107 — REPRÉSENTATIONS ET CARACTÈRES D'UN GROUPE FINI SUR UN $\mathbb{C}$-ESPACE VECTORIEL.

CADRE : Dans toute cette leçon, on considère des groupes finis et des $\mathbb{C}$-espaces vectoriels de dimension finie. Soit donc G un groupe fini d'élément neutre e.

I/ Représentation d'un groupe fini.

A) Définitions et premiers exemples

[COLM] p.235

Déf : Si V est un $\mathbb{C}$-espace vectoriel, alors une représentation de G sur V est la donnée d'un morphisme $\rho : G \longrightarrow GL(V)$, $g \longmapsto \rho_g$ appelé morphisme de représentation.

Rem : • Il s'agit en fait d'une action de G sur V qui est compatible avec la structure d'espace vectoriel de V. En particulier, cela implique le fait que : $\rho(gh) = \rho(g)\rho(h)$ pour tous $g, h \in G$ où l'action est donnée par $g \cdot v := \rho_g(v)$.
• Dans la suite, on dira de même selon les commodités que ρ ou que V est une représentation du groupe G.

Déf. On appelle degré d'une représentation V de G la dimension de V vu comme espace vectoriel. [COLM] p.245 et [PEYR] p.192

Déf. Deux représentations V_1 et V_2 de G sont dites isomorphes s'il existe un isomorphisme linéaire $u : V_1 \to V_2$ qui commute à l'action de G, c'est-à-dire que si ρ_1 et ρ_2 sont les morphismes de représentations associées à V_1 et V_2, alors u doit vérifier $u \circ \rho_1(g) = \rho_2(g) \circ u$ pour tout $g \in G$.

Rem : Deux représentations isomorphes ont nécessairement le même degré.

Ex. • La représentation triviale $\rho : G \longrightarrow \mathbb{C}$, $g \longmapsto id$ est de degré 1.

• La représentation régulière est la représentation donnée par l'action de translation de G sur G $((g,h) \in G \times G \mapsto gh \in G)$. Cela revient à se donner un espace vectoriel V de dimension [COLM] p.239 $|G|$ et une base $(e_h)_{h \in G}$ de V indicée par G et à définir le morphisme ρ qui pour tout $g \in G$ associe l'automorphisme linéaire qui pour tout $h \in G$ envoie e_h sur e_{gh}.

• La représentation de $\mathbb{Z}/n\mathbb{Z}$ est la donnée d'un $\mathbb{C}$-espace vectoriel V et d'un élément $u \in GL(V)$ vérifiant $u^n = id$. [COLM] p.235

B) Sous-représentations et opérations sur les représentations

Prop & déf. Soit V une représentation de G de morphisme de représentation ρ. Si W est un sous-espace vectoriel de V stable sous l'action de G, alors $\rho^W : G \longrightarrow GL(W)$, $g \longmapsto \rho(g)_{|W}$ est une représentation appelée sous-représentation de G. [COLM] p.242 et [PEYR] p.193

Ex. $\mathbb{C}(1, \dots, 1)$ est une sous-représentation de la représentation régulière qui est isomorphe à la représentation triviale.

Déf. Pour deux représentations ρ_V et ρ_W respectivement sur V et W, on définit la représentation somme $\rho_{V \oplus W}$ sur $V \oplus W$ par : [PEYR] p.196

$$\forall g \in G,\ \forall (v, w) \in V \times W,\ \rho_{V\oplus W}(g)(v, w) := \rho_V(g)(v) + \rho_W(g)(w)$$

Déf. Pour deux représentations ρ_V et ρ_W respectivement sur V et W, on définit la représentation des morphismes $\rho_{L(V,W)}$ sur l'espace $L(V, W)$ par : [PEYR] p.196

$$\forall g \in G,\ \forall f \in L(V, W),\ \rho_{L(V,W)}(g)(f) := \rho_W(g) \circ f \circ \rho_V(g^{-1})$$

C) Représentations irréductibles

Déf. Une représentation V de G est dite irréductible si V ne possède pas de sous-représentation autre que V et $\{0\}$. [PEYR] p.199

Rem : Une représentation de degré 1 est irréductible ; en particulier, la représentation triviale est irréductible.

THM (Maschke): Toute sous-représentation admet un supplémentaire.

