\alpha_p,\beta_p)} = \prod_{\substack{p \text{ premier} \\ \alpha_p > \beta_p}} p^{\alpha_p} \times \prod_{\substack{p \text{ premier} \\ \alpha_p \leqslant \beta_p}} p^{\beta_p}.$$

Donc, si l'on pose :

$$s' = \prod_{\substack{p \text{ premier} \\ \alpha_p > \beta_p}} p^{\alpha_p}, \text{ et : } t' = \prod_{\substack{p \text{ premier} \\ \alpha_p \leqslant \beta_p}} p^{\beta_p},$$

alors :

— s' divise s ;

— t' divise t ;

— $s't' = \text{ppcm}(s,t)$;

— s' et t' sont premiers entre eux parce qu'ils n'ont pas de diviseur premier en commun.

De plus, il est facile de vérifier que $x^{\frac{s}{s'}}$ est d'ordre s' et $y^{\frac{t}{t'}}$ d'ordre t'. D'après la question précédente, le produit $z = x^{\frac{s}{s'}} y^{\frac{t}{t'}}$ est d'ordre $s't' = \text{ppcm}(s,t)$: d'où le résultat.

Remarque. Attention, en général $z = xy$ ne convient pas : il suffit de prendre x quelconque d'ordre $s \geqslant 2$ et $y = x^{-1}$ (qui est aussi d'ordre s) pour s'en convaincre : le produit xy est, dans ce cas, égal à l'élément neutre et est donc d'ordre $1 \neq \text{ppcm}(s,s)$.

(c) Notons t l'ordre de h. Soit $x \in H$, et notons s son ordre. D'après la question précédente, il existe un élément de H d'ordre $\text{ppcm}(s,t)$; mais $\text{ppcm}(s,t) \geqslant t$, et par hypothèse t est l'ordre maximal d'un élément de H. Ceci impose : $\text{ppcm}(s,t) = t$, c'est-à-dire : s divise t.
On a ainsi démontré que l'ordre de tout élément de H divise l'ordre de h.

(d) Soit d l'ordre maximal d'un élément de $G = (\mathbb{Z}/p\mathbb{Z})^\times$: démontrons que $d = \text{card}\,(G) = p-1$.
On a bien sûr $d \leqslant p-1$, et de plus, la question précédente implique :

$$\forall x \in G, \quad x^d = 1.$$

On en déduit que le polynôme $X^d - 1 \in \mathbb{Z}/p\mathbb{Z}[X]$ a au moins, pour racines, tous les éléments de G ; il a donc au moins $p-1$ racines. Or il est à coefficients dans un corps, donc il ne peut pas avoir plus de racines que son degré. Par conséquent : $d \geqslant p-1$. On en déduit : $d = p-1$. Il existe donc un élément d'ordre $p-1$ dans G : par conséquent il engendre G, qui est cyclique.

Remarque. Plus généralement, un sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique.

8. (a) Soit a un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ (qui existe d'après la question précédente), de sorte que tout $n \in G$ s'écrive sous la forme : $n = a^k$, où k est un entier relatif. Si $n \in G$ s'écrit $n = a^k$, on note alors $\chi_n : G \to \mathbb{U}$ le morphisme entièrement défini par : $\chi_n(a) = \exp\left(\frac{2ik\pi}{p-1}\right)$. Il est bien à valeurs dans $\mathbb{U}$, et correctement défini parce que k est unique modulo $p-1$: en effet, si $n = a^k = a^\ell$ où $k, \ell \in \mathbb{Z}$, alors $a^{k-\ell} = 1_G$ et donc l'ordre de a divise $k - \ell$; or a est d'ordre $p-1$, donc : $k \equiv \ell \bmod p-1$.
Montrons alors que l'application :

$$\Phi : \begin{cases} G & \to & \widehat{G} \\ n & \mapsto & \chi_n \end{cases}$$

est un isomorphisme de groupes. Si $n = a^k$ et $n' = a^\ell$ sont dans G, alors $nn' = a^{k+\ell}$, et donc :

$$\Phi(nn')(a) = \chi_{nn'}(a) = \exp\left(\frac{2i(k+\ell)\pi}{p-1}\right) = \exp\left(\frac{2ik\pi}{p-1}\right)\cdot\exp\left(\frac{2i\ell\pi}{p-1}\right) = \Phi(n)(a)\cdot\Phi(n')(a).$$

Les morphismes $\Phi(nn')$ et $\Phi(n)\Phi(n')$ coïncident sur le générateur ω de G, donc :

$$\Phi(nn') = \Phi(n)\Phi(n').$$

Ainsi Φ est bien un morphisme. Montrons qu'il est injectif : si $n = a^k \in \ker(\Phi)$, alors $\Phi(n) = 1_{\widehat{G}}$, donc : $\Phi(n)(a) = \exp\left(\frac{2ik\pi}{p-1}\right) = 1$. On en déduit qu'il existe $\ell \in \mathbb{Z}$ tel que : $\frac{2k\pi}{p-1} = 2\ell\pi$, c'est-à-dire : $k = \ell\cdot(p-1)$, donc $k \equiv 0 \bmod p-1$. On en déduit que $n = a^0 = 1$, donc $\ker(\Phi) = \{1\}$; ainsi Φ est de noyau trivial donc est injectif.
Montrons qu'il est surjectif : soit $\chi \in \widehat{G}$. Alors :

$$(\chi(a))^{p-1} = \chi(a^{p-1}) = \chi(1_G) = 1,$$

donc $\chi(a)$ est une racine $(p-1)$-ième de l'unité : il existe $k \in \mathbb{Z}$ tel que :

$$\chi(a) = \exp\left(\frac{2ik\pi}{p-1}\right) = \chi_{a^k}(a).$$

Donc les morphismes χ et χ_{a^k} coïncident sur un générateur de G, et on en déduit :

$$\chi = \chi_{a^k} = \Phi(a^k).$$

Par conséquent Φ est surjectif.
Nous avons donc démontré que Φ est un isomorphisme de groupes entre G et $\widehat{G}$. On en déduit : $\mathrm{card}(\widehat{G}) = \mathrm{card}(G) = p-1$, et de plus G est cyclique, donc $\widehat{G} = \Phi(G)$ également : d'où le résultat.

(b) Notons g le caractère de G naturellement associé à χ. Soit ℓ un entier relatif inversible modulo p et tel que $\chi(\ell) \neq 1$ (il en existe puisque χ est supposé non principal). L'application $\bar{k} \mapsto \overline{\ell k}$ est une permutation de G, d'inverse $k \mapsto \bar{\ell}^{-1}\bar{k}$. Par conséquent :

$$\mu_p(\chi) = \sum_{\bar{k}\in G} g(\bar{k}) = \sum_{\bar{k}\in G} g(\overline{\ell k}) = \sum_{\bar{k}\in G} g(\bar{\ell})g(\bar{k}) = g(\bar{\ell})\mu_p(\chi),$$

or $g(\bar{\ell}) \neq 1$ par hypothèse sur ℓ, donc : $\mu_p(\chi) = 0$.

(c) Soit c un entier premier à p. Pour tout caractère χ modulo p, on a $\overline{\chi}(c) = (\chi(c))^{-1}$ (inverse pour la multiplication), étant donné que $|\chi(c)|^2 = 1$ par définition d'un caractère. On en déduit, en utilisant la multiplicativité des caractères :

$$\sum_{\chi \bmod p} \chi(n)\overline{\chi}(c) = \sum_{\chi \bmod p} \chi(n)(\chi(c))^{-1} = \sum_{\chi \bmod p} \chi(nc^{-1}),$$

où c^{-1} est l'inverse de c modulo p. Si n n'est pas premier à p alors cette somme est trivialement nulle : supposons donc n premier à p. Alors, en notant a un générateur de G et Φ l'isomorphisme entre G et $\widehat{G}$ de la question précédente, on a :

$$\sum_{\chi \bmod p} \chi(nc^{-1}) = \sum_{g\in\widehat{G}} g(nc^{-1}) = \sum_{m\in G} \Phi(m)(nc^{-1}) = \sum_{k=0}^{p-2} \Phi(a^k)(nc^{-1}) = \sum_{k=0}^{p-2} \Big(\Phi(a)(nc^{-1})\Big)^k,$$

et en revenant à la définition de Φ donnée dans la question précédente, on observe que l'application $\Phi(a)(m)$ n'égale 1 qu'évaluée en l'élément neutre (du fait que l'image par $\Phi(a)$ d'un générateur de G soit une racine primitive $(p-1)$-ième de l'unité), et on en déduit :

— si $nc^{-1} \equiv 1 \bmod p$ (c'est-à-dire : $n \equiv c \bmod p$), alors :

$$\sum_{\chi \bmod p} \chi(nc^{-1}) = \sum_{k=0}^{p-2} 1 = p-1;$$

— si $nc^{-1} \not\equiv 1 \bmod p$ (c'est-à-dire : $n \not\equiv c \bmod p$), alors $\Phi(a)(nc^{-1}) \neq 1$ et on a :

$$\sum_{\chi \bmod p} \chi(nc^{-1}) = \frac{(\Phi(a)(nc^{-1}))^{p-1} - 1}{\Phi(a)(nc^{-1}) - 1} = \frac{1-1}{\Phi(a)(nc^{-1}) - 1} = 0.$$

En conclusion :

$$\sum_{\chi \bmod p} \chi(nc^{-1}) = \begin{cases} p-1 & \text{si } n \equiv c \bmod p, \\ 0 & \text{si } n \not\equiv c \bmod p. \end{cases}$$

Remarque. Le résultat de cette question est implicitement un résultat « d'orthogonalité » des caractères. On peut le généraliser à tout groupe fini commutatif, grâce à la dualité de Pontryagin.

9. (a) L'énoncé n'est pas clair là-dessus : il s'agit de démontrer l'existence d'un nombre réel $T_{k,\varepsilon}$ adéquat pour **tout** $\varepsilon > 0$, comme on le constate au moment de traiter la question suivante.

Il est admis dans l'énoncé que le produit de convolution est associatif. On a donc :

$$\forall k \geqslant 3, \quad \tau_k = \underbrace{(1 * \cdots * 1)}_{k-2 \text{ fois}} * (1 * 1) = \tau_{k-2} * \tau_2.$$

Cette relation incite à raisonner par récurrence (forte) sur k : pour tout entier $k \geqslant 2$, soit P_k la proposition :

$$\text{« } \forall \varepsilon > 0,\ \exists T_{k,\varepsilon} \in \mathbb{R}_+,\ \forall n \in \mathbb{N}^* : \quad \tau_k(n) \leqslant T_{k,\varepsilon} n^{\varepsilon}. \text{ »}$$

Si $k = 2$, alors cette proposition est admise par l'énoncé. Soit, donc, $k \geqslant 2$ un entier naturel tel qu'on ait P_j pour tout rang $j \leqslant k$. Soit $\varepsilon > 0$. Pour tout entier $n \geqslant 1$, on a alors :

$$\tau_{k+1}(n) = \tau_{k-1} * \tau_2(n) = \sum_{d|n} \tau_2(d) \tau_{k-1}\left(\frac{n}{d}\right),$$

et donc d'après P_2 et P_{k-1} (utilisées avec $\frac{\varepsilon}{2}$) on a pour tout entier $n \geqslant 1$:

$$\tau_{k+1}(n) \leqslant \sum_{d|n} T_{2,\frac{\varepsilon}{2}} d^{\frac{\varepsilon}{2}} T_{k-1,\frac{\varepsilon}{2}} \left(\frac{n}{d}\right)^{\frac{\varepsilon}{2}} = n^{\frac{\varepsilon}{2}} T_{2,\frac{\varepsilon}{2}} T_{k-1,\frac{\varepsilon}{2}} \sum_{d|n} 1 = n^{\frac{\varepsilon}{2}} T_{2,\frac{\varepsilon}{2}} T_{k-1,\frac{\varepsilon}{2}} \tau_2(n) \leqslant n^{\varepsilon} \left(T_{2,\frac{\varepsilon}{2}}\right)^2 T_{k-1,\frac{\varepsilon}{2}},$$

d'où P_{k+1} en posant $T_{k+1,\varepsilon} = \left(T_{2,\frac{\varepsilon}{2}}\right)^2 T_{k-1,\frac{\varepsilon}{2}}$.
Ainsi on a P_2, et pour tout entier $k \geqslant 2$ les propositions P_j, pour tout $j \in [\![2, k]\!]$, impliquent P_{k+1}. Donc, par principe de récurrence : pour tout $\varepsilon > 0$, il existe un nombre réel $T_{k,\varepsilon}$ tel que, pour tout $n \in \mathbb{N}^*$, on ait : $\tau_k(n) \leqslant T_{k,\varepsilon} n^{\varepsilon}$.

(b) Nous allons encore raisonner par récurrence sur k : pour tout entier $k \geqslant 1$, soit P_k la proposition :

$$\text{« } \forall \varepsilon > 0,\ \exists M_k(p,\varepsilon) \in \mathbb{R}_+,\ \forall x \in \mathbb{R}_+ : \quad |S_{\chi\tau_k}(x)| \leqslant M_k(p,\varepsilon) x^{1-\frac{1}{k}+\varepsilon}. \text{ »}$$

Notons que dans toute cette étude, le cas où $x < 1$ ne nous intéresse pas : dans ce cas $S_{\chi\tau_k}(x) = 0$ et la majoration voulue est vraie peu importe la constante réelle choisie. Il ne coûte donc rien de prendre $x \geqslant 1$.

Si $k = 1$, alors $\tau_k \chi = \chi$, et dans la question 8.(b) nous avons démontré que $\mu_p(\chi) = 0$ si χ n'est pas principal. Alors, en reprenant la résolution de la question 5.(c), *mutatis mutandis*, on a l'existence de $M \in \mathbb{R}_+$ tel que :

$$\forall x \geqslant 1, \quad |S_\chi(x)| \leqslant M. \tag{10}$$

En fait, on peut même prendre $M = p$.
Donc, pour tout $\varepsilon > 0$ et tout $x \geqslant 1$, on a : $|S_\chi(x)| \leqslant M x^{\varepsilon} = M x^{1-\frac{1}{1}+\varepsilon}$; d'où P_1 (on prend $M_1(p,\varepsilon) = M$ pour tout $\varepsilon > 0$).

