Analyse harmonique sur les groupes finis commutatifs

Abdellah Bechata

Table des matières

Résumé

Cet article est consacré à l'étude complète de l'analyse harmonique sur les groupes finis commutatifs (caractères, décomposition de la représentations régulière, dualité de Pontriaguin ainsi que sa spécialisation au cas des espaces vectoriels)

En des termes moins barbares, il s'agit simplement de l'analyse de Fourier sur les groupes finis commutatifs qui peut être aborder dans toute sa généralité par un étudiant en spé MP ou MP*. L'analyse de Fourier lorsque le groupe G est un groupe de congruence $\mathbb{Z}/n\mathbb{Z}$ ou un produit de tels groupes, est tout simplement la fameuse transformée de Fourier rapide (TFR).On retrouvera également les fameuses sommes de Gauss. et certaines de leurs propriétés comme découlant des facteurs Gamma

1 Notations :

Soit $(G,+)$ un groupe fini commutatif dont le cardinal est noté $|G|$.
Si $(S^1,\times)$ désigne le groupe multiplicatif des nombres complexe de module 1, on appelle caractère unitaire de G tout morphisme de $(G,+)$ dans $(S^1,\times)$.
Le dual unitaire de G, que l'on note $\widehat{G}$, est l'ensemble des caractères unitaires de G : il s'agit d'un groupe commutatif pour la multiplication des applications c'est-à-dire que

$$(\chi_1\chi_2)(g)=\chi_1(g)\chi_2(g) \quad \forall \chi_1,\chi_2\in\widehat{G} \text{ et } \forall g\in G \tag{1}$$

L'ensemble des applications de G dans $\mathbb{C}$ est noté $L^2(G)$. Bien entendu, l'ensemble des applications de $\widehat{G}$ dans $\mathbb{C}$ est noté $L^2(\widehat{G})$.

Définition 1 (représentation régulière de G)
On appelle représentation régulière de G l'application de G dans $GL(L^2(G))$ définie par

$$R:\left\{\begin{array}{c} G\to GL(L^2(G)) \\ g\mapsto R(g)\end{array}\right. \quad \text{avec } \forall u\in L^2(G) \text{ et } \forall h\in G,\ \ [R(g)u](h)=u(h+g)$$

[0] site web : http ://abdellah.bechata.free.fr

Pour g fixé, l'opérateur $R(g)$ est simplement un opérateur de translation par g. Il est immédiat que pour tout g appartenant à G, $R(g)$ est un automorphisme de $L^2(G)$. Un calcul élémentaire montre que

$$R(g)R(g') = R(g+g') \ \forall g, g' \in G \text{ et } R(0) = Id_{L^2(G)}$$

ce qui implique que R est un morphime de $(G,+)$ dans $GL(L^2(G))$.
Munissons l'espace $L^2(G)$ du produit scalaire hermitien

$$< u, v >_{L^2(G)} = \frac{1}{|G|} \sum_{g \in G} u(g)\overline{v(g)}$$

et l'espace $L^2(\widehat{G})$ du produit scalaire hermitien

$$< \varphi, \psi >_{L^2(\widehat{G})} = \frac{1}{\left|\widehat{G}\right|} \sum_{\chi \in \widehat{G}} \varphi(\chi)\overline{\psi(\chi)}.$$

Lemme 1
Les opérateurs $R(g)$ sont des endomorphismes unitaires de $(L^2(G), <,>_{L^2(G)})$.

Preuve :
Soient u, v deux éléments de $L^2(G)$ et

$$h \in G. < R(h)u, R(h)v >_{L^2(G)} = \frac{1}{|G|} \sum_{g \in G} [R(h)u](g)\overline{[R(h)v](g)} = \frac{1}{|G|} \sum_{g \in G} u(g+h)\overline{v(g+h)}$$

L'application $g \to g+h$ est une bijection de G sur G donc si l'on effectue le changement de variable $g \leftarrow g+h$, on obtient

$$< R(h)u, R(h)v >_{L^2(G)} = \frac{1}{|G|} \sum_{g \in G} u(g)\overline{v(g)} =< u, v >_{L^2(G)}$$

■

2 Etude des opérateurs $R(g)$.

Lemme 2 (critère de codiagonalisation)
Soit E un espace hermitien de dimension finie et $u_1, .., u_n$ des endomorphismes unitaires de E.
Alors il existe une base orthonormale $\mathcal{B}$ de E qui diagonalise tous les u_i si et seulement si les u_i commutent deux à deux c'est-à-dire

$$u_i \circ u_j = u_j \circ u_i \ \forall i, j \in \{1, .., n\}.$$

Preuve :

1. Supposons qu'il existe une base $\mathcal{B} = (e_1, .., e_{\dim E})$ de E qui diagonalise tous les u_i.
   Il existe donxc une famille $\lambda_{i,j}$ d'éléments de $\mathbb{C}$ telle que

   $$u_i(e_k) = \lambda_{i,k} e_k \ \forall i \in \{1, .., n\}, \forall k \in \{1, .., \dim E\}$$

   d'où $\forall i, j \in \{1, .., n\}$ et $\forall k \in \{1, .., \dim E\}$

   $$(u_i \circ u_j)(e_k) = u_i(u_j(e_k)) = \lambda_{j,k} u_i(e_k) = \lambda_{i,k}\lambda_{j,k} e_k = (u_j \circ u_i)(e_k).$$

   Les endomorphismes $u_i \circ u_j$ et $u_j \circ u_i$ sont égaux sur la base $\mathcal{B}$ donc ils sont égaux.