[COLM] p.244 **Cor**: Toute représentation de G est somme directe de représentations irréductibles. *

[COLM] p.244 **THM (lemme de Schur)**: Soit G un groupe et soient V_1 et V_2 deux représentations irréductibles de G.

(i) Si V_1 et V_2 ne sont pas isomorphes alors $\mathrm{Hom}_G(V_1, V_2) = 0$

(ii) Si $V_1 = V_2$, alors $\mathrm{Hom}_G(V_1,V_2)$ est la droite des homothéties

II / Théorie des caractères

A) Définition et premières propriétés et exemples

[COLM] p.237 **Déf.** Le caractère d'une représentation V portée par ρ_V est l'application

$$\chi_V : G \longrightarrow \mathbb{C}, \quad g \longmapsto \mathrm{tr}(\rho_V(g))$$

Rem: On a en particulier $\chi_V(e) = \mathrm{tr}(id) = \dim(V)$.

Ex: • Si ρ_V est une représentation de degré 1, alors $\chi_V = \rho_V$

[COLM] p.239 • Représentation de permutation: Si X est un G-ensemble fini muni de l'action $(g,x) \mapsto g\cdot x$, on définit la représentation V_X de degré $|X|$ par l'action linéaire de G sur les vecteurs de la base $(e_x)_{x\in X}$ de V_X donnée par $g\cdot e_x = e_{g\cdot x}$. Le caractère de cette représentation est donné par: $\chi_{V_X}(g) = \#\{x \in X : g\cdot x = x\}$

• En particulier, le caractère de la représentation régulière V_G de G est donné par $\chi_{V_G}(e) = |G|$ et $\chi_{V_G}(g) = 0$ si $g \in G\setminus\{e\}$.

[COLM] p.240 * : **Rem**: Si V_1 et V_2 sont deux représentations de G, notons $\mathrm{Hom}_G(V_1,V_2)$ l'ens. des applications linéaires de V_1 dans V_2 qui commute avec l'action de G. Si $f \in \mathcal{L}(V_1,V_2)$, alors $f \in \mathrm{Hom}_G(V_1,V_2)$ ssi $g\cdot f(v) = f(g\cdot v)$, $\forall g \in G$, $\forall v \in V_1$.

Prop: Soit V une représentation du groupe G. [COLM] p.237-238

(i) Pour tout $g \in G$, on a $\chi_V(g^{-1}) = \overline{\chi_V(g)}$

(ii) Pour tous $g, h \in G$, on a $\chi_V(hgh^{-1}) = \chi_V(g)$.

Prop: Soient V_1 et V_2 des représentations du groupe G. [COLM] p.239

(i) $\chi_{V_1\oplus V_2} = \chi_{V_1} + \chi_{V_2}$

(ii) $\chi_{\mathcal{L}(V_1,V_2)}(g) = \overline{\chi_{V_1}(g)}\,\chi_{V_2}(g)$, pour tout élément $g \in G$. [COLM] p.240

B) Caractères irréductibles et orthogonalité.

Déf: Un caractère est dit irréductible s'il est le caractère d'une représentation irréductible. [COLM] p.246

Déf: Une fonction $\varphi : G \to \mathbb{C}$ est dite centrale si elle est constante sur chaque classe de conjugaison de G, autrement dit si elle vérifie $\varphi(ghg^{-1}) = \varphi(h)$ pour tous $g, h \in G$.

Rem: Les caractères sont des fonctions centrales.

Prop: Si on note $R_{\mathbb{C}}(G)$ l'espace vectoriel des fonctions centrales (c'en est un), alors l'application $\langle , \rangle$ qui à $\varphi_1, \varphi_2 \in R_{\mathbb{C}}(G)$ associe $\langle \varphi_1, \varphi_2\rangle := \frac{1}{|G|}\sum_{g\in G} \overline{\varphi_1(g)}\,\varphi_2(g)$ est un produit scalaire hermitien sur $R_{\mathbb{C}}(G)$. [COLM] p.246

THM (Frobenius): Les caractères irréductibles forment une base orthonormée de l'espace $R_{\mathbb{C}}(G)$ des fonctions centrales. [COLM] p.246

Cor: Le nombre de représentations irréductibles de G est égal au nombre de classes de conjugaison de G. Il est donc fini. [COLM] p.247

Cor: Si $\mathrm{Irr}(G)$ désigne l'ensemble des représentations irréductibles de G, alors toute représentation V de G se décompose de la façon suivante: [COLM] p.248

$$V = \bigoplus_{W \in \mathrm{Irr}(G)} W^{\langle \chi_V, \chi_W \rangle}.$$

Prop: Deux représentations ayant le même caractère sont isomorphes. [COLM] p.243

104

C) Table de caractères d'un groupe fini

[PEYR] p. 225

Déf. La table de caractères de G est défini comme étant le tableau qui donne les valeurs des caractères irréductibles sur les classes de conjugaison de G : en lignes on a les caractères et en colonnes les classes de conjugaison.