À présent, soit $k \in \mathbb{N}^*$ tel qu'on ait P_k. D'après la question 6.(c), on a : $\chi\tau_{k+1} = \chi * (\chi\tau_k)$, donc, pour tout $x \geqslant 1$ et tout $y \in [1, x]$, on a d'après la méthode de l'hyperbole :

$$S_{\chi\tau_{k+1}}(x) = S_{\chi*(\chi\tau_k)}(x) = \sum_{1\leqslant n\leqslant y} \chi(n) S_{\chi\tau_k}\left(\frac{x}{n}\right) + \sum_{1\leqslant n\leqslant \frac{x}{y}} \chi(n)\tau_k(n) S_\chi\left(\frac{x}{n}\right) - S_{\chi\tau_k}\left(\frac{x}{y}\right) S_\chi(y).$$

Majorons ces trois quantités, à commencer par la première somme. Un caractère est borné par 1. En utilisant P_k on a, pour tout $\varepsilon > 0$, tout $x \geqslant 1$ et tout $y \in [1, x]$:

$$\left|\sum_{1\leqslant n\leqslant y} \chi(n) S_{\chi\tau_k}\left(\frac{x}{n}\right)\right| \leqslant \sum_{1\leqslant n\leqslant y} \left|S_{\chi\tau_k}\left(\frac{x}{n}\right)\right| \leqslant M_k(p,\varepsilon) x^{1-\frac{1}{k}+\varepsilon} \sum_{1\leqslant n\leqslant y} \frac{1}{n^{1-\frac{1}{k}+\varepsilon}}.$$

Il nous est nécessaire de savoir majorer les sommes partielles de Riemann. Or, en adaptant (7) à la situation, on obtient :

$$\forall s \in]0,+\infty[\setminus\{1\},\ \forall y \geqslant 1, \quad \sum_{1\leqslant n\leqslant y} \frac{1}{n^s} = \frac{[y]}{y^s} + s\int_1^y \frac{[t]}{t^{s+1}}\mathrm{d}t \leqslant \frac{1}{y^{s-1}} + s\int_1^y \frac{\mathrm{d}t}{t^s}$$
$$= \frac{1}{y^{s-1}} + \frac{s}{s-1}\left(1 - \frac{1}{y^{s-1}}\right)$$
$$= 1 + \frac{1}{s-1}\left(1 - \frac{1}{y^{s-1}}\right)$$

(une comparaison entre série et intégrale donne le même résultat ; nous laissons l'élève en exercice vérifier que pour $s = 1$ on a : $\forall y \geqslant 1$, $\sum_{1\leqslant n\leqslant y} \frac{1}{n} \leqslant 1 + \ln(y)$). Donc, pour tout $x \geqslant 1$, tout $y \in [1, x]$, et tout $\varepsilon > 0$ différent de $\frac{1}{k}$, en prenant $s = 1 - \frac{1}{k} + \varepsilon$, on a :

$$\left|\sum_{1\leqslant n\leqslant y} \chi(n) S_{\chi\tau_k}\left(\frac{x}{n}\right)\right| \leqslant M_k(p,\varepsilon) x^{1-\frac{1}{k}+\varepsilon}\left(1 + \frac{1}{\varepsilon - \frac{1}{k}}\left(1 - \frac{1}{y^{\varepsilon-\frac{1}{k}}}\right)\right). \tag{11}$$

En utilisant la majoration (10) et celle de la question précédente, on a également, pour tout $x \geqslant 1$, tout $y \in [1, x]$ et tout $\varepsilon > 0$:

$$\left|\sum_{1\leqslant n\leqslant \frac{x}{y}} \chi(n)\tau_k(n) S_\chi\left(\frac{x}{n}\right)\right| \leqslant MT_{k,\varepsilon} \sum_{1\leqslant n\leqslant \frac{x}{y}} n^\varepsilon \leqslant MT_{k,\varepsilon}\left(1 + \frac{1}{\varepsilon+1}\left(\left(\frac{x}{y}\right)^{\varepsilon+1} - 1\right)\right) \tag{12}$$

Enfin on utilise P_k pour montrer que, pour tout $x \geqslant 1$, tout $y \in [1, x]$ et tout $\varepsilon > 0$:

$$\left|S_{\chi\tau_k}\left(\frac{x}{y}\right) S_\chi(y)\right| \leqslant M \cdot M_k(p,\varepsilon)\left(\frac{x}{y}\right)^{1-\frac{1}{k}+\varepsilon}. \tag{13}$$

Pour voir quel est le meilleur choix de y à effectuer, examinons les ordres de grandeur : en combinant (11), (12) et (13), on a informellement :

$$|S_{\chi\tau_{k+1}}(x)| \ll x^{1-\frac{1}{k}+\varepsilon} \pm x\left(\frac{x}{y}\right)^{-\frac{1}{k}+\varepsilon} + \left(\frac{x}{y}\right)^{1+\varepsilon} + \left(\frac{x}{y}\right)^{1-\frac{1}{k}+\varepsilon},$$

Or, pour $\varepsilon > 0$, $x \geqslant 1$ et $y \leqslant x$, on a $x^{1-\frac{1}{k}+\varepsilon} \leqslant x^{1-\frac{1}{k+1}+\varepsilon}$ et $\left(\frac{x}{y}\right)^{1-\frac{1}{k}+\varepsilon} \leqslant \left(\frac{x}{y}\right)^{1-\frac{1}{k+1}+\varepsilon}$, donc les seuls termes à poser souci en vue de démontrer P_{k+1} sont le deuxième et le troisième. Pour cela, prenons $y = x^{\frac{1}{(1+\varepsilon)(1+k)}}$; ce choix est fait, entre autres, de sorte que :

$$\left(\frac{x}{y}\right)^{1+\varepsilon} = x^{1-\frac{1}{k+1}+\varepsilon}.$$

On a bien $y \in [1,x]$ parce que $x \geqslant 1$ et $\frac{1}{(1+\varepsilon)(1+k)} \leqslant 1$. On a aussi :

$$\forall \varepsilon > 0,\ \forall x \geqslant 1, \quad x\left(\frac{x}{y}\right)^{-\frac{1}{k}+\varepsilon} = x^{1+\varepsilon-\frac{1}{k+1}+\frac{1}{k}\left(\frac{1}{1+\varepsilon}-1\right)} \leqslant x^{1+\varepsilon-\frac{1}{k+1}}.$$

Alors, pour tout $\varepsilon > 0$ différent de $\frac{1}{k}$ et tout $x \geqslant 1$, les inégalités (11), (12) et (13) avec ce choix de y impliquent (après quelques majorations simplificatrices) :

$$|S_{\chi\tau_{k+1}}(x)| \leqslant \left[M_k(p,\varepsilon)\left(1+\left|\frac{1}{\varepsilon-\frac{1}{k}}\right|\right) + 2MT_{k,\varepsilon} + M\cdot M_k(p,\varepsilon)\right] x^{1-\frac{1}{k+1}+\varepsilon},$$

d'où le résultat voulu pour tout $\varepsilon > 0$ différent de $\frac{1}{k}$, en prenant pour $M_{k+1}(p,\varepsilon)$ le terme en facteur de $x^{1-\frac{1}{k+1}+\varepsilon}$.

On pourrait se passer du cas $\varepsilon = \frac{1}{k}$ pour la suite du problème, mais par acquit de conscience traitons-le également. Si $\varepsilon = \frac{1}{k}$, alors la majoration $\sum\limits_{1\leqslant n\leqslant y} \frac{1}{n} \leqslant 1+\ln(y)$ est la seule modification à apporter à nos majorations, qui aboutissent à :

$$|S_{\chi\tau_{k+1}}(x)| \leqslant M_k(p,\varepsilon)\left(1+\frac{\ln(x)}{(1+\varepsilon)(1+k)}\right) x^{1-\frac{1}{k}+\varepsilon} + \left(2MT_{k,\varepsilon} + M\cdot M_k(p,\varepsilon)\right) x^{1-\frac{1}{k+1}+\varepsilon},$$

et par croissances comparées l'application $x \mapsto \left(1+\frac{\ln(x)}{(1+\varepsilon)(1+k)}\right)\frac{1}{x^{\frac{1}{k}-\frac{1}{k+1}}}$ est de limite nulle au voisinage de $+\infty$, et continue sur $[1,+\infty[$, donc est bornée par une constante réelle $M'(\varepsilon,k) > 0$ selon un argument classique. On a donc :

$$|S_{\chi\tau_{k+1}}(x)| \leqslant \left[M_k(p,\varepsilon)M'(\varepsilon,k)x^{1-\frac{1}{k+1}+\varepsilon} + 2MT_{k,\varepsilon} + M\cdot M_k(p,\varepsilon)\right] x^{1-\frac{1}{k+1}+\varepsilon},$$

donc pour $\varepsilon = \frac{1}{k}$ nous avons également le résultat. Ainsi P_k implique P_{k+1}. Par récurrence, nous avons donc bien :

$$\forall k \in \mathbb{N}^*,\ \forall \varepsilon > 0,\ \exists M_k(p,\varepsilon) \in \mathbb{R}_+,\ \forall x \in \mathbb{R}_+ : \quad |S_{\chi\tau_k}(x)| \leqslant M_k(p,\varepsilon)x^{1-\frac{1}{k}+\varepsilon}.$$

10. Soit $k \in \mathbb{N}^*$. D'après la question précédente, pour tout $\varepsilon > 0$, il existe une constante $M_k(p,\varepsilon)$ telle que pour tout $x \geqslant 1$, on ait :

$$|S_{\chi\tau_k}(x)| \leqslant M_k(p,\varepsilon)x^{1-\frac{1}{k}+\varepsilon}.$$

Donc, d'après la question 5.(a), pour tout $\varepsilon > 0$ et tout $s > 1-\frac{1}{k}+\varepsilon$ la série $\sum\limits_{n\geqslant 1}\frac{\tau_k(n)\chi(n)}{n^s}$ converge. Or tout réel s de l'intervalle $\left]1-\frac{1}{k},+\infty\right[$ est inclus dans un intervalle de la forme $\left]1-\frac{1}{k}+\varepsilon,+\infty\right[$ pour un bon choix de $\varepsilon > 0$ (il suffit de prendre : $\varepsilon = \frac{s-(1-1/k)}{2} > 0$), donc

pour tout $s > 1 - \frac{1}{k}$ la série $\sum_{n\geqslant 1} \frac{\tau_k(n)\chi(n)}{n^s}$ converge, et sa somme égale $D_k(s,\chi)$; en particulier, $D_k(1,\chi)$ est bien défini. La continuité de $s \mapsto D_k(s,\chi)$ sur $\left]1-\frac{1}{k}, +\infty\right[$ se déduit de la même manière, à l'aide de la question 5.(b).

Soit $s > 1$. Nous allons démontrer par récurrence sur $k \geqslant 1$ l'égalité :

$$D_k(s,\chi) = L(s,\chi)^k.$$

Si $k = 1$, c'est vrai par définition, étant donné que dans ce cas on a : $D_1(s,\chi) = L(s,\tau_1\chi)$, or $\tau_1 = 1$, donc : $D_1(s,\chi) = L(s,\chi)$.

Soit $k \geqslant 1$ un entier tel que la relation : $D_k(s,\chi) = L(s,\chi)^k$ soit vérifiée. Les séries $\sum_{n\geqslant 1} \frac{\chi(n)}{n^s}$ et $\sum_{n\geqslant 1} \frac{\tau_k(n)\chi(n)}{n^s}$ convergent absolument (d'après la question 4.(a) pour la première série, et d'après le résultat de la question 9 pour la seconde, qui implique en particulier : $\frac{\tau_k(n)\chi(n)}{n^s} = \underset{n\to+\infty}{O}\left(\frac{1}{n^{\frac{s+1}{2}}}\right)$) donc, d'après la question 4.(b), la série $\sum_{n\geqslant 1} \frac{(\chi * \tau_k\chi)(n)}{n^s}$ converge absolument, et en appliquant la relation (6) on a :

$$\sum_{n=1}^{+\infty} \frac{(\chi * \tau_k\chi)(n)}{n^s} = \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s} \times \sum_{n=1}^{+\infty} \frac{\tau_k(n)\chi(n)}{n^s}.$$

La première somme du membre de droite égale $L(s,\chi)$, et la seconde égale $D_k(s,\chi)$, c'est-à-dire $L(s,\chi)^k$ d'après l'hypothèse de récurrence. Donc :

$$\sum_{n=1}^{+\infty} \frac{(\chi * \tau_k\chi)(n)}{n^s} = L(s,\chi)^{k+1}.$$

Mais, d'après la question 6.(c), la somme du membre de gauche est $\sum_{n=1}^{+\infty} \frac{(\chi\tau_{k+1})(n)}{n^s} = D_{k+1}(s,\chi)$. On a donc :

$$D_{k+1}(s,\chi) = L(s,\chi)^{k+1},$$

et ceci démontre que l'égalité au rang k implique celle au rang $k+1$. Par principe de récurrence, on a bien :

$$\forall k \in \mathbb{N}^*, \quad D_k(s,\chi) = L(s,\chi)^k. \tag{14}$$

Cette égalité vaut pour tout $s > 1$. Pour en déduire l'égalité en $s = 1$, prenons la limite de ces deux fonctions quand $s \to 1$; comme elles sont continues en 1 d'après ce qui précède et la question 5.(c), on en déduit :

$$\forall k \in \mathbb{N}^*, \quad D_k(1,\chi) = L(1,\chi)^k.$$

III – Calculs autour de $D_k(1,f)$.