2. Supposons que les u_i commutent deux à deux.
   On procède par récurrence sur n.
   Posons $(\mathcal{H}_n)$: n endomorphismes unitaires de E qui commutent deux à deux alors il existe une base qui les diagonalise simultanément.
   L'hypothèse $(\mathcal{H}_1)$ est vraie car un opérateur unitaire est diagonalisable en base orthonormale.
   Suppposons que $(\mathcal{H}_n)$ soit vraie et soient $u_1, .., u_{n+1}$ des endomorphismes unitaires de E qui commutent deux à deux. Par conséquent, pour tout $i \in \{1, .., n\}$, on a $u_{n+1} \circ u_i = u_i \circ u_{n+1}$. On en déduit que chaque espace propre $E_\lambda(u_{n+1})$ de u_{n+1} est stable par tous les u_i. Posons $v_i = u_{i|_{E_\lambda(u_{n+1})}}$: c'est un endomorphisme unitaire de $E_\lambda(u_{n+1})$ et
   $$v_i \circ v_j = v_j \circ v_i \ \forall i, j \in \{1, .., n\}.$$
   On applique l'hypothèse de récurrence à la famille $(v_i)_i$. Donc il existe une base orthonormale $\mathcal{B}_\lambda$ qui diagonalise tous les v_i. L'endomorphisme u_{n+1} est diagonalisable en base orthonormale et $E = \overset{\perp}{\bigoplus_{\lambda \in sp(u_{n+1})}} E_\lambda(u_{n+1})$.
   si l'on concaténe toutes les bases $\mathcal{B}_\lambda$ obtenues précédemment, on obtient une base orthonormale $\mathcal{B} = (\mathcal{B}_\lambda)_{\lambda \in sp(u_{n+1})}$ de E. Par construction, chaque élément de $\mathcal{B}$ est un vecteur propre de tous les $(u_i)_{i \in \{1,..,n\}}$ et il appartient à un certain $E_\lambda(u_{n+1})$ donc il s'agit également d'un vecteur propre de u_{n+1}

■

On remarquera que ce lemme se généralise sans aucune modification en remplaçant d'une part $\mathbb{C}$ par un corps absolument quelconque et, d'autre part, le terme unitaire par diagonalisable sans aucune hypothèse sur la dimension de E.

Considèront maintenant la représentation régulière de G (définition 1), alors pour tout $g, g' \in G$,

$$R(g)R(g') = R(g+g') = R(g'+g) = R(g')R(g). \qquad \text{(Commutation des endomorphismes } R(g))$$

Par conséquent, pour tou couple $(g, g') \in G^2$,les opérateurs $R(g)$ et $R(g')$ commutent. Le lemme 1 montre qu'il s'agit d'opérateurs unitaires et le lemme 2 montre qu'il existe une base de $L^2(G)$ qui diagonalise tous les $R(g)$. Explicitons maintenant une telle base $\mathcal{B}$.
Soit u un élément de cette base $\mathcal{B}$ (donc $u \neq 0$!) : pour tout g, il existe $\chi_g \in S^1$ tel que $R(g)u = \chi_g u$. On obtient que

$$u(h+g) = \chi_g u(h) \ \forall h, g \in G \Rightarrow u(g) = \chi_g u(0) \ \forall g \in G$$

D'autre part, $R(g)R(g')u = R(g+g')u \ \forall g, g' \in G$ donc $R(g)R(g')u = R(g+g')$ c'est-à-dire

$$\chi_{g+g'} = \chi_g \chi_{g'} \ \forall g, g' \in G.$$

L'application $g \mapsto \chi_g$ est donc un caractère de G. Un calcul direct montre que $< \chi, \chi >_{L^2(G)} = 1$ et l'égalité $< u, u >_{L^2(G)} = 1$, montre que $|u(0)| = 1$. On peut ainsi supposer que $u = \{g \mapsto \chi_g\}$.
En conclusion, on peut supposer que chaque élément de $\mathcal{B}$ est un certain caractère de G. Réciproquement, soit χ un caractère de G, alors χ est un vecteur propre de tous les opérateurs $R(g)$. En effet, par définition $\chi \neq 0$ (ses valeurs sont de module 1) et on a

$$\begin{aligned} \forall g, h \quad &\in \quad G, \ [R(g)\chi](h) = \chi(h+g) = \chi(g)\chi(h) \\ &\Rightarrow \quad \forall g \in G, \ [R(g)\chi] = \chi(g)\chi. \end{aligned}$$

On en déduit le théorème suivant

Théorème 1
L'ensemble $\widehat{G}$ des caractères unitaires de G forme une base orthonormale de $L^2(G)$ qui diagonalise tous les $R(g)$, $g \in G$.

Théorème 2
Soit G un groupe fini commutatif.

1. $$\left|\widehat{G}\right| = |G|. \tag{2}$$

2. *Si $g \neq 0$ alors il existe un caractère χ de G tel que $\chi(g) \neq 1$.*
3. *Il existe un isomorphime entre G et $\widehat{\widehat{G}}$ (l'ensemble des caractères de $\widehat{G}$).*
4. $$\frac{1}{|G|}\sum_{g\in G}\chi(g)\overline{\chi'(g)} = \begin{cases} 1 \text{ si } \chi = \chi' \\ 0 \text{ si } \chi \neq \chi' \end{cases} \quad et \ \frac{1}{|G|}\sum_{\chi\in\widehat{G}}\chi(g)\overline{\chi(g')} = \begin{cases} 1 \text{ si } g = g' \\ 0 \text{ si } g \neq g' \end{cases} \tag{3}$$

Preuve :