[COLM] p. 253

Ex: La table du groupe multiplicatif $\{1,-1\}$ est donnée par : —

	1	-1
1	1	1
χ	1	-1

Prop: On note encore ici $\mathrm{Irr}(G)$ l'ens. des représentations irr de G.

(i) (formule de Burnside) On a $\sum_{W\in\mathrm{Irr}(G)} (\dim W)^2 = |G|$

(ii) Si $g\in G\setminus\{e\}$, on a alors $\sum_{W\in\mathrm{Irr}(G)} \dim(W)\,\chi_W(g) = 0$

[PEYR] p. 228, 229 et 239

Ex: • Table de $\mathfrak{S}_4$ $\boxed{\text{DVP}}$ • Table de Q_8

	1 id	6 [2 1 1]	8 [3 1]	6 [4]	3 [2 2]
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_S	3	1	0	-1	-1
χ_W	3	-1	0	1	-1
χ_V	2	0	-1	0	2

	$\{1\}$	$\{-1\}$	$\{i,-i\}$	$\{j,-j\}$	$\{k,-k\}$
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	1
χ_3	1	1	-1	1	-1
χ_4	1	1	1	-1	-1
χ_5	2	-2	0	0	0

II/ Le cas des groupes abéliens.

A) Caractères d'un groupe abélien.

[COLM] p. 249

Prop: Si G est un groupe abélien, alors toutes les représentations irréductibles de G sont de degré 1. (Rés)

[PEYR] p. 4

Ex: Si G est un groupe cyclique engendré par $g\in G$ ($G=\langle g\rangle$), alors les caractères irréductibles de G sont les χ_j tels que $\chi_j(g)=\omega_m^j$ pour $j\in[\![0;m-1]\!]$ avec $\omega_m = e^{2i\pi/m}$.

B) Dual d'un groupe fini

Déf & prop: Le dual du groupe fini G est l'ensemble noté $\widehat{G}$ est l'ensemble des caractères de G. C'est un groupe pour la multiplication des applications que l'on appelle groupe dual de G. [PEYR] p. 2

Prop: Si G est un groupe cyclique, on a alors un isomorphisme de groupes entre G et son dual : $G\simeq\widehat{G}$. [PEYR] p. 4

Prop: Si G est abélien et si H est un sous-groupe de G, alors tout caractère χ de H peut être prolongé en un carac. de G. $\boxed{\text{DVP}}$ [PEYR] p. 67

Prop: Si G est abélien, alors G et $\widehat{G}$ ont le même ordre

THM (structure des groupes abéliens finis): Si G est un groupe abélien fini, il existe alors des entiers strictement positifs $m_1,\dots,m_r$ uniquement déterminés tels que m_k divise m_{k+1} pour tout $k\in[\![1,r-1]\!]$ et tels que l'on ait l'isomorphisme : $G\simeq \mathbb{Z}/m_1\mathbb{Z}\times\mathbb{Z}/m_2\mathbb{Z}\times\dots\times\mathbb{Z}/m_r\mathbb{Z}$. [PEYR] p. 8

THM: Si G est un groupe abélien fini, alors il existe un isomorphisme de groupes entre G et son dual $G\simeq\widehat{G}$. [PEYR] p. 8
↳ ce résultat est appelé Théorème d'isomorphisme

C) Notion de bidual d'un groupe fini abélien

Déf. Le bidual de G est défini comme le dual du groupe dual de G. On le note $\widehat{\widehat{G}}$ [PEYR] p. 8

Rem: Le bidual est bien défini d'après le théorème d'isomorphisme.

Prop: On a un isomorphisme canonique entre G et $\widehat{\widehat{G}}$ (dans le cas où G est abélien) qui est donné par l'application [PEYR] p. 9

$$\Phi : G \longrightarrow \widehat{\widehat{G}}$$
$$g \longmapsto (\Phi_g : \chi\mapsto\chi(g))$$

Table de caractère de $\mathfrak{S}_4$

Antoine LOUAZEL et Zoïs MOITIER

19 novembre 2014

Référence : G. PEYRÉ, *L'algèbre discrète de la transformée de Fourier*. Ellipses. p.228-230.