11. Tout entier est congru à r modulo p si et seulement s'il est congru à $r+p$ modulo p ; il est donc évident que l'application $r \mapsto x_k(r;p)$ est p-périodique. Vérifions qu'elle est impaire : soit $r \in \mathbb{Z}$. L'application définie sur :

$$\left\{(m_1,\dots,m_k) \in [\![1,p-1]\!]^k \mid \prod_{i=1}^{k} m_i \equiv -r \bmod p\right\}$$

et à valeurs dans :

$$\left\{(m_1,\dots,m_k) \in [\![1,p-1]\!]^k \mid \prod_{i=1}^{k} m_i \equiv r \bmod p\right\},$$

définie par : $(m_1,\dots,m_{k-1},m_k) \mapsto (m_1,\dots,m_{k-1},p-m_k)$, est une bijection, de réciproque : $(m_1,\dots,m_{k-1},m_k) \mapsto (m_1,\dots,m_{k-1},p-m_k)$. On en déduit :

$$\begin{aligned} x_k(-r;p) = \frac{1}{p^k} \sum_{\substack{(m_1,\dots,m_r)\in[\![1,p-1]\!]^k \\ \prod_{i=1}^{r} m_i \equiv -r \bmod p}} \prod_{i=1}^{r} \cot\left(\frac{\pi m_i}{p}\right) &= \frac{1}{p^k} \sum_{\substack{(m_1,\dots,m_r)\in[\![1,p-1]\!]^k \\ \prod_{i=1}^{r} m_i \equiv r \bmod p}} \prod_{i=1}^{r-1} \cot\left(\frac{\pi m_i}{p}\right) \cot\left(\frac{\pi(p-m_r)}{p}\right) \\ &= -\frac{1}{p^k} \sum_{\substack{(m_1,\dots,m_r)\in[\![1,p-1]\!]^k \\ \prod_{i=1}^{r} m_i \equiv r \bmod p}} \prod_{i=1}^{r-1} \cot\left(\frac{\pi m_i}{p}\right) \cot\left(\frac{\pi m_r}{p}\right) \\ &= -x_k(r;p), \end{aligned}$$

démontrant que $r \mapsto x_k(r;p)$ est une fonction impaire : d'où le résultat.

12. Soit $N \geqslant 1$. On utilise la relation « d'orthogonalité » de la question 8.(c). Elle implique :

$$\frac{1}{p-1} \sum_{\chi \bmod p} \sum_{n=1}^{N} \bar{\chi}(r)\chi(n)\frac{\tau_k(n)}{n} = \frac{1}{p-1} \sum_{n=1}^{N} \frac{\tau_k(n)}{n} \sum_{\chi \bmod p} \bar{\chi}(r)\chi(n) = \sum_{\substack{n=1 \\ n\equiv r \bmod p}}^{N} \frac{\tau_k(n)}{n}. \tag{15}$$

Un raisonnement en tous points analogue aboutit à :

$$\begin{aligned} \frac{1}{p-1} \sum_{\chi \bmod p} \sum_{n=1}^{N} \bar{\chi}(-r)\chi(n)\frac{\tau_k(n)}{n} = \sum_{\substack{n=1 \\ n\equiv -r \bmod p}}^{N} \frac{\tau_k(n)}{n} &= \sum_{\substack{n=-1 \\ -n\equiv -r \bmod p}}^{-N} \frac{\tau_k(-n)}{-n} \\ &= -\sum_{\substack{n=-1 \\ n\equiv r \bmod p}}^{-N} \frac{\tau_k(|n|)}{n}. \end{aligned} \tag{16}$$

Or $\bar\chi(-r) = \bar\chi(-1)\bar\chi(r)$, et $\bar\chi(-1) \in \{-1, 1\}$ d'après la question 6.(b), donc $\bar\chi(-1) = \chi(-1)$. On en déduit, en soustrayant (15) et (16) :

$$\frac{1}{p-1} \sum_{\chi \bmod p} \bar\chi(r)(1-\chi(-1)) \sum_{n=1}^{N} \chi(n) \frac{\tau_k(n)}{n} = \sum_{\substack{|n|\leqslant N \\ n \equiv r \bmod p}} \frac{\tau_k(|n|)}{n}.$$

Le terme de la somme correspondant au caractère principal est nul, puisque $\chi_0(-1) = 1$, et on peut donc l'enlever si on souhaite être conforme à l'énoncé (mais nous ne le ferons pas, en vue de la question 16). Quand $N \to +\infty$, le membre de gauche a une limite finie, égale à :

$$\frac{1}{p-1} \sum_{\chi \bmod p} \bar\chi(r)(1-\chi(-1)) D_k(1,\chi) \overset{(14)}{=} \frac{1}{p-1} \sum_{\chi \bmod p} \bar\chi(r)(1-\chi(-1)) L(1,\chi)^k,$$

donc le membre de droite admet aussi une limite finie. On a démontré :

$$\frac{1}{p-1} \sum_{\chi \bmod p} \bar\chi(r)(1-\chi(-1)) L(1,\chi)^k = \lim_{N\to+\infty} \left(\sum_{\substack{|n|\leqslant N \\ n \equiv r \bmod r}} \frac{\tau_k(|n|)}{n} \right). \tag{17}$$

13. Pour tout $a \in [\![1, p-1]\!]$, on a $\frac{a}{p} \in]0,1[$ (et en particulier $\frac{a}{p} \notin \mathbb{Z}$), donc :

$$\sum_{a=1}^{p-1} B\left(\frac{a}{p}\right) \mathbf{e}\left(\frac{am}{p}\right) = \sum_{a=1}^{p-1} \left(\frac{a}{p} - \frac{1}{2}\right) \mathbf{e}\left(\frac{am}{p}\right) = \frac{1}{p} \sum_{a=1}^{p-1} a \left(\mathbf{e}\left(\frac{m}{p}\right)\right)^a - \frac{1}{2} \sum_{a=1}^{p-1} \left(\mathbf{e}\left(\frac{m}{p}\right)\right)^a,$$

et nous savons que pour tout $x \in \mathbb{C}$ différent de 1 :

$$\sum_{a=0}^{p-1} x^a = \frac{1-x^p}{1-x}, \text{ et : } \sum_{a=1}^{p-1} a x^a = -\frac{p x^p}{1-x} + x \frac{1-x^p}{(1-x)^2},$$

où la seconde somme s'obtient en dérivant la première, et en la multipliant par x. On peut prendre $x = \mathbf{e}\left(\frac{m}{p}\right)$; en effet m n'est pas divisible par p par hypothèse, donc $\mathbf{e}\left(\frac{m}{p}\right) \neq 1$. Alors, en utilisant le fait que $\left(\mathbf{e}\left(\frac{m}{p}\right)\right)^p = 1$:

$$\begin{aligned}
\sum_{a=1}^{p-1} B\left(\frac{a}{p}\right) \mathbf{e}\left(\frac{am}{p}\right) &= -\frac{1}{p} \frac{p}{1-\mathbf{e}\left(\frac{m}{p}\right)} - \frac{\mathbf{e}\left(\frac{m}{p}\right)}{2} \frac{1-\left(\mathbf{e}\left(\frac{m}{p}\right)\right)^{p-1}}{1-\mathbf{e}\left(\frac{m}{p}\right)} \\
&= -\frac{1}{1-\mathbf{e}\left(\frac{m}{p}\right)} - \frac{1}{2} \frac{\mathbf{e}\left(\frac{m}{p}\right)-1}{1-\mathbf{e}\left(\frac{m}{p}\right)} \\
&= \frac{\mathbf{e}\left(\frac{m}{p}\right)+1}{2\left(\mathbf{e}\left(\frac{m}{p}\right)-1\right)}.
\end{aligned}$$

En utilisant la technique de l'arc moitié, on obtient :

$$\frac{\mathbf{e}\left(\frac{m}{p}\right)+1}{\mathbf{e}\left(\frac{m}{p}\right)-1}=\frac{\mathbf{e}\left(\frac{m}{2p}\right)+\mathbf{e}\left(-\frac{m}{2p}\right)}{\mathbf{e}\left(\frac{m}{2p}\right)-\mathbf{e}\left(-\frac{m}{2p}\right)}=\frac{2\cos\left(\frac{\pi m}{p}\right)}{2i\sin\left(\frac{\pi m}{p}\right)}=-i\cot\left(\frac{\pi m}{p}\right), \tag{18}$$

et on en déduit le résultat voulu :

$$\sum_{a=1}^{p-1} B\left(\frac{a}{p}\right)\mathbf{e}\left(\frac{am}{p}\right)=-\frac{i}{2}\cot\left(\frac{\pi m}{p}\right).$$

14. (a) *Remarque.* Par commodité, ici et dans le reste de ce corrigé, nous interpréterons toute somme sur $k\in[\![1,p]\!]$ comme une somme sur $\bar{k}\in\mathbb{Z}/p\mathbb{Z}$, tant que nous sommons des fonctions p-périodiques ; c'est en particulier le cas des caractères modulo p et de $x\mapsto\mathbf{e}\left(\frac{mx}{p}\right)$. Notamment, lorsqu'il apparaîtra a^{-1} dans une telle somme, où a est un entier, nous y entendrons bien sûr l'inverse de a modulo p.

Si n est un multiple de p, alors $\chi(n)=0$, mais on a aussi $\mathbf{e}\left(\frac{mn}{p}\right)=1$ pour tout entier m, et donc dans ce cas : $\tau(\chi,n)=\mu_p(\chi)=0$ (d'après la question 8.(b)). Ainsi l'égalité $\tau(\chi,n)=\chi(n)\tau(\chi)$ est bien vérifiée sous cette hypothèse.
Supposons à présent que n est premier à p. Notre raisonnement suit de près celui de la question 8.(b) : l'application $\bar{m}\mapsto\bar{m}\bar{n}$ est une permutation de G, d'inverse $\bar{m}\mapsto\bar{m}\bar{n}^{-1}$. Par conséquent :

$$\tau(\chi)=\sum_{m=1}^{p-1}\chi(m)\mathbf{e}\left(\frac{m}{p}\right)=\sum_{m=1}^{p-1}\chi(mn)\mathbf{e}\left(\frac{mn}{p}\right)=\chi(n)\sum_{m=1}^{p-1}\chi(m)\mathbf{e}\left(\frac{mn}{p}\right)=\chi(n)\tau(\chi,n),$$

donc finalement, en utilisant le fait que $\chi(n)^{-1}=\chi(n^{-1})=\bar{\chi}(n)$:

$$\tau(\chi,n)=\bar{\chi}(n)\tau(\chi),$$

d'où le résultat dans tous les cas.

(b) Pour tout $n\in[\![1,p]\!]$, on a d'après la question précédente : $|\tau(\chi,n)|^2=|\tau(\chi)|^2$, par conséquent :

$$\sum_{n=1}^{p}|\tau(\chi,n)|^2=(p-1)|\tau(\chi)|^2. \tag{19}$$

Mais on a aussi :

$$\begin{aligned}\sum_{n=1}^{p}|\tau(\chi,n)|^2&=\sum_{n=1}^{p}\sum_{m_1,m_2\in G}\chi(m_1)\mathbf{e}\left(\frac{m_1n}{p}\right)\bar{\chi}(m_2)\overline{\mathbf{e}\left(\frac{m_2n}{p}\right)}\\&=\sum_{n=1}^{p}\sum_{m_1,m_2\in G}\chi(m_1)\bar{\chi}(m_2)\mathbf{e}\left(\frac{(m_1-m_2)n}{p}\right).\end{aligned}$$

Pour calculer cette somme, nous allons utiliser le fait que pour tout $k \in \mathbb{Z}$, on a :

$$\sum_{n=1}^{p} \mathbf{e}\left(\frac{kn}{p}\right) = \begin{cases} p & \text{si } k \equiv 0 \bmod p, \\ 0 & \text{si } k \not\equiv 0 \bmod p. \end{cases}$$

Le calcul est immédiat. On en déduit :

$$\begin{aligned} \sum_{n=1}^{p} |\tau(\chi, n)|^2 = \sum_{m_1, m_2 \in G} \chi(m_1)\bar{\chi}(m_2) \sum_{n=1}^{p} \mathbf{e}\left(\frac{(m_1 - m_2)n}{p}\right) &= \sum_{\substack{m_1, m_2 \in G \\ m_1 = m_2}} \chi(m_1)\bar{\chi}(m_2)p \\ &= p \sum_{m_1=1}^{p-1} |\chi(m_1)|^2 \\ &= p(p-1). \end{aligned} \tag{20}$$

En comparant (19) et (20), on obtient :

$$|\tau(\chi)|^2 = p.$$

(c) Le résultat de cette question est FAUX si on ne suppose pas χ **impair**. Nous le faisons donc dans ce qui suit (et en particulier χ n'est pas le caractère principal).

D'après la question précédente, on a $\tau(\chi) \neq 0$ car $|\tau(\chi)|^2 = p$, et on a : $\tau(\chi) = \dfrac{p}{\overline{\tau(\chi)}}$; de plus, en prenant le conjugué dans l'identité de la question 14.(a), on a :

$$\forall n \in \mathbb{N}^*, \quad \chi(n)\overline{\tau(\chi)} = \overline{\tau(\chi, n)},$$

et on vérifie aisément que $\overline{\tau(\chi, n)} = \tau(\bar{\chi}, -n)$ pour tout $n \in \mathbb{N}^*$, donc :

$$\forall n \in \mathbb{N}^*, \quad \chi(n) = \frac{1}{\overline{\tau(\chi)}}\tau(\bar{\chi}, n) = \frac{\tau(\chi)}{p}\tau(\bar{\chi}, -n).$$

Alors :

$$L(1, \chi) = \frac{\tau(\chi)}{p} \sum_{n=1}^{+\infty} \frac{\tau(\bar{\chi}, -n)}{n} = \frac{\tau(\chi)}{p} \sum_{n=1}^{+\infty} \sum_{a=1}^{p} \frac{\bar{\chi}(m)}{n} \mathbf{e}\left(-\frac{an}{p}\right) = \frac{\tau(\chi)}{p} \sum_{a=1}^{p} \bar{\chi}(a) \sum_{n=1}^{+\infty} \frac{1}{n} \mathbf{e}\left(-\frac{an}{p}\right).$$

De plus, si χ est impair, on a immédiatement $\tau(\bar{\chi}, -n) = -\tau(\bar{\chi}, n)$ (après le changement d'indice de sommation $a \mapsto -a$, qui permute G), donc on a également :

$$L(1, \chi) = -\frac{\tau(\chi)}{p} \sum_{n=1}^{+\infty} \frac{\tau(\bar{\chi}, n)}{n} = -\frac{\tau(\chi)}{p} \sum_{a=1}^{p} \bar{\chi}(a) \sum_{n=1}^{+\infty} \frac{1}{n} \mathbf{e}\left(\frac{an}{p}\right).$$

Donc, en faisant la moyenne des deux égalités ci-dessus :

$$L(1,\chi) = \frac{\tau(\chi)}{p} \sum_{a=1}^{p} \bar{\chi}(a) \sum_{n=1}^{+\infty} \frac{1}{2n} \left(\mathbf{e}\left(-\frac{an}{p}\right) - \mathbf{e}\left(\frac{an}{p}\right)\right).$$