1. $\widehat{G}$ forme une base de $L^2(G)$ donc
$$\dim_{\mathbb{C}} L^2(G) = \left|\widehat{G}\right|. \tag{4}$$
On appelle masse de Dirac en g la fonction de $L^2(G)$ définie par $\delta_g(h) = \begin{cases} 1 \text{ si } h = g \\ 0 \text{ si } h \neq g \end{cases}$ .Tout élément u de $L^2(G)$ s'écrit $u = \sum_{g\in G} u(g)\delta_g$ et cette écriture est unique, ce qui montre que $\dim_{\mathbb{C}} L^2(G) = |G|$ d'où $\left|\widehat{G}\right| = |G|$.
2. On raisonne par contraposée. Soit $g \in G$ tel que $\chi(g) = 1\ \forall \chi \in \widehat{G}$: étudions l'opérateur $R(g)$
$$\forall \chi \in \widehat{G},\ [R(g)\chi] = \chi(g)\chi = \chi.$$
L'opérateur $R(g)$ laisse fixe tous les $\chi \in \widehat{G}$ qui forment une base de $L^2(G)$ donc $R(g) = Id_{L^2(G)}$. Par conséquent,
$$[R(g)\delta_g] = \delta_g \Leftrightarrow \forall h \in G,\ \delta_g(h+g) = \delta_g(h)$$
ce qui implique que $\delta_g(2g) = \delta_g(g) = 1$ donc $2g = g$ c'est-à-dire $g = 0$.
3. Pour g fixé dans G, l'application $\chi \overset{f_g}{\mapsto} \chi(g)$ est un caractère de $\widehat{G}$. En effet, $|f_g(\chi)| = |\chi(g)| = 1$ et
$$f_g(\chi\chi') = (\chi\chi')(g) = \chi(g)\chi'(g) = f_g(\chi)f_g(\chi')$$
L'application $g \mapsto f_g$ est un morphisme de G dans $\widehat{\widehat{G}}$ car
$$\forall \chi \in \widehat{G},\ (f_{gg'})(\chi) = \chi(gg') = \chi(g)\chi(g') = f_g(\chi)f_{g'}(\chi)$$
donc
$$f_{gg'} = f_g f_{g'}$$
Soit $H : \begin{cases} G \to \widehat{\widehat{G}} \\ g \mapsto (\chi \mapsto \chi(g)) \end{cases}$. Les calculs précédents montre que H est un morphisme de groupe. Comme $\left|\widehat{\widehat{G}}\right| = \left|\widehat{G}\right| = |G|$, il suffit de montrer que H est injectif pour prouver que H est l'isomorphisme cherché. Il est nécessaire de remarquer que $\chi \longmapsto 1$ est l'élément neutre de $\widehat{\widehat{G}}$.
Si $H(g) = 1_{\widehat{\widehat{G}}}$ alors
$$\forall \chi \in \widehat{G}\ [H(g)](\chi) = 1 \Leftrightarrow \forall \chi \in \widehat{G}\ \chi(g) = 1$$
donc $g = 0$ d'après le théorème 2.
4. la famille $(\chi)_{\chi\in\widehat{G}}$ forme une base orthonormée de $L^2(G)$ ce qui montre la première formule.
Si l'on remplace G par $\widehat{G}$ dans cette dernière formule, on obtient que, quelques soient les caractères A et A' de $\widehat{G}$,
$$\frac{1}{\left|\widehat{G}\right|}\sum_{\chi\in\widehat{G}} A(\chi)\overline{A'(\chi)} = \begin{cases} 1 \text{ si } \chi = \chi' \\ 0 \text{ si } \chi \neq \chi' \end{cases}$$

.Bien entendu, A et A' sont des éléments de $\widehat{\widehat{G}}$.
L'application $H : \begin{cases} G \to \widehat{\widehat{G}} \\ g \mapsto (\chi \mapsto \chi(g)) \end{cases}$ est un isomorphisme de G sur $\widehat{\widehat{G}}$, si $A \in \widehat{\widehat{G}}$, il existe un unique $g \in G$ tel que $A = H(g)$. Par conséquent,

$$\begin{aligned} \exists! g &\in G \text{ tel que } \forall \chi \in \widehat{G},\ A(\chi) = \chi(g) \\ \text{et } \exists! g' &\in G \text{ tel que } \forall \chi \in \widehat{G},\ A'(\chi) = \chi(g') \end{aligned}$$

En utilisant l'égalité 2, on en déduit que

$$\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(g)\overline{\chi(g')} = \begin{cases} 1 \text{ si } \chi = \chi' \\ 0 \text{ si } \chi \neq \chi' \end{cases}$$

■

Remarque 1
la formule 2 peut nous faire penser que les groupes G et $\widehat{G}$ sont isomorphes. Ce résultat est vrai pour les groupes finis commutatifs : il découle de la structure des groupes finis commutatifs. Le cas du groupe $\mathbb{Z}/n\mathbb{Z}$, qui est le prototype des groupes finis cycliques, est traité dans l'exemple 1, page 6, mais il est en général faux pour les groupes commutatifs infinis

3 La transformation de Fourier sur G.

Soit u une fonction appartenant à $L^2(G)$. Le théorème 1 montre qu'il existe une famille de complexes $(c_\chi)_{\chi \in \widehat{G}}$ telle que

$$u = \sum_{\chi \in \widehat{G}} c_\chi \chi. \tag{5}$$

Puisque la famille $(\chi)_{\chi \in \widehat{G}}$ est une base orthonormale, on a

$$c_\chi = < u, \chi >_{L^2(G)} = \frac{1}{|G|} \sum_{g \in G} u(g)\overline{\chi(g)} \tag{6}$$

et le théorème de Pythagore nous fournit l'égalité

$$\|u\|^2_{L^2(G)} = \sum_{\chi \in \widehat{G}} |c_\chi|^2 \tag{7}$$

Définition 2
Soit u une fonction appartenant à $L^2(G)$. On appelle transformée de Fourier de u, la fonction $\widehat{u}$ appartenant à $L^2(\widehat{G})$ définie par

$$\forall \chi \in \widehat{G} \quad \widehat{u}(\chi) = \frac{1}{|G|^{\frac{1}{2}}} \sum_{g \in G} u(g)\overline{\chi(g)}.$$

Théorème 3 (Transformation de Fourier)

1. ***La formule de Parseval.***
   La transformation de Fourier est une isométrie de $L^2(G)$ sur $L^2(\widehat{G})$ c'est-à-dire

$$\forall u \in L^2(G),\ \ \|u\|^2_{L^2(G)} = \|\widehat{u}\|^2_{L^2(\widehat{G})} \tag{8}$$

   ou encore

$$\forall u, v \in L^2(G), \qquad < u, v >_{L^2(G)} = < \widehat{u}, \widehat{v} >_{L^2(\widehat{G})} \tag{9}$$

2. ***Développement en "série de Fourier"***

$$\forall u \in L^2(G),\ u = \frac{1}{\left|\widehat{G}\right|^{\frac{1}{2}}} \sum_{\chi \in \widehat{G}} \widehat{u}(\chi)\chi. \tag{10}$$

Preuve :

1. La formule 8 découle tout simplement de la formule 7 et de la formule 3.
   La formule 9 s'obtient par polarisation de la formule 8 (c'est-à-dire que l'on remplace u par $u+v$ puis on dévelloppe).
   La transformation de Fourier est clairement une application linéaire. Puisque la transformation est une isométrie de $L^2(G)$ dans $L^2(\widehat{G})$, elle est injective. D'autre par, la formule 4 que l'on applique à G et à $\widehat{G}$ ainsi que la formule 2 montrent que $\dim_{\mathbb{C}} L^2(G) = \dim_{\mathbb{C}} L^2(\widehat{G})$ ce qui implique que la transformation de Fourier est une isométrie de $L^2(G)$ sur $L^2(\widehat{G})$.
2. Cela découle immédiatement des égalités 5 et 6.