Propriétés. *La table de caractère de $\mathfrak{S}_4$ est :*

	1 Id	6 transposition	8 3-cycle	6 4-cycle	3 double transposition
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1
χ_s	3	1	0	-1	-1
χ_W	3	-1	0	1	-1
$\chi_{W'}$	2	0	-1	0	2

Démonstration. On commence par déterminer les classes de conjugaison de $\mathfrak{S}_4$. On sait que les classes de conjugaison sont entièrement déterminées par le nombre et la longueur des cycles dans la décomposition en cycles à supports disjoint. On obtient :

- La classe de l'identité. Elle possède un élément.
- La classe des transpositions. Elle possède $\binom{4}{2} = 6$ éléments.
- La classe des 3-cycles. Elle possède $\dfrac{4 \times 3 \times 2}{3} = 8$ éléments.
- La classe des 4-cycles. Elle possède $\dfrac{4 \times 3 \times 2 \times 1}{4} = 6$ éléments.
- La classe des double transpositions. Elle possède $\dfrac{1}{2}\binom{4}{2} = 3$ éléments.

On sait qu'il y a le même nombre de caractères irréductibles que de classes de conjugaison. Donc on doit trouver 5 carctères irréductibles.

On connait déjà la représentation triviale de degré 1 et de caractère χ_1 et la représentation alterné de degré 1 et de caractère $\chi_\varepsilon = \varepsilon$:

	Id	transposition	3-cycle	4-cycle	double transposition
χ_1	1	1	1	1	1
χ_ε	1	-1	1	-1	1

On considère la représentation de permutation de $\mathfrak{S}_4$ définie par :

$$\rho : \begin{array}{ccc} \mathfrak{S}_4 & \longrightarrow & GL_4(\mathbb{C}) \\ \sigma & \longmapsto & M_\sigma \end{array}$$

où M_σ est la matrice de permutation de σ. Cette représentation n'est pas irréductible car la droite $V_1 = \mathbb{C}(1,1,1,1)$ et l'hyperplan $V_s = \{(x,y,z,t) \in \mathbb{C}^4 \,|\, x+y+z+t = 0\}$ sont $\mathfrak{S}_4$-invariants et supplémentaires. Or la sous-représentation V_1 est la représentation triviale. D'où le caractère de la représentation de permutation $\chi_p = \chi_1 + \chi_s$ et $\chi_p(\sigma)$ est le nombre de points fixes de σ, ce qui nous donne χ_s. On a :

$$\begin{aligned}\langle \chi_s, \chi_s \rangle =& \frac{1}{24}\left((4-1)^2 + 6\times(2-1)^2 + 8\times(1-1)^2 + 6\times(0-1)^2 + 3\times(0-1)^2\right)\\ =& \frac{9+6+6+3}{24}\\ =& 1\end{aligned}$$

donc χ_s est un caractère irréductible et :

	Id	transposition	3-cycle	4-cycle	double transposition
χ_s	3	1	0	-1	-1

Il nous reste à trouver 2 caractères irréductibles. La formule $\sum_{W\in \mathrm{Irr}(\mathfrak{S}_4)} \dim(W)^2 = |\mathfrak{S}_4|$ nous donne que si p et q sont les dimensions des 2 représentations irréductibles manquantes, on a $p^2+q^2 = 13$. Ce qui donne une seule possibilité : une de degré 2 et l'autre de degré 3.

On considère la représentation $W = \mathcal{L}(V_s, V_\varepsilon)$ où $(\varepsilon, V_\varepsilon)$ est la représentation alternée. Elle est de degré 3 et son caractère est $\chi_W = \overline{\chi_s}\chi_\varepsilon$ et on vérifie rapidement que $\langle \chi_W, \chi_W\rangle = 1$. C'est donc un caractère irréductible :

	Id	transposition	3-cycle	4-cycle	double transposition
χ_W	3	-1	0	1	-1

On déduit le dernier caractère irréductible $\chi_{W'}$ de degré 2 à l'aide de la formule suivante pour tout $\sigma \neq \mathrm{Id}$ on a $\sum_{W\in \mathrm{Irr}(\mathfrak{S}_4)} \dim(W)\chi_W(g) = 0$:

	Id	transposition	3-cycle	4-cycle	double transposition
$\chi_{W'}$	2	0	-1	0	2

$\square$

Un groupe abélien et son dual ont même ordre

Antoine LOUAZEL et Zoïs MOITIER

19 novembre 2014

Référence : G. PEYRÉ, *L'algèbre discrète de la transformée de Fourier*. Ellipses. p.4-7.