Or, d'après la formule admise dans l'énoncé, pour tout $a \in \mathbb{Z}$ on a :

$$\sum_{n=1}^{+\infty} \frac{1}{2n} \left(\mathbf{e}\left(-\frac{an}{p}\right) - \mathbf{e}\left(\frac{an}{p}\right)\right) = -i \sum_{n=1}^{+\infty} \frac{1}{n} \sin\left(\frac{2\pi na}{p}\right) = i\pi B\left(\frac{a}{n}\right).$$

En conclusion, si χ est impair :

$$L(1,\chi) = \frac{i\pi\tau(\chi)}{p} \sum_{a=1}^{p} \bar{\chi}(a) B\left(\frac{a}{n}\right).$$

15. Soit χ un caractère modulo p impair. Alors $\tau(\chi) = \sum_{m=1}^{p-1} \chi(m)\mathbf{e}\left(\frac{m}{p}\right)$, et en injectant cette expression dans l'égalité de la question précédente on a :

$$L(1,\chi) = \frac{i\pi}{p} \sum_{a=1}^{p} \sum_{m=1}^{p} \chi(m)\bar{\chi}(a) B\left(\frac{a}{n}\right) \mathbf{e}\left(\frac{m}{p}\right) = \frac{i\pi}{p} \sum_{a=1}^{p-1} \sum_{m=1}^{p-1} \chi(ma^{-1}) B\left(\frac{a}{n}\right) \mathbf{e}\left(\frac{m}{p}\right)$$

Or, pour $a \in [\![1, p-1]\!]$, l'application $\bar{m} \mapsto \bar{a}\bar{m}$ est une permutation de G, suivant un raisonnement déjà utilisé précédemment. Donc :

$$\begin{aligned} L(1,\chi) = \frac{i\pi}{p} \sum_{a=1}^{p-1} \sum_{m=1}^{p-1} \chi(ama^{-1}) B\left(\frac{a}{n}\right) \mathbf{e}\left(\frac{am}{p}\right) &= \frac{i\pi}{p} \sum_{m=1}^{p-1} \sum_{a=1}^{p-1} \chi(m) B\left(\frac{a}{n}\right) \mathbf{e}\left(\frac{am}{p}\right) \\ &= \frac{i\pi}{p} \sum_{m=1}^{p-1} \chi(m)\sigma_p(m), \end{aligned}$$

où σ_p fut défini dans la question 13. En réutilisant le résultat de cette question, on en déduit :

$$L(1,\chi) = \frac{\pi}{2p} \sum_{m=1}^{p-1} \chi(m) \cot\left(\frac{\pi m}{p}\right).$$

16. D'après la question précédente, pour tout caractère impair χ :

$$L(1,\chi)^k = \left(\frac{\pi}{2p}\right)^k \left(\sum_{m=1}^{p-1} \chi(m) \cot\left(\frac{\pi m}{p}\right)\right)^k = \frac{1}{p^k} \left(\frac{\pi}{2}\right)^k \sum_{(m_1,\dots,m_k)\in[\![1,p-1]\!]^k} \prod_{i=1}^{k} \chi(m_i) \prod_{i=1}^{k} \cot\left(\frac{\pi m_i}{p}\right).$$

Alors, la relation (17) de la question 12 :

$$\frac{1}{p-1} \sum_{\chi \bmod p} \bar{\chi}(r)(1-\chi(-1))L(1,\chi)^k = \lim_{N\to+\infty} \left(\sum_{\substack{|n|\leqslant N \\ n\equiv r \bmod p}} \frac{\tau_k(|n|)}{n}\right)$$

implique :

$$\frac{1}{p^k}\left(\frac{\pi}{2}\right)^k \frac{1}{p-1} \sum_{(m_1,\dots,m_k)\in[\![1,p-1]\!]^k} \prod_{i=1}^k \cot\left(\frac{\pi m_i}{p}\right) \sum_{\chi \bmod p} \bar\chi(r)(1-\chi(-1))\chi\left(\prod_{i=1}^k m_i\right) = \lim_{N\to+\infty} \left(\sum_{\substack{|n|\leqslant N \\ n\equiv r \bmod p}} \frac{\tau_k(|n|)}{n} \right). \quad (21)$$

L'expression de $L(1,\chi)^k$ en fonction des cotangentes ne vaut *a priori* que pour les caractères impairs, mais nous pouvons bel et bien l'utiliser pour tous les caractères dans la somme ci-dessus : en effet $\chi(-1)-1=0$ pour tout caractère non impair, comme nous l'avions déjà déduit de la relation (9), et donc n'importe quel nombre en facteur de $\chi(-1)-1$, pour χ non impair, n'affecte pas la valeur de la somme ci-dessus.
En utilisant la relation « d'orthogonalité » de la question 8.(c), on a :

$$\frac{1}{p-1}\sum_{\chi \bmod p} \bar\chi(r)\chi\left(\prod_{i=1}^k m_i\right) = \begin{cases} 1 & \text{si } m_1\cdots m_k \equiv r \bmod p, \\ 0 & \text{si } m_1\cdots m_k \not\equiv r \bmod p. \end{cases}$$

De plus, $\chi(-1)\in\mathbb{R}$ et un caractère est complètement multiplicatif, donc pour tout $r\in\mathbb{Z}$ on a $\bar\chi(r)\chi(-1) = \bar\chi(r)\bar\chi(-1) = \bar\chi(-r)$, et on en déduit semblablement :

$$\frac{1}{p-1}\sum_{\chi \bmod p} \bar\chi(r)\chi(-1)\chi\left(\prod_{i=1}^k m_i\right) = \begin{cases} 1 & \text{si } m_1\cdots m_k \equiv -r \bmod p, \\ 0 & \text{si } m_1\cdots m_k \not\equiv -r \bmod p. \end{cases}$$

En conclusion :

$$\frac{1}{p^k}\left(\frac{\pi}{2}\right)^k \frac{1}{p-1} \sum_{(m_1,\dots,m_k)\in[\![1,p-1]\!]^k} \prod_{i=1}^k \cot\left(\frac{\pi m_i}{p}\right) \sum_{\chi \bmod p} \bar\chi(r)(1-\chi(-1))\chi\left(\prod_{i=1}^k m_i\right) = \frac{1}{p^k}\left(\frac{\pi}{2}\right)^k \left(\sum_{\substack{(m_1,\dots,m_k)\in[\![1,p-1]\!]^k \\ m_1\cdots m_r\equiv r \bmod p}} \prod_{i=1}^k \cot\left(\frac{\pi m_i}{p}\right) - \sum_{\substack{(m_1,\dots,m_k)\in[\![1,p-1]\!]^k \\ m_1\cdots m_r\equiv -r \bmod p}} \prod_{i=1}^k \cot\left(\frac{\pi m_i}{p}\right) \right).$$

On reconnaît $\left(\frac{\pi}{2}\right)^k (x_k(r;p) - x_k(-r;p))$ par définition. Or $r\mapsto x_k(-r;p)$ est impaire d'après la question 11. On en déduit :

$$\frac{1}{p^k}\left(\frac{\pi}{2}\right)^k \frac{1}{p-1} \sum_{(m_1,\dots,m_k)\in[\![1,p-1]\!]^k} \prod_{i=1}^k \cot\left(\frac{\pi m_i}{p}\right) \sum_{\chi \bmod p} \bar\chi(r)(1-\chi(-1))\chi\left(\prod_{i=1}^k m_i\right) = 2\left(\frac{\pi}{2}\right)^k x_k(r;p). \quad (22)$$

En combinant (21) et (22), on obtient l'identité désirée :

$$x_k(r;p) = \frac{1}{2}\left(\frac{2}{\pi}\right)^k \lim_{N\to+\infty} \left(\sum_{\substack{|n|\leqslant N \\ n\equiv r \bmod p}} \frac{\tau_k(|n|)}{n} \right). \tag{23}$$

À présent, supposons $p \neq 2$ (sinon $\frac{p-1}{2} \notin \mathbb{N}$), et montrons :

$$\forall f \in \mathcal{F}_p^-(\mathbb{Z},\mathbb{C}), \quad D_k(1,f) = 2\left(\frac{\pi}{2}\right)^k \sum_{r=1}^{\frac{p-1}{2}} f(r)x_k(r,p).$$

Les applications $f \mapsto D_k(1,f)$ et $f \mapsto 2\left(\frac{\pi}{2}\right)^k \sum_{r=1}^{\frac{p-1}{2}} f(r)x_k(r,p)$ sont définies sur $\mathcal{F}_p^-(\mathbb{Z},\mathbb{C})$ et $\mathbb{Q}$-linéaires. Par conséquent, pour montrer qu'elles sont égales, il suffit de démontrer qu'elles coïncident sur une famille génératrice de $\mathcal{F}_p^-(\mathbb{Z},\mathbb{C})$.
Or nous avons le résultat suivant : le $\mathbb{Q}$-espace vectoriel $\mathcal{F}_p^-(\mathbb{Z},\mathbb{C})$ est engendré par les caractères impairs modulo p. Admettons-le *provisoirement*, et voyons comment en déduire la formule demandée : si χ est un caractère impair modulo p, alors la parité et la périodicité de χ et de $r \mapsto x_k(r;p)$ impliquent :

$$\sum_{r=1}^{\frac{p-1}{2}} \chi(r)x_k(r;p) \overset{(1)}{=} \sum_{r=1}^{\frac{p-1}{2}} (-\chi(p-r))(-x_k(p-r;p)) = \sum_{r=\frac{p-1}{2}+1}^{p-1} \chi(r)x_k(r;p),$$

et donc, en utilisant la relation (23) :

$$\begin{aligned}
2\left(\frac{\pi}{2}\right)^k \sum_{r=1}^{\frac{p-1}{2}} \chi(r)x_k(r;p) = \left(\frac{\pi}{2}\right)^k \sum_{r=1}^{p-1} \chi(r)x_k(r;p) &= \frac{1}{2}\sum_{r=1}^{p-1} \lim_{N\to+\infty} \left(\sum_{\substack{|n|\leqslant N \\ n\equiv r \bmod p}} \chi(n)\frac{\tau_k(|n|)}{n} \right) \\
&= \frac{1}{2}\lim_{N\to+\infty} \sum_{|n|\leqslant N} \chi(n)\frac{\tau_k(|n|)}{n} \\
&= \frac{1}{2}\lim_{N\to+\infty} \left(\sum_{n=1}^{N} \chi(n)\frac{\tau_k(n)}{n} + \sum_{n=-1}^{-N} \chi(n)\frac{\tau_k(-n)}{n} \right) \\
&= \frac{1}{2}\lim_{N\to+\infty} \left(\sum_{n=1}^{N} \chi(n)\frac{\tau_k(n)}{n} + \sum_{n=1}^{N} \chi(-n)\frac{\tau_k(n)}{-n} \right).
\end{aligned}$$

Le caractère χ étant impair, pour tout $n \in \mathbb{Z}$ on a $\chi(-n) = -\chi(n)$, et on en déduit :

$$2\left(\frac{\pi}{2}\right)^k \sum_{r=1}^{\frac{p-1}{2}} \chi(r)x_k(r;p) = \lim_{N\to+\infty} \sum_{n=1}^{N} \chi(n)\frac{\tau_k(n)}{n} = D_k(1,\chi),$$

donc la relation désirée est vérifiée pour tout caractère impair modulo p, et d'après le résultat admis ci-dessus cette égalité vaut également pour toute fonction $f \in \mathcal{F}_p^-(\mathbb{Z},\mathbb{C})$.

Démontrons à présent le résultat admis. Si f est une fonction p-périodique s'annulant en les multiples entiers de p alors, en notant $\mathbf{1}_k : \mathbb{Z} \to \mathbb{C}$ la fonction indicatrice de $k + p\mathbb{Z}$ (autrement dit : elle vaut 1 en les entiers congrus à k modulo p, et 0 ailleurs), et ce pour tout $k \in \mathbb{Z}$, on a :

$$f = \sum_{k=1}^{p-1} f(k)\mathbf{1}_k,$$

et il suffit donc d'écrire ces fonctions indicatrices à l'aide de caractères. D'après la question 8.(c) :

$$\forall k \in [\![1, p-1]\!], \quad \mathbf{1}_k = \frac{1}{p-1} \sum_{\chi \bmod p} \bar{\chi}(k)\chi,$$

donc toutes ces fonctions indicatrices s'écrivent comme combinaison linéaire de caractères, et par suite c'est le cas de toute fonction p-périodique s'annulant en les multiples entiers de p. Ceci démontre en passant que pour toute fonction p-périodique f s'annulant en les multiples de p :

$$f = \frac{1}{p-1} \sum_{\chi \bmod p} \left(\sum_{k=1}^{p-1} f(k)\bar{\chi}(k) \right) \chi, \tag{24}$$

relation que nous reverrons dans la question 18.

À présent, si $f \in \mathcal{F}_p^-(\mathbb{Z},\mathbb{C})$, c'est-à-dire si f est de plus supposée impaire, alors pour tout caractère χ non impair, on a $\chi(-1) = 1$ (voir (9)), et donc $\chi(n) = \chi(-n)$ pour tout $n \in \mathbb{Z}$ d'après (8). Par conséquent, pour tout caractère χ non impair, par p-périodicité on a :

$$\sum_{k=1}^{p-1} f(k)\bar{\chi}(k) \overset{(1)}{=} \sum_{k=1}^{p-1} -f(p-k)\bar{\chi}(k) = -\sum_{k=1}^{p-1} f(p-k)\bar{\chi}(-k) = -\sum_{k=1}^{p-1} f(p-k)\bar{\chi}(p-k),$$

et le changement d'indice de sommation $k \mapsto p-k$ implique que pour tout caractère χ non impair :

$$\sum_{k=1}^{p-1} f(k)\bar{\chi}(k) = -\sum_{k=1}^{p-1} f(k)\bar{\chi}(k),$$

c'est-à-dire : $\sum_{k=1}^{p-1} f(k)\bar{\chi}(k) = 0$. On en déduit que si $f \in \mathcal{F}_p^-(\mathbb{Z},\mathbb{C})$, alors la relation (24) se réécrit :

$$f = \frac{1}{p-1} \sum_{\substack{\chi \bmod p \\ \chi \text{ impair}}} \left(\sum_{k=1}^{p-1} f(k)\bar{\chi}(k) \right) \chi.$$

Autrement dit, toute fonction de $\mathcal{F}_p^-(\mathbb{Z},\mathbb{C})$ s'écrit comme combinaison linéaire de caractères impairs modulo p, et c'est ce qu'on voulait démontrer.