■

Exemple 1
Soient n un entier et G le groupe $\mathbb{Z}/n\mathbb{Z}$.

1. Soit χ un caractère de $\mathbb{Z}/n\mathbb{Z}$, alors $\chi(\overline{k}) = \chi(k.\overline{1}) = (\chi(\overline{1}))^k$ et $\chi(\overline{n}) = \chi(\overline{0}) = 1$. Ainsi $\chi(1)$ est une racine $n^{ème}$ de l'unité. Soit ζ une racine primitive $n^{ème}$ de l'unité (c'est-à-dire $\zeta^n = 1$ et $\zeta^k \neq 1$ si $k \in \{1, ..n-1\}$ ou encore ζ est un générateur du groupe $\mathbb{U}_n$ des racines $n^{èmes}$ de l'unité) : il existe $a \in \mathbb{Z}$ tel que $\chi(1) = \zeta^a$, ce qui nous donne
   $$\forall k \in \mathbb{Z}/n\mathbb{Z},\ \chi(\overline{k}) = \zeta^{ak}.$$
   Par suite, tout caractère de $\mathbb{Z}/n\mathbb{Z}$ est de la forme $\overline{k} \mapsto \zeta^{ak}$ pour un certain $a \in \mathbb{Z}$.
   Considérons l'application définie sur $\mathbb{Z}$ à valeurs dans $\widehat{\mathbb{Z}/n\mathbb{Z}}$ donnée par
   $$a \overset{H}{\mapsto} H(a) = \left\{ \begin{array}{c} \mathbb{Z}/n\mathbb{Z} \to \mathbb{S}^1 \\ \overline{k} \mapsto \zeta^{ak} \end{array} \right. .$$
   Un calcul élémentaire montre que H est un morphisme de groupe. Son image est $\widehat{\mathbb{Z}/n\mathbb{Z}}$ et son noyau est $n\mathbb{Z}$ ($H(a) = 1$ ssi $1 = \zeta^{a1} = \zeta^a$ donc $a \mid n$). Le premier théorème d'isomorphisme montre que $\widehat{\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z}$.
2. Fixons une racine primitive $n^{ème}$ de l'unité, par exemple $\zeta = \exp(\frac{2\pi i}{n})$. Soit u une fonction sur $\mathbb{Z}/n\mathbb{Z}$ et χ un caractère de $\mathbb{Z}/n\mathbb{Z}$. Il existe donc $a \in \mathbb{Z}/n\mathbb{Z}$ tel que $\chi(\overline{k}) = \exp(\frac{2ak\pi i}{n})$. La transformation de Fourier de u peut donc être vue comme une fonction sur $\mathbb{Z}/n\mathbb{Z}$. définie par
   $$\forall a \in \mathbb{Z}/n\mathbb{Z} \quad \widehat{u}(\overline{a}) = \frac{1}{\sqrt{n}} \sum_{k \in \mathbb{Z}/n\mathbb{Z}} u(\overline{k}) \exp(-\frac{2\pi iak}{n}).$$
   On a donc la formule d'inversion de Fourier
   $$\forall \overline{k} \in \mathbb{Z}/n\mathbb{Z},\ u(\overline{k}) = \frac{1}{\sqrt{n}} \sum_{k \in \mathbb{Z}/n\mathbb{Z}} \widehat{u}(\overline{a}) \exp(\frac{2\pi iak}{n})$$

4 Dualité de Pontriaguin

Nous supposons acquis les notions élémentaires sur les groupes (groupes produits et quotient, dont les trois théorèmes d'isomorphes de Noether).
Rappellons en outre, que le dual d'un groupe est muni de la loi produit définie par la formule 1.

Proposition 1
Soient G et H deux groupes commutatifs finis. Le groupe $\widehat{G \times H}$ est isomorphe à $\widehat{G} \times \widehat{H}$.

Preuve :
Soit χ un caractère de $G \times H$. Nous définissons bien un caractère de G (resp. H) en posant

$$\chi_G(g) = \chi((g,0)) \quad (\text{resp. } \chi_H(h) = \chi((0,h))).$$

L'application $T : \begin{cases} \widehat{G \times H} \to \widehat{G} \times \widehat{H} \\ \chi \mapsto (\chi_G, \chi_H) \end{cases}$ est un morphisme de groupe (c'est élémentaire). La formule 2 montre que les groupes $\widehat{G \times H}$ et $\widehat{G} \times \widehat{H}$ ont même cardinal, donc il suffit de prouver que T est injectif.
Soit χ un caractère de $G \times H$ tel que $T(\chi) = 1$ i.e. $\chi_G(g) = \chi((g,0)) = 1$ et $\chi_H(h) = \chi((0,h)) = 1 \; \forall (g,h) \in G \times H$.
En particulier on a $\forall (g,h) \in G \times H \quad \chi((g,h)) = \chi((g,0) + (0,h)) = \chi((g,0))\chi((0,h)) = 1$, ce qui signifie que $\chi = 1$. ■

Définition 3
Soit $(G,+)$ un groupe commutatif fini et H un sous-groupe de G.
On appelle orthogonal de H dans G le sous-groupe $H^\perp$ de $\widehat{G}$ défini par

$$H^\perp = \{\chi \in \widehat{G} \text{ tel que } \chi(h) = 1 \quad \forall h \in H\}$$

Théorème 4 (dualité de Pontriaguin abstraite)
Soit $(G,+)$ un groupe fini commutatif et H un sous-groupe de G.

