110

CARACTÈRES D'UN GROUPE ABÉLIEN FINI ET TRANSFORMÉE DE FOURIER DISCRÈTE. APPLICATIONS.

Cadre : $(G,+)$ est un groupe abélien fini.

I - CARACTÈRES ET DUALITÉ

1. Définitions et premières propriétés

Déf 1 : . On appelle caractère de G tout morphisme $\chi : G \to \mathbb{C}^*$.
. On appelle dual de G, et on note $\widehat{G}$, l'ensemble des caractères de G.

ex

Prop 2 : Pour tous $\chi \in \widehat{G}$ et $g \in G$, $\chi(g) \in \langle e^{2i\pi/n} \rangle$ où $n = |G|$.
En particulier $|\chi(g)| = 1$ et $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$.

Déf-Prop 3 : On munit $\widehat{G}$ de la loi $\cdot$ définie par
$$\forall \chi_1, \chi_2 \in \widehat{G}, \ \chi_1 \cdot \chi_2 : g \in G \mapsto \chi_1(g)\chi_2(g)$$
Pour cette loi, $\widehat{G}$ est un groupe abélien fini et $\forall \chi \in \widehat{G}, \chi^{-1} = \overline{\chi}$.

Prop 4 : Si G est un groupe cyclique d'ordre n engendré par un élément g, alors l'application $\left| \begin{array}{l} \mathbb{Z} \to \widehat{G} \\ k \mapsto \chi_k : jg \mapsto e^{\frac{2ijk\pi}{n}} \end{array} \right.$ se factorise en un isomorphisme $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \widehat{G}$.
En particulier $\widehat{G} \cong G$. (ex)

Ex 5 : Tables de caractères de $\mathbb{Z}/3\mathbb{Z}$ et $(\mathbb{Z}/5\mathbb{Z})^\times$. (cf Annexe)

2. Quelques isomorphismes

Th 6 : (Lemme de prolongement)
Si H est un sous-groupe de G, alors le morphisme $\left| \begin{array}{l} \widehat{G} \to \widehat{H} \\ \chi \mapsto \chi_{|H} \end{array} \right.$ est surjectif.

DVPT ①

Th 7 : (Théorème de structure des groupes abéliens finis)
Si G est non trivial, alors il existe une unique suite finie $(m_1, \dots, m_r)$ d'entiers ≥ 2 telle que $m_r | \dots | m_1$ et
$$G \cong \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$$

app / ex

Déf-Prop 8 : Si H est un sous-groupe de G, on appelle orthogonal de H, et on note $H^\perp$, $H^\perp = \{\chi \in \widehat{G} \mid \forall h \in H, \chi(h) = 1\}$.
$H^\perp$ est un sous-groupe de $\widehat{G}$.

Prop 9 : Soit H un sous-groupe de G. Considérons les morphismes $i : \left| \begin{array}{l} \widehat{G/H} \to \widehat{G} \\ \chi \mapsto \chi \circ \pi \end{array} \right.$ où $\pi : G \to G/H$ projection canonique et $p : \left| \begin{array}{l} \widehat{G} \to \widehat{H} \\ \chi \mapsto \chi_{|H} \end{array} \right.$.

ex

Alors la suite $1 \to \widehat{G/H} \xrightarrow{i} \widehat{G} \xrightarrow{p} \widehat{H} \to 1$ est exacte,
$\widehat{G/H} \cong H^\perp$ et $\widehat{G}/H^\perp \cong \widehat{H}$.

Cor 10 : $|\widehat{G}| = |G|$

ex

Appli 11 : Si $g \in G$ est d'ordre r, alors pour tout $\omega \in \langle e^{2i\pi/r} \rangle$,
$$|\{\chi \in \widehat{G} \mid \chi(g) = \omega\}| = \frac{|G|}{r}$$
En particulier, on a $\prod_{\chi \in \widehat{G}} (1 - \chi(g)T) = (1 - T^r)^{|G|/r}$ dans $\mathbb{C}[T]$.

ex

Prop 12 : Si G_1 et G_2 sont deux groupes abéliens finis, alors
$\left| \begin{array}{l} \widehat{G_1} \times \widehat{G_2} \longrightarrow \widehat{G_1 \times G_2} \\ (\chi_1, \chi_2) \longmapsto ((g_1, g_2) \mapsto \chi_1(g_1)\chi_2(g_2)) \end{array} \right.$ est un isomorphisme. (ex)

Ex 13 Table de caractères de $(\mathbb{Z}/15\mathbb{Z})^\times$. (cf Annexe)