17. En utilisant k fois la relation (6), démontrée dans la question 4.(b), avec la fonction ζ (qui est la somme d'une série absolument convergente pour tout $s > 1$ d'après la question 5.(d)), on a :

$$\zeta(s)^k = \sum_{n=1}^{+\infty} \frac{(1 * \cdots * 1)(n)}{n^s} = \sum_{n=1}^{+\infty} \frac{\tau_k(n)}{n^s},$$

la convergence absolue de $\displaystyle\sum_{n\geqslant 1} \frac{\tau_k(n)}{n^s}$ étant également conséquence du résultat de la question 4.(b).
De plus, en reprenant la démonstration de la question 10, où cette fois on prend $\chi = \chi_0$, on obtient :

$$L(s,\chi_0)^k = D_k(s,\chi_0) = \sum_{n=1}^{+\infty} \frac{\tau_k(n)\chi_0(n)}{n^s} = \sum_{\substack{n=1 \\ n\not\equiv 0 \bmod p}}^{+\infty} \frac{\tau_k(n)}{n^s}.$$

La nécessité de supposer $\chi \neq \chi_0$, dans la question 10, était pour avoir la convergence sur $\left]1-\frac{1}{k},+\infty\right[$, qui n'est plus vérifiée ici : elle l'est sur $]1,+\infty[$. Le reste de la démonstration se reprend sans dommage, puisque nous avons seulement besoin de la convergence absolue sur $]1,+\infty[$ pour utiliser la relation (6).
Par conséquent, on a bien l'égalité demandée :

$$\zeta(s)^k - L(s,\chi_0)^k = \sum_{n=1}^{+\infty} \frac{\tau_k(n)}{n^s} - \sum_{\substack{n=1 \\ n\not\equiv 0 \bmod p}}^{+\infty} \frac{\tau_k(n)}{n^s} = \sum_{\substack{n=1 \\ n\equiv 0 \bmod p}}^{+\infty} \frac{\tau_k(n)}{n^s}.$$

Pour montrer la relation : $L(s,\chi_0)^k = \zeta(s)^k \left(1-\frac{1}{p^s}\right)^k$, recourons au produit eulérien dont l'existence fut démontrée dans la question 4.(c). Comme 1 et χ_0 sont complètement multiplicatives, et bornées par 1 (hypothèse que nous avons rajoutée lors du traitement de cette question), on a :

$$\zeta(s) = \lim_{T\to+\infty} \prod_{\substack{\ell \text{ premier} \\ \ell\leqslant T}} \left(1-\frac{1}{\ell^s}\right)^{-1}, \tag{25}$$

et :

$$L(s,\chi_0) = \lim_{T\to+\infty} \prod_{\substack{\ell \text{ premier} \\ \ell\leqslant T}} \left(1-\frac{\chi_0(\ell)}{\ell^s}\right)^{-1}.$$

Par définition de χ_0, on a $\chi_0(p) = 0$ (c'est un caractère modulo p), et tout nombre premier ℓ distinct de p est premier à p, donc $\chi_0(\ell) = 1$. On en déduit :

$$L(s,\chi_0) = \lim_{T\to+\infty} \prod_{\substack{\ell \text{ premier} \\ \ell\neq p \\ \ell\leqslant T}} \left(1-\frac{1}{\ell^s}\right)^{-1}. \tag{26}$$

En comparant (25) et (26), la relation : $L(s,\chi_0)^k = \zeta(s)^k \left(1-\frac{1}{p^s}\right)^k$ devient une évidence.

18. En appliquant la relation (24) à $f - f(0)\mathbf{1}_p$, où $\mathbf{1}_p$ est la fonction indicatrice définie dans la résolution de la question 16 (égale à 1 en les multiples de p, égale à 0 sinon), on a :

$$f = f(0)\mathbf{1}_p + \frac{1}{p-1}\sum_{\chi \bmod p}\sum_{k=1}^{p-1} f(k)\chi(\bar{k})\chi = f(0)\mathbf{1}_p + \frac{1}{p-1}\sum_{\chi \bmod p} c_\chi(f)\chi,$$

où l'on a posé : $c_\chi(f) = \sum_{k=1}^{p-1} f(k)\bar{\chi}(k)$. Notons que $c_{\chi_0}(f) = \mu_p(f) - f(0)$.
On a donc, pour tout $s > 1$:

$$\begin{aligned} D_k(s,f) &= f(0)D_k(s,\mathbf{1}_p) + \frac{1}{p-1}\sum_{\chi \bmod p} c_\chi(f)D_k(s,\chi) \\ &\overset{(14)}{=} f(0)D_k(s,\mathbf{1}_p) + \frac{1}{p-1}\sum_{\chi \bmod p} c_\chi(f)L(s,\chi)^k. \end{aligned}$$

D'après la question précédente :

$$\forall s > 1, \quad D_k(s,\mathbf{1}_p) = \sum_{\substack{n=1 \\ n\equiv 0 \bmod p}}^{+\infty} \frac{\tau_k(n)}{n^s} = \zeta(s)^k - L(s,\chi_0)^k,$$

donc, pour tout $s > 1$, toujours d'après la question précédente :

$$\begin{aligned} D_k(s,f) &= f(0)\left(\zeta(s)^k - L(s,\chi_0)^k\right) + \frac{c_{\chi_0}(f)}{p-1}L(s,\chi_0)^k + \frac{1}{p-1}\sum_{\substack{\chi \bmod p \\ \chi\neq\chi_0}} c_\chi(f)L(s,\chi)^k \\ &= \zeta(s)^k\left[f(0) + \frac{\mu_p(f) - pf(0)}{p-1}\left(1 - \frac{1}{p^s}\right)^k\right] + \frac{1}{p-1}\sum_{\substack{\chi \bmod p \\ \chi\neq\chi_0}} c_\chi(f)L(s,\chi)^k. \end{aligned}$$

Pour tout χ non principal, l'application $s \mapsto L(s,\chi)^k$ est continue en 1, d'après la question 10. Par conséquent, $\lim_{s\to 1} D_k(s,f)$ existe, et est finie, si et seulement si :

$$\lim_{s\to 1}\zeta(s)^k\left[f(0) + \frac{\mu_p(f) - pf(0)}{p-1}\left(1 - \frac{1}{p^s}\right)^k\right] \tag{27}$$

existe, et est finie. En particulier, si $f(0) = 0$ et $\mu_p(f) = 0$, alors cette limite est clairement nulle. Dans ce cas $\lim_{s\to 1} D_k(s,f)$ existe et est finie, et on a $c_{\chi_0}(f) = 0$, donc :

$$\lim_{s\to 1} D_k(s,f) = \lim_{s\to 1}\frac{1}{p-1}\sum_{\substack{\chi \bmod p \\ \chi\neq\chi_0}} c_\chi(f)L(s,\chi)^k = \frac{1}{p-1}\sum_{\substack{\chi \bmod p \\ \chi\neq\chi_0}} c_\chi(f)L(1,\chi)^k.$$

Réciproquement, si $\lim_{s\to 1} D_k(s,f)$ existe et est finie, alors la limite de (27) existe également. Or $\zeta(s)^k \underset{s\to 1}{\sim} \dfrac{1}{(s-1)^k}$ d'après la question 5.(d) ; nous pouvons déjà en déduire que le terme en facteur de $\zeta(s)^k$ doit être nul quand on l'évalue en 1, mais ce n'est pas suffisant pour en déduire simplement que $f(0) = 0$ et $\mu_p(f) = 0$ (tout au plus peut-on en déduire que ces deux nombres sont proportionnels). Pour en tirer plus d'informations, notons que l'application :

$$g : s \mapsto f(0) + \frac{\mu_p(f) - pf(0)}{p-1}\left(1 - \frac{1}{p^s}\right)^k$$

est de classe C^∞ sur $\mathbb{R}$, et la formule de Taylor-Young assure qu'elle est équivalente quand $s \to 1$ à une quantité de la forme $\dfrac{g^{(j)}(1)}{j!}(s-1)^j$, où $g^{(j)}$ est la première dérivée à ne pas s'annuler en 1 (s'il en existe). Alors, l'existence de la limite (27), et l'équivalent $\zeta(s)^k \underset{s\to 1}{\sim} \dfrac{1}{(s-1)^k}$, impliquent que les $k-1$ premiers termes de son développement limité en 1 sont nuls. Par hypothèse $k \geqslant 2$, donc $k - 1 \geqslant 1$, et par conséquent $g(1) = g'(1) = 0$. C'est-à-dire, après simplifications :

$$\begin{cases} p(p^{k-1} - (p-1)^{k-1})f(0) + (p-1)^{k-1}\,\mu_p(f) &= 0, \\ -pf(0) + \mu_p(f) &= 0. \end{cases}$$

Déterminons si ce système est inversible. On a :

$$\begin{vmatrix} p(p^{k-1} - (p-1)^{k-1}) & (p-1)^{k-1} \\ -p & 1 \end{vmatrix} = p\begin{vmatrix} p^{k-1} & (p-1)^{k-1} \\ 0 & 1 \end{vmatrix} = p^k \neq 0,$$

donc nécessairement : $\mu_p(f) = f(0) = 0$.

En conclusion, $\lim_{s\to 1} D_k(s,f)$ existe, et est finie, si et seulement si $\mu_p(f) = f(0) = 0$, et dans ce cas :

$$\lim_{s\to 1} D_k(s,f) = \frac{1}{p-1}\sum_{\substack{\chi \bmod p \\ \chi \neq \chi_0}} c_\chi(f) L(1,\chi)^k.$$

IV – Un peu d'algèbre linéaire...

19. (a) L'ensemble $\mathbb{Q}[\alpha]$ est clairement l'image de l'application $\mathbb{Q}$-linéaire :

$$\Psi : \begin{cases} \mathbb{Q}[X] &\to \mathbb{C} \\ P &\mapsto P(\alpha) \end{cases}$$

donc c'est un $\mathbb{Q}$-espace vectoriel. Si l'on note $m = \deg(\pi_\alpha)$, montrons que $\left(\alpha^k\right)_{k\in[\![0,m-1]\!]}$ en est une base.

Montrons qu'il s'agit d'une famille libre de $\mathbb{Q}[\alpha]$: s'il existe une relation de dépendance linéaire : $\sum_{k=0}^{m-1} \lambda_k \alpha^k = 0$, où les λ_i sont des nombres rationnels, alors le polynôme $P = \sum_{k=0}^{m-1} \lambda_k X^k \in \mathbb{Q}[X]$ admet α pour racine et est de degré strictement inférieur à celui du polynôme minimal π_α : ce n'est possible que si $P = 0$. Donc les λ_i sont nuls et la seule relation de dépendance linéaire est la relation triviale : la famille $\left(\alpha^k\right)_{k\in[\![0,m-1]\!]}$ est $\mathbb{Q}$-libre.

Montrons qu'il s'agit d'une famille génératrice de $\mathbb{Q}[\alpha]$: soit $z \in \mathbb{Q}[X]$, et soit $P \in \mathbb{Q}[X]$ tel que $z = P(\alpha)$. Effectuons la division euclidienne dans $\mathbb{Q}[X]$ de P par π_α : il existe un couple unique $(Q, R) \in (\mathbb{Q}[X])^2$ tel que $\deg(R) < \deg(\pi_\alpha) = m$, de sorte que R puisse s'écrire $R = \sum_{k=0}^{m-1} \mu_k X^k$ où les μ_k sont des rationnels, et vérifiant : $P = Q\pi_\alpha + R$. En évaluant cette égalité en α, on obtient :

$$z = P(\alpha) = Q(\alpha)\underbrace{\pi_\alpha(\alpha)}_{=0} + R(\alpha) = \sum_{k=0}^{m-1} \mu_k \alpha^k,$$

ce qui démontre que tout élément de $\mathbb{Q}[\alpha]$ est une combinaison linéaire des éléments de la famille $\left(\alpha^k\right)_{k\in[\![0,m-1]\!]}$, donc elle engendre $\mathbb{Q}[\alpha]$.

Étant une famille libre et génératrice de $\mathbb{Q}[\alpha]$, la famille $\left(\alpha^k\right)_{k\in[\![0,m-1]\!]}$ en est une base. On en déduit :

$$\dim(\mathbb{Q}[\alpha]) = \operatorname{card}\left(\left(\alpha^k\right)_{k\in[\![0,m-1]\!]}\right) = m = \deg(\pi_\alpha),$$

d'où le résultat.

(b) Il s'agit de démontrer que pour tout $z \in \mathbb{Q}[\alpha]$, on a $xz \in \mathbb{Q}[\alpha]$: c'est une évidence, puisque pour tous polynômes P et Q dans $\mathbb{Q}[X]$, on a $P(\alpha)Q(\alpha) = (P \cdot Q)(\alpha)$. La $\mathbb{Q}$-linéarité de la multiplication par x provient de la distributivité de la multiplication par rapport à l'addition. Ainsi l'application $z \mapsto zx$ est un endomorphisme de $\mathbb{Q}[\alpha]$, clairement injectif puisque $\mathbb{Q}[\alpha]$ est intègre en tant que sous-anneau de $\mathbb{C}$: l'égalité $zx = 0$ implique $z = 0$ car $x \neq 0$. Or, en dimension finie, un endomorphisme est injectif si et seulement s'il est surjectif (si et seulement s'il est inversible). Comme $1 \in \mathbb{Q}[\alpha]$, on en déduit qu'il existe $z \in \mathbb{Q}[\alpha]$ tel que : $zx = 1$. Ainsi x est inversible dans $\mathbb{Q}[\alpha]$.

(c) L'inclusion $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}(\alpha)$ est évidente. Pour l'inclusion réciproque, soit $z \in \mathbb{Q}(\alpha)$; il s'écrit $z = \frac{P(\alpha)}{R(\alpha)}$ où $R(\alpha) \neq 0$. Or $R(\alpha)$ est inversible dans $\mathbb{Q}[\alpha]$ d'après la question précédente : il existe donc $Q \in \mathbb{Q}[X]$ tel que $R(\alpha)Q(\alpha) = 1$, et on a par conséquent :

$$z = \frac{P(\alpha)}{R(\alpha)} = P(\alpha)Q(\alpha) \in \mathbb{Q}[\alpha].$$

Ceci démontre que $z \in \mathbb{Q}[\alpha]$; donc $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}[\alpha]$, et on a bien l'égalité ensembliste voulue.