1. *Les groupes G et $\widehat{\widehat{G}}$ sont isomorphes*
2. *Le groupe $\widehat{G/H}$ est isomorphe au groupe $H^\perp$. En particulier $\left|H^\perp\right| = \dfrac{|G|}{|H|}$*
3. *$\widehat{H}$ est isomorphe à $\widehat{G}/(H^\perp)$.*

Preuve :

1. Ce résultat est déjà démontrée (cf. théorème 2).
2. A tout caractère χ de G/H, on associe le caractère $\widetilde{\chi}$ de G défini par $\widetilde{\chi}(g) = \chi(g \bmod H)$. L'application $S : \begin{cases} \widehat{G/H} \to \widehat{G} \\ \chi \mapsto \widetilde{\chi} \end{cases}$ est un morphisme de groupe. Explicitons son noyau et son image.
   Supposons que $\chi \in \ker S$: quelque soit $g \in G \quad \widetilde{\chi}(g) = \chi(g \bmod H) = 1$. Le caractère χ est trivial sur toutes les classes de G/H ce qui implique que χ est le caractère trivial et $\ker S = \{1\}$.
   Soit χ un caractère de G/H : la définition de $\widetilde{\chi}$ implique que $\widetilde{\chi}$ est trivial sur H (car $h \bmod H = 0 \bmod H$) donc $\chi \in H^\perp$ et $\operatorname{Im} S \subset H^\perp$.
   Réciproquement, soit χ' un caractère de G appartenant à $H^\perp$. Considérons deux éléments g et g' quelconques de G tels que $g \bmod H = g' \bmod H \Leftrightarrow g - g' \in H$ donc $g = g' + h$ pour un certain élément h de H. On en déduit que

   $$\chi'(g') = \chi'(g' + h) = \chi'(g')\chi'(h) = \chi'(g)$$

   et nous définissons bien une application χ sur G/H en posant

   $$\chi(g \bmod H) = \chi'(g).$$

   La loi de groupe de G/H implique que χ est un caractère de G/H tel que $\widetilde{\chi} = \chi'$. Par conséquent, pour tout élément $\chi' \in H^\perp$, il existe un élément $\chi \in \widehat{G/H}$ pour lequel $S(\chi) = \chi'$ i.e. $H^\perp \subset \operatorname{Im} S$ d'où $\operatorname{Im} S = H^\perp$.
   Conclusion : l'application S est injective et son image est $H^\perp$. En appliquant le premier théorème d'isomorphisme, on obtient l'isomorphisme recherché. La formule sur le cardinal est la conséquence de la formule 2

3. Considérons $T : \left\{ \begin{array}{c} \widehat{G} \to \widehat{H} \\ \chi \mapsto \chi_{|H} \end{array} \right.$ où $\chi_{|H}$ désigne la restriction du caractère χ au sous-groupe H. L'application T est visiblement un morphisme de groupe. Son noyau est exactement $H^\perp$. Le premier théorème d'isomorphisme montre que $\operatorname{Im} T$ est isomorphe à $\widehat{G}/(H^\perp)$. En particulier,

$$\begin{aligned} |\operatorname{Im} T| &= \left|\widehat{G}/(H^\perp)\right| = \frac{\left|\widehat{G}\right|}{|H^\perp|} = \frac{|G|}{\frac{|G|}{|H|}} \text{ (le résultat 2 du théorème présent)} \\ &= |H| = \left|\widehat{H}\right| \text{ (cf. formule 2)} \end{aligned}$$

Or $\operatorname{Im} T \subset \widehat{H}$ donc $\operatorname{Im} T = \widehat{H}$.

■

Ce théorème de dualité est très important : il montre que la connaissance complète du dual de G fournit le dual d'un quotient quelconque de celui-ci ainsi que le dual d'un sous-groupe quelconque. Comme nous l'avons déjà remarquer G est isomorphe avec son dual. Nous pouvons le démontrer sous une condition supplémentaire sur le groupe G que nous allons énoncer dans la définition et le théorème suivant (qui nous sera très utile pour des calculs explicites)

Définition 4
Soit G un groupe fini commutatif.
Un bicaractère ϱ symétrique non dégénérée est une applcation de $G \times G$ dans S^1 tel que

$$\begin{array}{l} \forall g, g', g" \in G, \quad \varrho(gg", g') = \varrho(g, g')\varrho(g", g') \quad \varrho(g, g'g") = \varrho(g, g')\varrho(g, g") \text{ (}"\textit{bilinéarité}"\text{)} \\ \forall g \in G, \quad [(\varrho(g, g') = 1 \quad \forall g' \in G] \Rightarrow g = 0) \text{ (}\textit{non dégénéré}\text{)} \end{array}$$

Théorème 5 (Dualité de Pontriaguin pour les groupes munis d'un bicaractère non dégénéré)
Soit ϱ un bicaractère non dégénéré d'un groupe fini commutatif G.
L'application $U : \left\{ \begin{array}{c} G \to \widehat{G} \\ g \mapsto (g' \mapsto \varrho(g, g')) \end{array} \right.$ *est un ismorphisme entre G et $\widehat{G}$.*

Preuve :
Cette application U est visiblement un morphisme de groupe (il suffit de l'écrire) entre deux groupes de mêmes cardinaux (d'après la formule 2) Il nous suffit de montrer qu'elle est injective. Soit $g \in G$ tel que $U(g) = 1$ i.e. $\forall g' \in V$, $\varrho(g, g') = 1$. Par conséquent $g = 0$ (ρ est non dégénéré) et l'application U est injective donc bijective. ■

Remarque 2
L'isomorphisme entre G et $\widehat{G}$ n'est pas intrinsèque à G. Il dépend du choix arbitraire d'un bicaractère non dégénérée ρ.

5 Formule sommatoire de Poisson

Théorème 6 (Formule sommatoire de Poisson abstraite)
Soient G un groupe fini commutatif et H un sous-groupe de G. Pour toute fonction $u \in L^2(G)$, on a :

$$\frac{1}{|H|^{\frac{1}{2}}} \sum_{h \in H} u(h) = \frac{1}{|H^\perp|^{\frac{1}{2}}} \sum_{\chi \in H^\perp} \widehat{u}(\chi)$$

Preuve :
On définit sur G la fonction v_0 par

$$\forall g \in G \quad v_0(g) = \sum_{h \in H} u(g + h).$$

Un simple changement de variable montre que $v_0(g+h_1)=v_0(g)\ \forall h_1\in H$ et $\forall g\in G$. Par conséquent, la formule

$$\forall \overline{g}=g \bmod H\in G/H \quad v(\overline{g})=v_0(g)$$

définit une fonction v appartenant à $L^2(G/H)$. La formule d'inversion de Fourier (10), appliquée à cette fonction v et évaluée au point $\overline{g}=\overline{0}$, nous fournit l'égalité suivante :

$$v(\overline{0})=\frac{1}{\left|\widehat{G/H}\right|^{\frac{1}{2}}}\sum_{\chi'\in\widehat{G/H}}\widehat{v}(\chi') \tag{11}$$

Déterminons les coefficients de Fourier de $\widetilde{v}$.. Soit χ' un caractère de G/H, on a

$$\widehat{v}(\chi')=\frac{1}{|G/H|^{\frac{1}{2}}}\sum_{\overline{g}\in G/H}v(\overline{g})\overline{\chi'(\overline{g})}$$

Nous allons expliciter ce coefficient de Fourier. La dualité de Pontriaguin (théorème 4) montre qu'il existe un unique caractère χ appartenant à $H^\perp$ tel que $\forall g\in G/H \quad \chi'(\overline{g})=\chi(g)$.
Considérons une famille de représentants de G/H dans G, i.e. une famille $S=\{g_r\}_{1\leqslant i\leqslant r}$ avec

- $G/H=\{\overline{g_i},\ 1\leqslant i\leqslant r\}$
- $\forall i\neq j \quad \overline{g_i}\neq\overline{g_i} \bmod H$.