Propriété. *Soit G un groupe abélien fini. Alors on a $|G| = |\widehat{G}|$.*

Pour démontrer cela on besion de trois résultats intermédiaires :
- Dans le cas des groupes cyclique fini, la propeiété est vraie (on pourra alors ici expliciter l'ensemble des caractères du groupe).
- Si on a un caractère d'un sous-groupe on peut le prolonguer en un caractère du groupe.
- Lemme technique.

Propriété (Cas du groupe cyclique). *Soit G un groupe cyclique de cardinal fini. Alors on a $|G| = |\widehat{G}|$.*

Démonstration. Soit $G = \langle g \rangle$ de cardinal n, soit $\chi \in \widehat{G}$. Pour déterminer χ, il nous faut calculer $\chi(g^k)$ pour $k \in \{0, \dots, n-1\}$:

$$\chi(g^k) = \chi(g)^k$$

En fait χ est entièrement déterminé par la valeur de $\chi(g)$, or

$$\chi(g)^n = \chi(g^n) = \chi(1) = 1$$

donc $\chi(g)$ est nécessairement une racine n-ième de l'unité d'où $|\widehat{G}| \leq n$. Réciproquement, pour $j \in \{0, \dots, n\}$, les applications $\chi_j : G \to \mathbb{C}^*$ définies pour tout $k \in \{0, \dots, n-1\}$ par $\chi_j(g^k) = \mathrm{e}^{\frac{2i\pi kj}{n}}$ sont des caractères de G. Donc $|\widehat{G}| = n = |G|$ □

Propriété (Prolongement de caractères). *Soit G un groupe abélien fini et H un sous-groupe de G. Tout caractère χ de H peut être prolongué en un caractère de G.*

Démonstration. On effectue une récurrence sur $[G : H]$.
Pour $[G : H] = 1$, on a $G = H$ donc la propriété est vraie.
On suppose que $[G : H] > 1$, il existe donc $x \in G$ tel que $x \notin H$. Soit $K = \langle x, H \rangle$ le groupe engendré par x et H. Soit m le plus petit entier non nul tel que $x^m \in H$, il existe car $x^n = 1 \in H$ où n et le cardinal de G. Comme G est abélien, tout éléments de K s'écrit sous la forme $z = yx^k$ avec $y \in H$ et $k \in \{0, \dots, m-1\}$. De plus, cette écriture est unique. En effet, si $yx^k = y'x^{k'}$ avec $0 \leq k \leq k' \leq m-1$ alors $x^{k-k'} = y'y^{-1} \in H$ or $k - k' < m$ donc $k = k'$ et $y = y'$.
Pour la suite, on procède par analyse sythèse :
Analyse : Supposon qu'il existe $\widetilde{\chi}$ un prolongement de χ. Posons $\zeta = \widetilde{\chi}(x)$. Il nous faut $\zeta^n = \widetilde{\chi}(x^n) = 1$, d'où ζ est une racine n-ième de l'unité et $\zeta^m = \widetilde{\chi}(x^m) = \chi(x^m)$. On a alors si $z \in K$ s'écrit $z = yx^k$ avec $y \in H$ et $k \in \{0, ..., m-1\}$:

$$\widetilde{\chi}(z) = \widetilde{\chi}(yx^k) = \chi(y)\zeta^k$$

Syntèse : Il existe $p \in \{0, \dots, |H| - 1\}$ tel que $\chi(x^m) = \mathrm{e}^{\frac{2i\pi p}{|H|}}$ d'où $\chi(x^m) = \mathrm{e}^{\frac{2i\pi p[G:H]}{n}}$ or $m | [G : H]$ car m est l'ordre de x dans G/H. On peut choisir ζ une racine n-ième de l'unité telle que $\chi(x^m) = \zeta^m$.