20. (a) Il est clair que $P_p(X)$ est irréductible dans $\mathbb{Q}[X]$ si et seulement si $P_p(X+1)$ est irréductible dans $\mathbb{Q}[X]$: si l'un des deux polynômes admet une décomposition en facteurs non triviaux, alors l'autre polynôme aussi quitte à composer ces facteurs avec $X+1$ ou $X-1$.
Or :
$$P_p(X+1) = \frac{(X+1)^p - 1}{(X+1)-1} = \frac{\sum_{k=0}^{p} \binom{p}{k} X^k - 1}{X} = \frac{\sum_{k=1}^{p} \binom{p}{k} X^k}{X} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1},$$
c'est-à-dire :
$$P_p(X+1) = p + \sum_{k=2}^{p-1} \binom{p}{k} X^\ell + X^{p-1}.$$
Pour pouvoir utiliser le résultat admis dans l'énoncé, nous devons vérifier que pour tout $k \in [\![1, p-1]\!]$, le coefficient binomial $\binom{p}{k}$ est un multiple de p (ce résultat classique n'est valable que si p est premier). Pour cela, soit $k \in [\![1, p-1]\!]$; on écrit :
$$\binom{p}{k} k! = \frac{p!}{(p-k)!} = p \prod_{i=1}^{k-1} (p-i)$$
(nous multiplions par $k!$ pour n'avoir que des entiers dans cette égalité, et nous pouvons alors faire de l'arithmétique dans $\mathbb{Z}$). On en déduit que p divise $\binom{p}{k} k!$; mais p est premier à $k!$ puisqu'il s'agit d'un produit d'entiers tous strictement inférieurs à p, et qui ne peuvent donc admettre p comme diviseur premier. On en déduit, par le lemme d'Euclide (ou le théorème de Gauß), que p divise $\binom{p}{k}$: c'est ce qu'on voulait démontrer.

Reprenons notre réflexion : p divise tous les coefficients de $P_p(X+1)$, sauf le coefficient dominant, et p^2 ne divise pas le coefficient constant. Donc, d'après le résultat admis dans l'énoncé, $P_p(X+1)$ est irréductible dans $\mathbb{Q}[X]$ et donc P_p l'est également.

Remarque. Le résultat admis dans l'énoncé s'appelle *critère d'Eisenstein.*

(b) Tout d'abord, vérifions que P_p annule bien ξ_p :
$$P_p(\xi_p) = \sum_{k=0}^{p-1} \xi_p^k = \frac{\xi_p^p - 1}{\xi_p - 1} = 0. \tag{28}$$
Ensuite, du fait que P_p soit irréductible dans $\mathbb{Q}[X]$, le polynôme P_p est le polynôme minimal de ξ_p : en effet, il est bien unitaire, et si l'on fait la division euclidienne de P_p par π_{ξ_p} on obtient l'existence de $(Q, R) \in (\mathbb{Q}[X])^2$ tel que :
$$P_p = \pi_{\xi_p} Q + R,$$
et $\deg(R) < \deg(\pi_{\xi_p})$. En évaluant cette égalité en ξ_p, on obtient $R(\xi_p) = 0$, ce qui n'est possible que si $R = 0$ (sinon on contredit la minimalité de π_{ξ_p}). Alors : $P_p = \pi_{\xi_p} Q$, mais

comme P_p est irréductible et π_{ξ_p} non constant (sinon il n'annulerait pas ξ_p, à moindre d'être nul, mais il ne serait pas unitaire dans ce cas), cela impose que le polynôme Q est constant. Du fait que P_p et π_{ξ_p} soient unitaires, on a même $Q = 1$, donc $P_p = \pi_{\xi_p}$: d'où le résultat voulu.

Pour le dernier résultat demandé : soit $c \in [\![1, p-1]\!]$. Alors $\xi_p^c \neq 1$ parce que ξ_p est une racine primitive p-ième de l'unité, et par le même argument que dans l'égalité (28) :

$$P_p(\xi_p^c) = \sum_{k=0}^{p-1} \left(\xi_p^c\right)^k = \frac{\xi_p^{cp} - 1}{\xi_p^c - 1} = 0.$$

(c) Pour l'existence de l'application $\Phi_c : \mathbb{Q}[\xi_p] \to \mathbb{Q}[\xi_p]$ de l'énoncé, vérifiant :

$$\forall P \in \mathbb{Q}[X], \quad \Phi_c(P(\xi_p)) = P(\xi_p^c),$$

la subtilité est de vérifier qu'elle est bien définie : si un nombre $z \in \mathbb{Q}[\xi_p]$ s'écrit de deux façons différentes comme un polynôme en ξ_p, est-ce que l'image par Φ_c de z dépend du polynôme retenu ?

Pour cela, on note que si z s'écrit : $z = P(\xi_p)$ et $z = Q(\xi_p)$, où P et Q sont deux polynômes à coefficients rationnels, alors leur différence $P-Q$ annule ξ_p, donc est un multiple du polynôme minimal P_p (on le voit une fois de plus en faisant la division euclidienne de $P - Q$ par P_p, et en remarquant que le reste dans cette division euclidienne doit être nul, sinon il serait un polynôme annulateur de ξ_p contredisant la minimalité de P_p). Or $P_p(\xi_p^c) = 0$ d'après la question précédente, donc $P(\xi_p^c) - Q(\xi_p^c) = 0$, puis : $P(\xi_p^c) = Q(\xi_p^c)$. Ainsi la valeur de $\Phi_c(z)$ ne dépend pas du polynôme choisi représentant z.

Vérifier qu'il s'agit d'un morphisme de corps de $\mathbb{Q}[\xi_p]$ découle du fait que pour tous polynômes P et Q à coefficients rationnels, on ait :

$$P(\xi_p^c)Q(\xi_p^c) = (PQ)(\xi_p^c), \text{ et : } P(\xi_p^c) + Q(\xi_p^c) = (P+Q)(\xi_p^c).$$

Il est donc injectif comme tout morphisme de corps non nul, et c'est aussi une application $\mathbb{Q}$-linéaire sur $\mathbb{Q}[\xi_p]$ comme on le vérifie aisément (il faut s'assurer qu'il laisse invariants les nombres rationnels). Or $\mathbb{Q}[\xi_p]$ est de dimension finie (égale à $p-1$) d'après la question 19.(a), et un endomorphisme défini sur un espace vectoriel de dimension finie est injectif si et seulement s'il est bijectif, donc Φ_c est bijectif. C'est donc un automorphisme de corps.

(d) Si $R \in \mathbb{Q}[X]$ vérifie $R(\xi_p) \neq 0$, alors P_p ne divise pas R ; or P_p est irréductible, donc cela signifie que P_p et R sont premiers entre eux. Il existe donc une relation de Bézout entre ces deux polynômes : il existe $(U, V) \in (\mathbb{Q}[X])^2$ tel que : $UP_p + RV = 1$. Or $P_p(\xi_p) = P_p(\xi_p^c) = 0$; en évaluant cette égalité en ξ_p et ξ_p^c, on obtient donc :

$$\frac{1}{R(\xi_p)} = V(\xi_p), \text{ et } \frac{1}{R(\xi_p^c)} = V(\xi_p^c).$$

De cela, et de la question précédente, il découle immédiatement l'identité attendue.

21. (a) En utilisant la relation (18), on a :

$$i^k x_k(r;p) = \frac{i^k}{p^k} \sum_{\substack{(m_1,\dots,m_k)\in[\![1,p-1]\!]^k \\ m_1\cdots m_r \equiv r \bmod p}} i^k \prod_{i=1}^{k} \frac{\xi_p^{m_i}+1}{\xi_p^{m_i}-1} = \frac{(-1)^k}{p^k} \sum_{\substack{(m_1,\dots,m_k)\in[\![1,p-1]\!]^k \\ m_1\cdots m_r \equiv r \bmod p}} \prod_{i=1}^{k} \frac{\xi_p^{m_i}+1}{\xi_p^{m_i}-1}, \quad (29)$$

donc $i^k x_k(r;p)$ est une somme de fractions rationnelles en ξ_p ; un corps est stable par somme, donc $i^k x_k(r;p) \in \mathbb{Q}(\xi_p)$.

(b) En reprenant la propriété de Φ_c démontrée dans la question 20.(d), et l'égalité de la question précédente, on a :

$$\Phi_c(i^k x_k(r;p)) = \frac{(-1)^k}{p^k} \sum_{\substack{(m_1,\dots,m_k)\in[\![1,p-1]\!]^k \\ m_1\cdots m_r \equiv r \bmod p}} \prod_{i=1}^{k} \frac{\xi_p^{cm_i}+1}{\xi_p^{cm_i}-1}.$$

Or c est premier à p, donc inversible modulo p. On en déduit que l'application définie sur :

$$\left\{(m_1,\dots,m_k) \in [\![1,p-1]\!]^k \mid \prod_{i=1}^{k} m_i \equiv r \bmod p\right\}$$

et à valeurs dans :

$$\left\{(m_1,\dots,m_k) \in [\![1,p-1]\!]^k \mid \prod_{i=1}^{k} m_i \equiv c^k r \bmod p\right\},$$

définie par : $(m_1,\dots,m_k) \mapsto (cm_1,\dots,cm_k)$, est une bijection, de réciproque : $(m_1,\dots,m_k) \mapsto (c^{-1}m_1,\dots,c^{-1}m_k)$. On a donc le résultat voulu :

$$\Phi_c(i^k x_k(r;p)) = \frac{(-1)^k}{p^k} \sum_{\substack{(m_1,\dots,m_k)\in[\![1,p-1]\!]^k \\ m_1\cdots m_r \equiv c^k r \bmod p}} \prod_{i=1}^{k} \frac{\xi_p^{m_i}+1}{\xi_p^{m_i}-1} \overset{(29)}{=} i^k x_k(c^k r;p).$$

22. (a) Si $D_k(1,f) = 0$, alors la deuxième relation de la question 16 implique :

$$0 = 2\left(\frac{\pi}{2}\right)^k \sum_{r=1}^{\frac{p-1}{2}} f(r) x_k(r;p).$$

Mais nous avions démontré dans cette même question, avec un caractère impair au lieu d'une fonction f impaire (mais le raisonnement reste le même), qu'en vérité :

$$2\sum_{r=1}^{\frac{p-1}{2}} f(r) x_k(r;p) = \sum_{r=1}^{p-1} f(r) x_k(r;p).$$

En utilisant le fait que les puissances d'un générateur de G parcourent $G = (\mathbb{Z}/p\mathbb{Z})^\times$, on en déduit :

$$\sum_{j=0}^{p-2} f(a^j) x_k(a^j; p) = 0.$$

À présent, soit $\ell \in \mathbb{Z}$, et soit $k' \in \mathbb{Z}$ un entier tel que $kk' \equiv 1 \bmod p-1$; il en existe car k est premier à $p-1$. On pose alors : $c = a^{k'\ell} \in G$.
Multiplions l'égalité ci-dessus par i^k, et considérons l'image par Φ_c de ses deux membres. En sa dignité de morphisme de corps, il vérifie $\Phi_c(0) = 0$, et aussi :

$$\Phi_c\left(i^k \sum_{j=0}^{p-2} f(a^j) x_k(a^j; p)\right) = \sum_{j=0}^{p-2} \Phi_c(f(a^j)) \Phi_c(i^k x_k(a^j; p)).$$

Or Φ_c laisse invariant les nombres rationnels (conséquence classique du fait qu'il soit un morphisme de corps, ou de la relation de la question 20.(c)), et f est supposée à valeurs rationnelles, donc $\Phi_c(f(a^j)) = f(a^j)$ pour tout $j \in [\![0, p-2]\!]$. D'après la question précédente, on a :

$$\forall j \in [\![0, p-2]\!], \quad \Phi_c(i^k x_k(a^j; p)) = i^k x_k(c^k a^j; p) = i^k x_k(a^{kk'\ell} a^j; p).$$

On a $kk'\ell \equiv \ell \bmod p-1$, et comme $a^{p-1} = 1$ on en déduit : $a^{kk'\ell} = a^\ell$. Par conséquent :

$$\Phi_c\left(i^k \sum_{j=0}^{p-2} f(a^j) x_k(a^j; p)\right) = \sum_{j=0}^{p-2} f(a^j) i^k x_k(a^{kk'\ell} a^j; p) = \sum_{j=0}^{p-2} f(a^j) x_k(a^{\ell+j}; p).$$

En recoupant tout ce que nous avons établi, on a donc :

$$\forall \ell \in \mathbb{Z}, \quad \sum_{j=0}^{p-2} f(a^j) x_k(a^{\ell+j}; p) = 0. \tag{30}$$

Pour réduire le nombre de termes de la somme, notons que f et $r \mapsto x_k(r; p)$ étant des fonctions impaires, leur produit est une fonction paire, et donc :

$$\forall \ell \in \mathbb{Z},\ \forall j \in \left[\!\left[0, \frac{p-3}{2}\right]\!\right], \quad f\left(-a^j\right) x_k(-a^{\ell+j}; p) = f\left(a^j\right) x_k(a^{\ell+j}; p).$$

En utilisant le fait que $a^{\frac{p-1}{2}} = -1$ (exercice facile) on en déduit :

$$\forall \ell \in \mathbb{Z},\ \forall j \in \left[\!\left[0, \frac{p-3}{2}\right]\!\right], \quad f\left(a^{j+\frac{p-1}{2}}\right) x_k(a^{\ell+j+\frac{p-1}{2}}; p) = f\left(a^j\right) x_k(a^{\ell+j}; p).$$

Or, quand j parcourt $[\![0, \frac{p-3}{2}]\!]$, $j + \frac{p-1}{2}$ parcourt $[\![\frac{p-1}{2}, p-2]\!]$. Ainsi :

$$\forall \ell \in \mathbb{Z}, \quad 2\sum_{j=0}^{\frac{p-3}{2}} f\left(a^j\right) x_k(a^{\ell+j}; p) = \sum_{j=0}^{p-2} f\left(a^j\right) x_k(a^{\ell+j}; p) \overset{(30)}{=} 0,$$

d'où le résultat voulu.