De façon équivalente, $G=\coprod_{i=1}^{r}\{g_i+H\}$ où le symbole $\coprod$ désigne la réunion de parties disjointes

$$\begin{aligned}\sum_{\overline{g}\in G/H}v(\overline{g})\overline{\chi'(\overline{g})} &= \sum_{i=1}^{r}v(g_i)\overline{\chi(g_i)}=\sum_{i=1}^{r}\sum_{h\in H}u(g_i+h)\overline{\chi(g_i)}\\ &= \sum_{i=1}^{r}\sum_{h\in H}u(g_i+h)\overline{\chi(g_i+h)}\ (\text{car }\chi\text{ est trivial sur }H)\\ &= \sum_{g\in G}u(g)\overline{\chi(g)}=|G|^{\frac{1}{2}}\,\widehat{u}(\chi).\end{aligned}$$

Nous déduisons de cette dernière égalité et de l'égalité $|G/H|=\dfrac{|G|}{|H|}$ la formule suivante :

$$\forall\chi'\in\widehat{G/H}\quad \widehat{v}(\chi')=|H|^{\frac{1}{2}}\,\widehat{u}(\chi)$$

oùχ' est un caractère de G/H et χ est l'unique caractère de $H^\perp$ tel que $\forall g\in G/H \quad \chi'(\overline{g})=\chi(g)$.
Lorsque le caractères χ' décrit $\widehat{G/H}$, le caractère χ décrit $H^\perp$ et $\left|\widehat{G/H}\right|=\left|H^\perp\right|$ (c'est la dualité de Pontriaguin).
La formule (11) devient

$$\begin{aligned}v(\overline{0})&=\frac{|H|^{\frac{1}{2}}}{|H^\perp|^{\frac{1}{2}}}\sum_{\chi\in H^\perp}\widehat{v}(\chi)\\ \Leftrightarrow\ \frac{1}{|H|^{\frac{1}{2}}}\sum_{h\in H}u(h)&=\frac{1}{|H^\perp|^{\frac{1}{2}}}\sum_{\chi\in H^\perp}\widehat{u}(\chi)\end{aligned}$$

■

6 Cas des espaces vectoriels

Remarque 3
Le théorème de Wedderburn montre que tout corps fini est commutatif. Nous ne l'utiliserons pas dans cette section.

Définition 5
Soit V un espace vectoriel sur un corps commutatif k. Une forme bilinéaire b est dite non dégénérée ssi

$$\forall x \in V, \quad (b(x,y) = 0 \quad \forall y \in V \Rightarrow x = 0))$$

En particulier, l'application $(x \mapsto (y \mapsto b(x,y)))$ est un isomorphisme (d'espace vectoriel) de V sur $V^* = \mathcal{L}(V,k)$

En effet, il s'agit d'une application linéaire entre deux espaces vectoriels de même dimension et et son noyau est réduit à 0 (par hypothèse sur b). Bien entendu, tout espace vectoriel de dimension finie possède une forme bilinéaire non dégénérée : il suffit de considérer, par exemple, la forme bilinéaire définie dans une base convenable $\mathcal{B}$ par

$$\rho((x_1,..,x_n),(y_1,..,y_n)) = \sum_{i=1}^{n} x_i y_i.$$

Théorème 7 (Dualité de Pontriaguin pour les espaces vectoriels)
Soit b une forme bilinéaire non dégénérée d'un espace vectoriel $(V,+,.)$ sur un corps fini commutatif k et χ_0 un caractère additif non trivial de $(k,+)$.
L'application $U : \begin{cases} V \to \widehat{V} \\ x \mapsto (y \mapsto \chi_0(\varrho(x,y)) \end{cases}$ *est un ismorphisme entre V et $\widehat{V}$.*

Preuve :
Je laisse vérifier au lecteur que l'application $\varrho(x,y) = \chi_0(\varrho(x,y))$ est un bicaractère de V. Ce bicaractère est non dégénéré. En effet, soit $x \in V$ tel que $U(x) = 1$ i.e. $\forall y \in V$, $\chi_0(\varrho(x,y)) = 1$.
Supposons que $x \neq 0$.
Le caractère χ_0 n'étant pas trivial, il existe $a_0 \in V$ tel que $\chi_0(a_0) \neq 1$. La forme linéaire $y \mapsto \varrho(x,y)$ n'est pas nulle (d'après la définition 5) donc son image est k. En particulier, il existe $y_0 \in V$ tel que $\varrho(x,y_0) = a_0$ d'où $\chi_0(\varrho(x,y)) = \chi_0(a_0) \neq 1$ ce qui est absurde.
Par conséquent $x = 0$ et l'application U est injective donc bijective.
Il suffit alors d'appliquer le théorème 5) ■

Remarque 4
L'isomorphisme entre V et $\widehat{V}$ n'est pas intrinsèque à V. Il dépend du choix arbitraire d'une forme bilinéaire (symétrique ou antisymétrique) non dégénérée ρ et d'un caractère additif non trivial χ_0.

Dans toute la suite de cette section V désigne un espace vectoriel de dimension fini sur un corps fini k, muni d'une forme bilinéaire non dégénérée b et d'un caractère additif non trivial de $(k,+)$: χ_0 . Le théorème 7 nous permet d'exprimer sous une forme plus simple les section 3 et 5.