Définissons, pour $z \in K$ décomposé sous la forme $z = yx^k$, le prolongement $\widetilde{\chi}$ par $\widetilde{\chi}(z) = \chi(y)\zeta^k$. On doit montrer que $\widetilde{\chi}$ est un élément de $\widehat{K}$. L'unicité de la décomposition montre que $\widetilde{\chi}$ est bien définie. Pour prouver le fait que c'est bien un morphisme, on prend $z = yx^k$ et $z' = y'x^{k'}$ deux éléments de K, et on distingue deux cas :

- Si $0 \leq k + k' \leq m - 1$, on a

$$\widetilde{\chi}(zz') = \widetilde{\chi}(yy'x^{k+k'}) = \chi(yy')\zeta^{k+k'} = \chi(y)\zeta^k\chi(y')\zeta^{k'} = \widetilde{\chi}(z)\widetilde{\chi}(z')$$

- Si $m \leq k + k' \leq 2m - 1$, on a

$$\widetilde{\chi}(zz') = \widetilde{\chi}(yy'x^m x^{k+k'-m}) = \chi(y)\chi(y')\chi(x^m)\zeta^{k+k'-m} = \widetilde{\chi}(z)\widetilde{\chi}(z')$$

On a H sous-groupe de K et K sous-groupe de G donc $[G : H] = [G : K][K : H]$ et $[K : H] > 1$. On a donc $[G : K] < [G : H]$. On peut alors avec l'hypothèse de récurrence, prolonger $\widetilde{\chi}$ à G. □

Lemme. *Soit H un sous-groupe de G un groupe abélien fini. On note $\rho : \widehat{G} \to \widehat{H}$ le morphisme de restriction et $j : \widehat{G/H} \to \widehat{G}$ le morphisme d'extension, défini par :*

$$j : \begin{array}{ccc} \widehat{G/H} & \longrightarrow & \widehat{G} \\ \chi & \longmapsto & \widetilde{\chi} \end{array} \quad \text{avec } \widetilde{\chi}(x) := \chi(xH)$$

On a la suite exacte :

$$\{1\} \to \widehat{G/H} \overset{j}{\hookrightarrow} \widehat{G} \overset{\rho}{\twoheadrightarrow} \widehat{H} \to \{1\}$$

Ce qui donne $|\widehat{G}| = |\widehat{H}||\widehat{G/H}|$.

Démonstration. j est injective par définition, ρ est surjective d'après la propriété de prolongement des caractères.
Si on considère $\chi \in \ker(\rho)$, alors $H \subset \ker(\chi)$, et donc par la propriété universelle du quotient, il existe $\widetilde{\chi} \in \widehat{G/H}$ tel que $\widetilde{\chi}(x) = \chi(xH)$, c'est à dire $j(\widetilde{\chi}) = \chi$, donc $\ker(\rho) \subset \mathrm{Im}(j)$. Réciproquement, un élément de $\mathrm{Im}(j)$ est trivial sur H. Donc on a bien $\ker(\rho) = \mathrm{Im}(j)$.
On définit :

$$\widetilde{\rho} : \begin{array}{ccc} \widehat{G}/j(\widehat{G/H}) & \longrightarrow & \widehat{H} \\ \chi j(\widehat{G/H}) & \longmapsto & \rho(\chi) \end{array}$$

$\widetilde{\rho}$ est bien défini par exactitude de la suite, elle est surjective car ρ est surjective et est injective car $\ker(\rho) = j(\widehat{G/H})$, donc elle est bijective et on a $|\widehat{G}| = |\widehat{H}||\widehat{G/H}|$. □

On peut mainetant démontrer la propriété énoncé.

Démonstration. On raisonne par récurrence sur $n = |G|$.
Pour $n = 1$, le résultat est trivial car $\widehat{G} = \{1\}$, où 1 est le caractère triviale.
On suppose $n \geq 2$, il existe un groupe cyclique non triviale $H \subset G$. Si $H = G$, le résultat est vrai d'après la propriété sur le cas cyclique. Sinon avec l'hypothèse de récurrence, on a $|H| = |\widehat{H}|$ et $|G/H| = |\widehat{G/H}|$, et le lemme nous dit que $|\widehat{G}| = |\widehat{H}||\widehat{G/H}|$. Donc on a $|\widehat{G}| = |H||G/H| = |G|$. □

Commentaire : Attention pour la démonstration du prolongement des carctères faite dans G.Peyré, il dit que $\zeta^m = \chi(x^m) = \chi(1) = 1$ ce qui est faux.