(b) On reprend la relation de la question précédente. Pour tout $\ell \in \left[\!\left[0, \frac{p-3}{2}\right]\!\right]$, on a :

$$\sum_{j=0}^{\frac{p-3}{2}} f\left(a^j\right) x_k(a^{\ell+j};p) = \sum_{\substack{j=0 \\ j+\ell<\frac{p-1}{2}}}^{\frac{p-3}{2}} f\left(a^j\right) x_k(a^{\ell+j};p) + \sum_{\substack{j=0 \\ j+\ell\geqslant\frac{p-1}{2}}}^{\frac{p-3}{2}} f\left(a^j\right) x_k(a^{\ell+j};p) = 0. \tag{31}$$

Si $\ell = 0$, la deuxième somme est vide. Pour tout $\ell \in \left[\!\left[1, \frac{p-3}{2}\right]\!\right]$, en utilisant la parité de $r \mapsto x_k(r;p)$, ainsi que les égalités $a^{p-1} = 1$ et $a^{\frac{p-1}{2}} = -1$, on a :

$$\begin{aligned}\sum_{\substack{j=0 \\ j+\ell\geqslant\frac{p-1}{2}}}^{\frac{p-3}{2}} f\left(a^j\right) x_k(a^{\ell+j};p) &= \sum_{\substack{j=0 \\ j+\ell\geqslant\frac{p-1}{2}}}^{\frac{p-3}{2}} f\left(a^j\right) x_k(a^{\ell+j-\frac{p-1}{2}-\frac{p-1}{2}};p) \\ &= -\sum_{\substack{j=0 \\ j+\ell\geqslant\frac{p-1}{2}}}^{\frac{p-3}{2}} f\left(a^j\right) x_k(a^{\ell+j-\frac{p-1}{2}};p),\end{aligned} \tag{32}$$

et pour tout $(j,l) \in \left[\!\left[0, \frac{p-3}{2}\right]\!\right]^2$ tel que $j+\ell \geqslant \frac{p-1}{2}$, on a $\ell + j - \frac{p-1}{2} < \frac{p-1}{2} - 1$.
Posons $m = \frac{p-1}{2}$. Si, pour tout $n \in \mathbb{Z}$, on note *très abusivement* $n \bmod m$ le représentant entre 0 et $m-1$ de n modulo m, et si l'on pose également :

$$\forall (i,j) \in [\![0, m-1]\!], \quad \varepsilon_{i,j} = \begin{cases} 1 & \text{si } i+j \leqslant m-1, \\ -1 & \text{sinon,} \end{cases}$$

alors les relations (31) et (32) se réinterprètent ainsi :

$$\forall \ell \in [\![0, m-1]\!], \quad \sum_{j=0}^{\frac{p-3}{2}} \varepsilon_{\ell,j} f\left(a^j\right) x_k\left(a^{\ell+j \bmod m};p\right) = 0. \tag{33}$$

Si, conformément à l'énoncé, on pose pour tout $\mathbf{v} = (v_0, \ldots, v_{m-1}) \in \mathbb{C}^m$:

$$A_m(\mathbf{v}) = \begin{pmatrix} v_0 & v_1 & \cdots & v_{m-2} & v_{m-1} \\ v_1 & v_2 & \cdots & v_{m-1} & -v_0 \\ \vdots & \vdots & & \vdots & \vdots \\ v_{m-1} & -v_0 & -v_1 & \cdots & -v_{m-2} \end{pmatrix} = \left(\left(\varepsilon_{i,j} v_{i+j \bmod m}\right)\right)_{0\leqslant i,j\leqslant m-1},$$

alors (33) s'écrit matriciellement :

$$A_m(\mathbf{x}) \cdot \mathbf{y} = 0,$$

où $\mathbf{x} = \left(x_k(1;p), x_k(a;p), \ldots, x_k\left(a^{\frac{p-3}{2}};p\right)\right)$ et ${}^t\mathbf{y} = \left(f(1), f(a), \ldots, f\left(a^{\frac{p-3}{2}}\right)\right)$: ce qu'on voulait démontrer.

23. (a) Si $\mathbf{v} = \mathbf{e}_1$, alors la matrice $A_m(\mathbf{v})$ est simplement :

$$A_m(\mathbf{e}_1) = \begin{pmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & -1 \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & -1 & 0 & \cdots & 0 \end{pmatrix}$$

On a donc :

$$\det(A_m(\mathbf{e}_1)) = (-1)^{m-1} \begin{vmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ \vdots & & \ddots & \ddots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 1 & 0 & \cdots & 0 \end{vmatrix}$$

Quitte à réordonner les $m-1$ dernières colonnes, on peut faire apparaître le déterminant de la matrice identité. Nous devons pour cela transposer la m colonne et la deuxième, puis la $(m-1)$-ième et la troisième, etc. On compte $\frac{m-1}{2}$ inversions si m est impair, $\frac{m-2}{2}$ si m est pair. On en déduit :

$$\det(A_m(\mathbf{e}_1)) = \begin{cases} (-1)^{m-1} \times (-1)^{\frac{m}{2}-1} = (-1)^{\frac{m}{2}} & \text{si } m \equiv 0 \bmod 2, \\ (-1)^{m-1} \times (-1)^{\frac{m-1}{2}} = (-1)^{\frac{m-1}{2}} & \text{si } m \equiv 1 \bmod 2. \end{cases} \tag{34}$$

Or, toujours dans ce cas :

$$\left(\cos\left(\frac{\pi m}{2}\right) + \sin\left(\frac{\pi m}{2}\right)\right) \prod_{\substack{\ell=0 \\ \ell \text{ impair}}}^{2m} \left(\sum_{j=0}^{m-1} v_j \xi_{2m}^{j\ell}\right) = \cos\left(\frac{\pi m}{2}\right) + \sin\left(\frac{\pi m}{2}\right) = \sqrt{2}\cos\left(\frac{\pi(2m-1)}{4}\right),$$

et on sait, grâce à la périodicité du cosinus et à ses valeurs remarquables, que pour tout $k \in \mathbb{Z}$ impair (l'élève consciencieux passera éventuellement par un raisonnement par récurrence),

$$\sqrt{2}\cos\left(\frac{k\pi}{4}\right) = \begin{cases} (-1)^{\frac{k-1}{4}} & \text{si } k \equiv 1 \bmod 4, \\ (-1)^{\frac{k+1}{4}} & \text{si } k \equiv -1 \bmod 4, \end{cases}$$

donc :

$$\sqrt{2}\cos\left(\frac{\pi(2m-1)}{4}\right) = \begin{cases} (-1)^{\frac{m-1}{2}} & \text{si } m \equiv 1 \bmod 2, \\ (-1)^{\frac{m}{2}} & \text{si } m \equiv 0 \bmod 2, \end{cases}$$

En comparant avec (34), on obtient bien le résultat désiré :

$$\det(A_m(\mathbf{e}_1)) = \sqrt{2}\cos\left(\frac{\pi(2m-1)}{4}\right) = \cos\left(\frac{\pi m}{2}\right) + \sin\left(\frac{\pi m}{2}\right),$$

d'où le résultat voulu si $\mathbf{v} = \mathbf{e}_1$.

(b) Il y a un conflit de notation avec la question précédente : $\mathbf{e}_0$ et $\mathbf{e}_1$ désignent le même vecteur. Dans cette question, $\mathbf{e}_1$ reste le vecteur $(1, 0, \dots, 0) \in \mathbb{C}^m$.

C'est un produit matriciel immédiat, mais on attend peut-être une démonstration formelle. Avec les mêmes notations que dans la question 22.(b) :

$$A_m(\mathbf{e}_1) = \left((\varepsilon_{i,j}\delta_{0,i+j \bmod m})\right)_{0\leqslant i,j\leqslant m-1},$$

où la lettre δ désigne le symbole de Kronecker. On espère obtenir :

$$C_m(\mathbf{v}) = \begin{pmatrix} v_0 & -v_{m-1} & \cdots & -v_2 & -v_1 \\ v_1 & v_0 & \cdots & -v_3 & -v_2 \\ \vdots & \vdots & & \vdots & \vdots \\ v_{m-1} & v_{m-2} & \cdots & v_1 & v_0 \end{pmatrix} = \left((\epsilon_{i,j}v_{i-j \bmod m})\right)_{0\leqslant i,j\leqslant m-1}$$

où $\epsilon_{i,j} = 1$ si $i \geqslant j$ et $\epsilon_{i,j} = -1$ sinon.
Or, pour tout $(i,j) \in [\![0, m-1]\!]^2$, le coefficient (i,j) du produit matriciel $A_m(\mathbf{v})A_m(\mathbf{e}_1)$ est :

$$\sum_{t=0}^{m-1} \varepsilon_{i,t}\varepsilon_{t,j}v_{i+t \bmod m}\delta_{0,t+j \bmod m} = \begin{cases} \varepsilon_{i,m-j}\varepsilon_{m-j,j}v_{i-j \bmod m} & \text{si } j \geqslant 1, \\ \varepsilon_{i,0}\varepsilon_{0,0}v_{i \bmod m} & \text{si } j = 0, \end{cases}$$

puisque l'unique entier $t \in [\![0, m-1]\!]$ tel que $t + j \equiv 0 \bmod m$ est $t = m - j$ si $j \geqslant 1$, et $t = 0$ si $j = 0$.
Soit $i \in [\![0, m-1]\!]$. Distinguons deux cas :

— si $j = 0$, alors $\varepsilon_{i,0}\varepsilon_{0,0} = 1$, donc on a bien $\varepsilon_{i,0}\varepsilon_{0,0} = \epsilon_{i,0}$;

— si $j \geqslant 1$, alors $\varepsilon_{i,m-j}\varepsilon_{m-j,j} = 1$ si l'on a simultanément $i+m-j \leqslant m-1$ et $j+m-j \leqslant m-1$ (ce qui est impossible), ou simultanément $i + m - j > m - 1$ et $j + m - j > m - 1$ (la deuxième inégalité est superflue car toujours vraie), c'est-à-dire si l'on a $j - i < 1$, ou encore : $j \leqslant i$; inversement, $\varepsilon_{i,m-j}\varepsilon_{m-j,j} = -1$ si $j > i$; on a donc : $\varepsilon_{i,m-j}\varepsilon_{m-j,j} = \epsilon_{i,j}$.

On a donc, pour tout $(i,j) \in [\![0, m-1]\!]$,

$$\sum_{t=0}^{m-1} \varepsilon_{i,t}\varepsilon_{t,j}v_{i+t \bmod m}\delta_{0,t+j \bmod m} = \epsilon_{i,j}v_{i-j \bmod m},$$

c'est-à-dire : $A_m(\mathbf{v})A_m(\mathbf{e}_1) = C_m(\mathbf{v})$.

(c) Soit $\ell \in [\![1, 2m]\!]$ un entier impair. Pour tout $i \in [\![0, m-1]\!]$, comparons le i-ième coefficient des vecteurs $C_m(\mathbf{v})c_\ell$ et c_ℓ ; il s'agit respectivement, avec les notations de la résolution de la question 23.(b), de :

$$\sum_{t=0}^{m-1} \epsilon_{i,t}v_{i-t \bmod m}\xi_{2m}^{(m-t)\ell}, \quad \text{et :} \quad \xi_{2m}^{(m-i)\ell}.$$

Pour $i = m-1$, faisons le changement d'indice de sommation $t \mapsto m-1-t$; on a alors :

$$\sum_{t=0}^{m-1} \epsilon_{i,t} v_{i-t \bmod m} \xi_{2m}^{(m-t)\ell} = \sum_{t=0}^{m-1} v_{m-1-t} \xi_{2m}^{(m-t)\ell} = \sum_{t=0}^{m-1} v_t \xi_{2m}^{(t+1)\ell} = \left(\sum_{t=0}^{m-1} v_t \xi_{2m}^{t\ell} \right) \xi_{2m}^{\ell},$$

et cette égalité suggère que si c_ℓ est bien un vecteur propre de $C_m(\mathbf{v})$, alors la valeur propre associée est $\sum_{t=0}^{m-1} v_t \xi_{2m}^{t\ell}$. Pour nous en convaincre, notons que pour tout $i \in [\![0, m-2]\!]$ on a :

$$\sum_{t=0}^{m-1} \epsilon_{i,t} v_{i-t} \xi_{2m}^{(m-t)\ell} = \sum_{t=0}^{i} v_{i-t \bmod m} \xi_{2m}^{(m-t)\ell} - \sum_{t=i+1}^{m-1} v_{m+i-t} \xi_{2m}^{(m-t)\ell},$$

et nous nous affranchissons du signe moins en constatant que $\xi_{2m}^{m} = -1$ (vérification facile) et donc $\xi_{2m}^{\ell m} = (-1)^\ell = -1$ parce que ℓ est impair, de sorte que pour tout $i \in [\![0, m-2]\!]$:

$$\begin{aligned}
\sum_{t=0}^{m-1} \epsilon_{i,t} v_{i-t \bmod m} \xi_{2m}^{(m-t)\ell} &= \sum_{t=0}^{i} v_{i-t} \xi_{2m}^{(m-t)\ell} + \sum_{t=i+1}^{m-1} v_{m+i-t} \xi_{2m}^{(2m-t)\ell} \\
&= \sum_{t=0}^{i} v_t \xi_{2m}^{(m-(i-t))\ell} + \sum_{t=i+1}^{m-1} v_t \xi_{2m}^{(2m-(m+i-t))\ell} \\
&= \left(\sum_{t=0}^{i} v_t \xi_{2m}^{t\ell} \right) \xi_{2m}^{(m-i)\ell} + \left(\sum_{t=i+1}^{m-1} v_t \xi_{2m}^{t\ell} \right) \xi_{2m}^{(m-i)\ell} \\
&= \left(\sum_{t=0}^{m-1} v_t \xi_{2m}^{t\ell} \right) \xi_{2m}^{(m-i)\ell},
\end{aligned}$$

et ceci étant vrai pour tout $i \in [\![0, m-1]\!]$ (le cas $i = m-1$ fut traité préalablement), on a :

$$C_m(\mathbf{v}) c_\ell = \left(\sum_{t=0}^{m-1} v_t \xi_{2m}^{t\ell} \right) c_\ell.$$

De plus c_ℓ est évidemment non nul ; ceci démontre donc que c_ℓ est un vecteur propre de $C_m(\mathbf{v})$, associé à la valeur propre $\sum_{t=0}^{m-1} v_t \xi_{2m}^{t\ell}$.