Définition 6
Soit u une fonction appartenant à $L^2(V)$. On appelle transformée de Fourier de u, la fonction $\widehat{u}$ appartenant à $L^2(V)$ définie par

$$\forall \xi \in V \quad \widehat{u}(\xi) = \frac{1}{|V|^{\frac{1}{2}}} \sum_{x \in V} u(x) \chi_0(-\rho(x,\xi))$$

Théorème 8 (Transformation de Fourier)

1. ***La formule de Parseval.***
   La transformation de Fourier est une isométrie de $L^2(V)$ sur $L^2(V)$ c'est-à-dire

$$\forall u \in L^2(V), \ \ \|u\|^2_{L^2(V)} = \|\widehat{u}\|^2_{L^2(V)} \tag{12}$$

   ou encore

$$\forall u, v \in L^2(V), \qquad < u, v >_{L^2(V)} = < \widehat{u}, \widehat{v} >_{L^2(V)} \tag{13}$$

2. ***Développement en "série de Fourier"***

$$\forall u \in L^2(V), \forall x \in V \quad u(x) = \frac{1}{|V|^{\frac{1}{2}}} \sum_{\xi \in V} \widehat{u}(\xi) \chi_0(\rho(x,\xi)) \tag{14}$$

Définition 7
Soit S une partie de V. On appelle orthogonal de S relativement à la dualité de Pontriaguin associé à (χ_0, ρ), l'ensemble suivant

$$S_\rho^o = \{y \in V \text{ tel que } \chi_0(\rho(x,y)) = 1 \ \forall x \in S\}.$$

Remarque 5
On ne peut identifier S_ρ^o à la partie orthogonale, relativement à ρ, défini dans le cours d'algèbre bilinéaire. Cela provient tout simplement du fait suivant

$$\chi_0(\rho(x,y)) = 1 \quad \forall x \in S \not\Rightarrow \rho(x,y) = 0 \quad \forall x \in S$$

car le noyau de χ_0 n'est pas nécessairement trivial. Nous en verrons des exemples dans un autre article.

Lemme 3
Si H est un sous-groupe additif de V alors H_ρ^o est un sous-groupe additif de V.

Preuve :
C'est immédiat. ■

Corollaire 1
Soit H un sous-groupe additif de V.

1. *les groupes $H^\perp$ et H_ρ^o sont isomorphes.*
2. *En particulier, $\left|H_\rho^o\right| = \left|H^\perp\right| = \dfrac{|G|}{|H|}$.*
3. *Si en outre, b est symétrique, on a $(H_\rho^o)_\rho^o = H$.*

Preuve :

1. Il suffit pour cela de considérer le morphisme de groupe $U' : \left\{ \begin{array}{c} H_\rho^o \to H^\perp \\ h^o \mapsto (x \mapsto \chi_0(\rho(x,h^o)) \end{array} \right.$.
   (il s'agit de la restriction à H_ρ^o du morphisme U défini dans le théorème 7)
   – Si $h^o \in H_\rho^o$, alors pour $h \in H$, on a $\chi_0(-\rho(h,h^o)) = \chi_0(0) = 1$ donc le caractère de V défini par $S(h^o)$ appartient bien à $H^\perp$.
   – L'injectivité de U' découle de l'injectivité de U.
   – Soit χ un élément de $H^\perp$. Le théorème 7 montre qu'il existe $\xi \in V$ tel que $\chi = U(\xi)$. Or le caractère χ est trivial sur H donc
   $$\forall h \in H \quad 1 = \chi(h) = \chi_0(\rho(h,\xi)),$$
   ce qui implique que $\xi \in H_\rho^o$ et U' est bien surjective.
2. Cela découle du 1.
3. On remarque pour commencer que $H \subset (H_\rho^o)_\rho^o$ (se référer au cours d'algèbre bilinéaire de deuxième année). Il suffit de vérifier alors que ces deux parties ont même cardinal
   $$\left|(H_\rho^o)_\rho^o\right| = \left|(H_\rho^o)^\perp\right| = \frac{|G|}{\left|H_\rho^o\right|} = \frac{|G|}{\dfrac{|G|}{|H|}} = |H|\,.$$

■

Théorème 9 (Formule sommatoire de Poisson pour les espaces vectoriels)
Soient V un espace vectoriel sur un corps fini commutatif k, H un sous-groupe additif de V commutatif et ρ une forme bilinéaire non dégénérée sur V. Pour toute fonction $u \in L^2(V)$, on a :

$$\frac{1}{|H|^{\frac{1}{2}}} \sum_{h \in H} u(h) = \frac{1}{\left|H_\rho^o\right|^{\frac{1}{2}}} \sum_{h^o \in H_\rho^o} \widehat{u}(h^o).$$

En particulier, si H est autodual, i.e. $H = H_\rho^o$, on a

$$\sum_{h \in H} u(h) = \sum_{h \in H} \widehat{u}(h).$$

7 Exercices

Exercice 1

1. Montrer que la tranformation de Fourier sur $\mathbb{Z}/n\mathbb{Z}$ est un endomorphisme hermitien c'est-à-dire

$$\forall u, v \in L^2(G), \quad < \widehat{u}, v >_{L^2(\mathbb{Z}/n\mathbb{Z})} = < u, \widehat{v} >_{L^2(\mathbb{Z}/n\mathbb{Z})}$$

2. Exprimer $\widehat{\widehat{u}}$ en fonction de u.

Exercice 2

Déterminer le groupe des caractères de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, expliciter la transformée de Fourier ainsi que la formule d'inversion et l'égalité de Parseval.

Exercice 3

Soit $u \in L^2(G)$ une fonction à valeurs réelles. *

1. Montrer que u s'écrit comme est une combinaison réelle de " cos " et de " sin " convenables.
2. Expliciter ces coefficients lorsque
   (a) $G = \mathbb{Z}/n\mathbb{Z}$
   (b) $G = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$

Exercice 4 (convolution)

Soit G un groupe fini additif. Soient u, v deux éléments de $L^2(G)$. On appelle convolée de u par v la fonction $u * v$ définie sur G par

$$(u * v)(x) = \sum_{y \in G} u(y)v(x - y).$$

Montrer que $\widehat{u * v} = \widehat{u}\widehat{v}$.

Exercice 5

Soit $G = \mathbb{Z}/n\mathbb{Z}$ et $T : \begin{cases} G \times G \to S^1 \\ (\overline{a}, \overline{b}) \mapsto \exp(\frac{2\pi iab}{n}) \end{cases}$

Montrer que l'application b est bien définie et qu'il s'agit d'un bicaractère non dégénéré ?
Retrouver le dual de G.

Exercice 6 (symbole de Legendre)

Soit p un nombre premier impair.