(d) Le déterminant de la famille $(c_\ell)_{\substack{1 \leqslant \ell \leqslant 2m \\ \ell \text{ impair}}}$ relativement à la base canonique est, à un facteur $\pm \prod_{\substack{1 \leqslant \ell \leqslant 2m \\ \ell \text{ impair}}} \xi_{2m}^{\ell} \neq 0$ près, un déterminant de Vandermonde. Pour justifier qu'il est non nul, il suffit de s'assurer qu'il ordonne des puissances de nombres distincts : or ξ_{2m} est une racine primitive $2m$-ième de l'unité, donc les nombres ξ_{2m}^k, pour $k \in [\![1, 2m]\!]$, sont tous distincts. C'est en particulier le cas des nombres ξ_{2m}^ℓ pour ℓ impair parcourant $[\![1, 2m]\!]$. On en déduit que ce déterminant de Vandermonde est non nul, donc la famille $(c_\ell)_{\substack{1 \leqslant \ell \leqslant 2m \\ \ell \text{ impair}}}$ est libre ; de plus,

elle contient m vecteurs, donc c'est une base de $\mathbb{C}^m$, constituée de vecteurs propres de $C_m(\mathbf{v})$. Par conséquent, la matrice $C_m(\mathbf{v})$ est semblable à la matrice diagonale dont les coefficients diagonaux sont les valeurs propres associées aux vecteurs propres de la base $(c_\ell)_{\substack{1\leqslant\ell\leqslant 2m\\ \ell \text{ impair}}}$; c'est-à-dire, d'après la question précédente :

$$\begin{pmatrix} \sum_{j=0}^{m-1} v_j\xi_{2m}^j & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \sum_{j=0}^{m-1} v_j\xi_{2m}^{j(2m-1)} \end{pmatrix}$$

et on a : $\det(C_m(\mathbf{v})) = \prod_{\substack{\ell=1\\ \ell \text{ impair}}}^{2m} \left(\sum_{j=0}^{m-1} v_j\xi_{2m}^{j\ell}\right)$. Alors, de la relation $A_m(\mathbf{v})A_m(\mathbf{e}_1) = C_m(\mathbf{v})$, on déduit :

$$\det(A_m(\mathbf{v}))\det(A_m(\mathbf{e}_1)) = \det(C_m(\mathbf{v})),$$

et il reste à diviser par $\det(A_m(\mathbf{e}_1))$ pour obtenir le déterminant cherché. Nous avons calculé $\det(A_m(\mathbf{e}_1))$ dans la question 23.(a) ; nous avons démontré qu'il égale $\cos\left(\frac{\pi m}{2}\right) + \sin\left(\frac{\pi m}{2}\right)$, et constaté en passant que c'est un nombre égal à 1 ou -1, donc en tous les cas il est égal à son inverse. Alors :

$$\begin{aligned}\det(A_m(\mathbf{v})) = \frac{\det(C_m(\mathbf{v}))}{\det(A_m(\mathbf{e}_1))} &= \det(A_m(\mathbf{e}_1))\det(C_m(\mathbf{v})) \\ &= \left(\cos\left(\frac{\pi m}{2}\right) + \sin\left(\frac{\pi m}{2}\right)\right) \prod_{\substack{\ell=1\\ \ell \text{ impair}}}^{2m} \left(\sum_{j=0}^{m-1} v_j\xi_{2m}^{j\ell}\right),\end{aligned}$$

d'où l'égalité désirée.

24. (a) Pour $\mathbf{x} = \left(x_k(1;p), x_k(a;p), \ldots, x_k\left(a^{\frac{p-3}{2}};p\right)\right) \in \mathbb{C}^{\frac{p-1}{2}}$, la question 23 donne :

$$\det\left(A_{\frac{p-1}{2}}(\mathbf{x})\right) = \left(\cos\left(\frac{\pi(p-1)}{4}\right) + \sin\left(\frac{\pi(p-1)}{4}\right)\right) \prod_{\substack{\ell=1\\ \ell \text{ impair}}}^{p-1} \left(\sum_{j=0}^{\frac{p-3}{2}} x_k(a^j;p)\xi_{p-1}^{j\ell}\right).$$

Dans la question 8.(a), nous avions explicité un isomorphisme entre G et $\hat{G}$, dont l'image d'un générateur a de G est le caractère $\chi_* : a^k \mapsto \xi_{p-1}^k$. Or l'image d'un générateur par un morphisme surjectif est un générateur, donc le caractère $\chi_* : \omega^k \mapsto \xi_{p-1}^k$ engendre $\widehat{G}$ (il ne serait pas coûteux de démontrer qu'on peut prendre n'importe quel générateur de $\hat{G}$ dans cette question, mais nous n'en avons pas besoin pour la suite). De plus :

$$\forall \ell \in \mathbb{Z}, \quad \sum_{j=0}^{\frac{p-3}{2}} x_k(a^j;p)\xi_{p-1}^{j\ell} = \sum_{j=0}^{\frac{p-3}{2}} x_k(a^j;p)(\chi_*(a^j))^\ell.$$

Admettons *provisoirement* que le caractère χ_*^ℓ est impair pour tout entier ℓ impair. Par un raisonnement déjà utilisé dans la question 22.(a) (voir notamment tout ce qui suit l'établissement de la relation (30)), on a même, du fait de la parité et périodicité de x_k et χ_*^ℓ :

$$2\sum_{j=0}^{\frac{p-3}{2}} x_k(a^j;p)(\chi_*(a^j))^\ell = \sum_{j=0}^{p-2} x_k(a^j;p)(\chi_*(a^j))^\ell = \sum_{r=1}^{p-1} x_k(r;p)(\chi_*(r))^\ell.$$

Or, d'après la question 16, on a :

$$\sum_{r=1}^{p-1} x_k(r;p)(\chi_*(r))^\ell = 2\sum_{r=1}^{\frac{p-1}{2}} x_k(r;p)(\chi_*(r))^\ell = \left(\frac{2}{\pi}\right)^k D_k(1,\chi_*^\ell),$$

et d'après la question 10 on a : $D_k(1,\chi_*^\ell) = L(1,\chi_*^\ell)^k$. On en déduit :

$$\sum_{j=0}^{\frac{p-3}{2}} x_k(a^j;p)(\chi_*(a^j))^\ell = \frac{2^{k-1}}{\pi^k} L(1,\chi_*^\ell)^k.$$

En conclusion :

$$\begin{aligned}\det\left(A_{\frac{p-1}{2}}(\mathbf{x})\right) &= \left(\cos\left(\frac{\pi(p-1)}{4}\right) + \sin\left(\frac{\pi(p-1)}{4}\right)\right) \prod_{\substack{\ell=1\\ \ell \text{ impair}}}^{p-1} \left(\frac{2^{k-1}}{\pi^k} L(1,\chi_*^\ell)^k.\right) \\ &= \left(\cos\left(\frac{\pi(p-1)}{4}\right) + \sin\left(\frac{\pi(p-1)}{4}\right)\right) \left(\frac{2^{k-1}}{\pi^k}\right)^{\frac{p-1}{2}} \prod_{\substack{\ell=1\\ \ell \text{ impair}}}^{p-1} L(1,\chi_*^\ell)^k.\end{aligned}$$

Justifions à présent que le caractère χ_*^ℓ est impair pour tout entier ℓ impair (nous en aurons aussi besoin dans la question suivante). Si ce n'était pas le cas, alors on aurait $\chi_*(-1) = 1$ d'après (9), et donc $\chi_*^k(-1) = 1$ pour tout $k \in \mathbb{Z}$: or χ_* engendre $\hat{G}$, donc il n'existerait pas de caractère impair. Mais c'est impossible si $p > 2$, puisque les caractères impairs modulo p engendrent $\mathcal{F}_p^-(\mathbb{Z},\mathbb{C})$, comme nous l'avons montré dans la question 16, et il existe bien des fonctions non nulles p-périodiques et impaires : prendre l'application $f = \mathbf{1}_1 - \mathbf{1}_{p-1}$ (avec les notations de la question 16) par exemple.

Maintenant, soit ℓ un entier impair. Rappelons que d'après la question 6.(b), les caractères impairs sont caractérisés par leur valeur en -1. En effet, un caractère χ modulo p est impair si et seulement si $\chi(-1) = -1$. Or χ_* est impair, et donc $\chi_*(-1) = -1$. Pour tout ℓ impair, on a également : $\chi_*^\ell(-1) = (-1)^\ell = -1$, donc χ_*^ℓ est impair pour tout $\ell \in [\![0, p-1]\!]$ impair.

(b) Supposons que $L(1,\chi) \neq 0$ pour tout caractère χ impair modulo p. D'après la fin de la question précédente, χ_*^ℓ est un caractère impair pour tout entier $\ell \in [\![0, p-1]\!]$ impair, donc

$L(1,\chi_*^\ell) \neq 0$ pour tout $\ell \in [\![0,p-1]\!]$ impair. Or le calcul effectué dans la question 23.(a) montre qu'on a également $\cos\left(\frac{\pi(p-1)}{4}\right) + \sin\left(\frac{\pi(p-1)}{4}\right) \neq 0$. On en déduit :

$$\det\left(A_{\frac{p-1}{2}}(\mathbf{x})\right) = \left(\cos\left(\frac{\pi(p-1)}{4}\right) + \sin\left(\frac{\pi(p-1)}{4}\right)\right) \frac{2^{\frac{(k-1)(p-1)}{2}}}{\pi^{\frac{k(p-1)}{2}}} \prod_{\substack{\ell=0 \\ \ell \text{ impair}}}^{p-1} L(1,\chi_*^\ell)^k \neq 0.$$

Autrement dit, la matrice $A_{\frac{p-1}{2}}(\mathbf{x})$ est inversible.

À présent, soit $f \in \mathcal{F}_p^-(\mathbb{Z},\mathbb{Q})$ telle que $D_k(1,f) = 0$. D'après la question 22.(b), si l'on pose :

$$\mathbf{y} = \begin{pmatrix} f(1) \\ f(a) \\ \vdots \\ f\left(a^{\frac{p-3}{2}}\right) \end{pmatrix} \in \mathbb{C}^{\frac{p-1}{2}},$$

alors : $A_{\frac{p-1}{2}}(\mathbf{x}) \cdot \mathbf{y} = 0$. L'inversibilité de la matrice $A_{\frac{p-1}{2}}(\mathbf{x})$ implique $\mathbf{y} = 0$, c'est-à-dire :

$$\forall k \in \left[\!\left[0, \frac{p-3}{2}\right]\!\right], \quad f\left(a^k\right) = 0.$$

Suivant le même raisonnement qu'en fin de question 22.(a), en utilisant la parité de f et l'égalité $a^{\frac{p-1}{2}} = -1$ on obtient $f(a^k) = 0$ pour tout $k \in [\![0,p-2]\!]$, et comme a est un générateur de G cela signifie que f est nulle sur $[\![1,p-1]\!]$ (et même sur $[\![0,p-1]\!]$ vu que f est impaire) ; or f est p-périodique, donc on en déduit $f = 0$.

En conclusion, nous avons démontré que si $L(1,\chi) \neq 0$ pour tout caractère impair modulo p, alors toute fonction $f \in \mathcal{F}_p^-(\mathbb{Z},\mathbb{Q})$ telle que $D_k(1,f) = 0$ est la fonction nulle, c'est-à-dire :

$$\{f \in V \mid D_k(1,f) = 0\}$$

est de dimension nulle. D'où le résultat.

25. D'après la question 14.(c) :

$$L(1,\chi) = \frac{\pi i \tau(\chi)}{p} \sum_{a=1}^{p} \bar{\chi}(a) B\left(\frac{a}{p}\right).$$

Comme $|\tau(\chi)| = \sqrt{p}$ d'après la question 14.(b), on a $\tau(\chi) \neq 0$. Nous devons donc démontrer :

$$\sum_{a=1}^{p} \bar{\chi}(a) B\left(\frac{a}{p}\right) \neq 0$$

pour avoir le résultat voulu. Or :

$$\sum_{a=1}^{p-1} \bar{\chi}(a) B\left(\frac{a}{p}\right) = \frac{1}{2p} \sum_{a=1}^{p-1} \bar{\chi}(a)(2a-p).$$

De plus, $\chi = \bar{\chi}$ est à valeurs réelles, et $\bar{\chi}(a) \in \mathbb{U}$ pour tout $a \in [\![1, p-1]\!]$, donc $\bar{\chi}(a) \in \{-1, 1\}$ pour tout $a \in [\![1, p-1]\!]$. On en déduit que $\sum_{a=1}^{p-1} \bar{\chi}(a)(2a-p)$ est un nombre entier, et on a :

$$\sum_{a=1}^{p-1} \bar{\chi}(a)(2a-p) \equiv \sum_{\substack{a=1 \\ a \text{ impair}}}^{p-1} \bar{\chi}(a)(2-p) \bmod 4 \equiv - \sum_{\substack{a=1 \\ a \text{ impair}}}^{p-1} \bar{\chi}(a) \bmod 4.$$

Il y a $\frac{p-1}{2}$ nombres impairs dans $[\![1, p-1]\!]$, donc $\frac{p-1}{2}$ termes dans cette somme. Or par hypothèse $p \equiv 3 \bmod 4$, donc $\frac{p-1}{2} \equiv 1 \bmod 2$. Nous avons donc là une somme d'un nombre impair de 1 et -1 : c'est impossible que cette somme donne zéro modulo 4. On en déduit que $\sum_{a=1}^{p-1} \bar{\chi}(a)(2a-p) \neq 0$, et donc $\sum_{a=1}^{p} \bar{\chi}(a) B\left(\frac{a}{p}\right) \neq 0$.

On peut conclure :

$$L(1, \chi) = \underbrace{\frac{\pi i \tau(\chi)}{p}}_{\neq 0} \underbrace{\left(\sum_{a=1}^{p} \bar{\chi}(a) B\left(\frac{a}{p}\right) \right)}_{\neq 0},$$

donc $L(1, \chi) \neq 0$: d'où le résultat.