1. Quel est le noyau de $\begin{cases} (\mathbb{Z}/p\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times \\ \overline{x} \mapsto \overline{x}^2 \end{cases}$. En déduire le nombre de carrés dans $\mathbb{Z}/p\mathbb{Z}$.
2. On définit l'application $\left(\frac{\cdot}{p}\right)$ (appelé symbole de Legendre) sur $\mathbb{Z}/p\mathbb{Z}$ par

$$\left(\frac{x}{p}\right) = \begin{cases} 1 \text{ si } x \text{ est un carré de } \mathbb{Z}/p\mathbb{Z} \\ -1 \text{ sinon} \end{cases}.$$

   Montrer que $\forall x \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \bmod(p)$. En déduire que le symbole de Legendre est un caractère de $(\mathbb{Z}/p\mathbb{Z})^\times$.
3. Calculer $S = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} \left(\frac{x}{p}\right)$ (on considérera un a tel que $\left(\frac{a}{p}\right) = -1$ ainsi que $\left(\frac{a}{p}\right) S$).
   En déduire $\sum_{x \in (\mathbb{Z}/p\mathbb{Z})} \left(\frac{x}{p}\right)$

Exercice 7 (Sommes de Gauss)
Le but de cet exercice est de calculer la somme de Gauss définie par $\tau_p = \sum_{k\in\mathbb{Z}/p\mathbb{Z}} \exp(\frac{2\pi i k^2}{p})$ lorsque p est un nombre premier impair.

Pour cela, on considère la fonction définie sur $\mathbb{Z}/p\mathbb{Z}$ par $u(\overline{x}) = \exp(\frac{2\pi i x^2}{p})$. Il est utile de connaitre la définition du symbole de Legendre (cf. exercice 6

1. Montrer que u est bien définie et expliciter la transformée de Fourier de u.
2. A l'aide d'un changement de variable adéquat, montrer que
$$\widehat{u}(2x) = \exp(-\frac{2\pi i x^2}{p})\tau_p$$
3. Calcul de $\sum_{k\in\mathbb{Z}/p\mathbb{Z}} \exp(-\frac{2\pi i k^2}{p})$.
   (a) Montrer que si -1 est un carré de $k \in (\mathbb{Z}/p\mathbb{Z})^\times$ alors $\tau_p = \sum_{k\in\mathbb{Z}/p\mathbb{Z}} \exp(-\frac{2\pi i k^2}{p})$.
   (b) On suppose que -1 n'est pas un carré de $(\mathbb{Z}/p\mathbb{Z})^\times$.
   Calculer $\sum_{k\in\mathbb{Z}/p\mathbb{Z}} \exp(-\frac{2\pi i k}{p})$ puis montrer que si k n'est pas un carré, alors il est de la forme $-a^2$.
   Vérifier que $\tau_p + \sum_{k\in\mathbb{Z}/p\mathbb{Z}} \exp(-\frac{2\pi i k^2}{p}) = 2\sum_{k\in\mathbb{Z}/p\mathbb{Z}} \exp(-\frac{2\pi i k}{p})$.
   (c) En déduire que $\sum_{k\in\mathbb{Z}/p\mathbb{Z}} \exp(-\frac{2\pi i k^2}{p}) = \left(\frac{-1}{p}\right)\tau_p$
4. Pourquoi a-t-on $\sum_{k\in\mathbb{Z}/p\mathbb{Z}} \widehat{u}(2x)\exp(\frac{2\pi i a x}{p}) = \sum_{k\in\mathbb{Z}/p\mathbb{Z}} \widehat{u}(x)\exp(\frac{4\pi i a x}{p})$?
5. En utilisant la formule d'inversion, montrer que $\tau_p^2 = \left(\frac{-1}{p}\right)p$

(on verra dans le chapitre sur la théorie des nombres algébriques que cette égalité implique la loi de réciprocité quadratique c'est-à-dire que si p et q sont deux nombres premiers impairs distincts alors
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Exercice 8 (fonctions Gamma et de Bessel)
Soit χ un caractère multilplicatif de $(\mathbb{Z}/n\mathbb{Z})^\times$. On l'étend en une fonction sur $(\mathbb{Z}/n\mathbb{Z})$ par
$$\widetilde{\chi}(\overline{k}) = \begin{cases} \chi(\overline{k}) \text{ si } \overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times \\ 0 \text{ si } \overline{k} \notin (\mathbb{Z}/n\mathbb{Z})^\times \end{cases}$$

Dans la suite, la fonction $\widetilde{\chi}$ sera noté χ.
On appelle facteur Gamma de χ la fonction $\Gamma(\chi)$ définie par :
$$\Gamma(\chi) = \sum_{k\in\mathbb{Z}/p\mathbb{Z}} \chi(\overline{k})\exp(-\frac{2\pi i k}{n}).$$

On appelle facteur de Bessel de χ_1, χ_2 la fonction $B(\chi_1, \chi_2)$ définie par :
$$B(\chi_1, \chi_2) = \sum_{k\in\mathbb{Z}/p\mathbb{Z}} \chi_1(\overline{k})\chi_2(\overline{1-k}).$$

1. Montrer que $\widetilde{\chi}$ est une fonction multiplicative de $\mathbb{Z}/n\mathbb{Z}$ c'est-à-dire

$$\forall \overline{a}, \overline{b} \in \mathbb{Z}/n\mathbb{Z},\ \widetilde{\chi}(\overline{ab}) = \widetilde{\chi}(\overline{a})\widetilde{\chi}(\overline{b})$$

2. Montrer que $\widehat{\chi} = \Gamma(\chi)\chi^{-1}$ puis que $\Gamma(\chi)\Gamma(\chi^{-1}) = \chi(-1)$.
   En déduire que $\forall \chi \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, $|\Gamma(\chi)| = 1$
3. Montrer que $\chi_1 * \chi_2 = B(\chi_1, \chi_2)\chi_1\chi_2$
4. Montrer que $B(\chi_1, \chi_2) = \dfrac{\Gamma(\chi_1)\Gamma(\chi_2)}{\Gamma(\chi_1\chi_2)}$ (on utilisera l'exercice 4)
5. On supose, seulement dans cette question,que $n = p$ est un nombre premier impair.
   (a) Exprimer $\Gamma(\chi)$ où χ est le symbole de Legendre (défini dans l'exercice 6) en fonction de τ_p.
   (b) Retrouver la formule de la question 5.de l'exercice 6.