Cor 14 : $\widehat{G} \cong G$

Rem 15 : Cet isomorphisme n'est pas canonique → ex

Prop 16 : On a un isomorphisme canonique $\left| \begin{array}{l} G \xrightarrow{\sim} \widehat{\widehat{G}} \\ g \longmapsto (\chi \mapsto \chi(g)) \end{array} \right.$

ex

II - L'ALGÈBRE $\mathbb{C}[G]$

1. Définitions et premières propriétés

Déf-Prop 17 : On note $\mathbb{C}[G]$ le $\mathbb{C}$-espace vectoriel des fonctions de G dans $\mathbb{C}$.
On le munit du produit scalaire hermitien défini par
$$\forall f_1, f_2 \in \mathbb{C}[G], \ \langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{f_1(g)} f_2(g)$$

ex

Déf-Prop 18 : Pour tout $g \in G$, notons $\delta_g : x \in G \mapsto \begin{cases} 1 & \text{si } x = g \\ 0 & \text{sinon} \end{cases} \in \mathbb{C}[G]$.
Alors $(\delta_g)_{g \in G}$ est une base orthogonale de $\mathbb{C}[G]$ et
$$\forall f \in \mathbb{C}[G], \ f = \sum_{g \in G} f(g)\delta_g$$

ex

Cor 19 : $\dim \mathbb{C}[G] = |G|$

Prop 20 : La loi $\cdot$ définie par $\forall f_1, f_2 \in \mathbb{C}[G], f_1 \cdot f_2 : g \in G \mapsto f_1(g) f_2(g)$ munit $\mathbb{C}[G]$ d'une structure d'algèbre commutative.

Rem 21 : Cette multiplication ne prend pas en compte la structure de groupe de G. On est donc amené à définir une nouvelle multiplication : la convolution → ex ?

Déf-Prop 22 : . La loi de composition $*$ définie sur $\{\delta_g \mid g \in G\}$ par
$\forall g_1, g_2 \in G, \ \delta_{g_1} * \delta_{g_2} = \delta_{g_1 + g_2}$ munit $\{\delta_g \mid g \in G\}$ d'une structure de groupe pour laquelle l'application canonique $G \to \{\delta_g \mid g \in G\}$ est un morphisme.

ex

- L'unique loi, encore notée $*$, qui prolonge $*$ par bilinéarité à $\mathbb{C}[G]$, munit $\mathbb{C}[G]$ d'une structure d'algèbre commutative.
On a $\forall f_1, f_2 \in \mathbb{C}[G]$, $f_1 * f_2 : g \in G \mapsto \sum_{h\in G} f_1(h) f_2(g-h)$

Prop23 : Si χ est un caractère de G, alors il existe un unique morphisme d'algèbres $\tilde{\chi} : (\mathbb{C}[G], *) \to \mathbb{C}$ qui prolonge χ.

2. Quelques relations d'orthogonalité

Th24 : $\widehat{G}$ forme une base orthonormée de $\mathbb{C}[G]$. (ex)

Rem25 : En particulier, les lignes de la table de caractères de G forment une base orthogonale de $\mathbb{C}^{|G|}$ muni de son produit scalaire usuel.

Cor26 : $\forall g_1, g_2 \in G$, $\frac{1}{|G|} \sum_{\chi\in\widehat{G}} \overline{\chi(g_1)}\chi(g_2) = \begin{cases} 1 & \text{si } g_1 = g_2 \\ 0 & \text{sinon} \end{cases}$

Rem27 : En particulier, les colonnes de la table de caractères de G forment une base orthogonale de $\mathbb{C}^{|G|}$ muni de son produit scalaire usuel. (App°)

III - TRANSFORMÉE DE FOURIER

1. Généralités

Déf28 : On appelle transformée de Fourier sur G l'application $\mathcal{F} : \begin{vmatrix} \mathbb{C}[G] \to \mathbb{C}[\widehat{G}] \\ f \mapsto \widehat{f} \end{vmatrix}$ où $\widehat{f}$ est définie par $\forall \chi\in\widehat{G}$, $\widehat{f}(\chi) = |G|\langle \overline{\chi}, f\rangle = \sum_{g\in G} f(g)\chi(g)$
(ex)

Prop29 : (Formule d'inversion)
$\forall f \in \mathbb{C}[G]$, $f = \frac{1}{|G|}\sum_{\chi\in\widehat{G}} \widehat{f}(\chi)\overline{\chi}$ (ex)

Th30 : $\mathcal{F}$ réalise un isomorphisme d'algèbres de $(\mathbb{C}[G], *)$ vers $(\mathbb{C}[\widehat{G}], \cdot)$.

Prop31 : (Formule de Plancherel)
$\forall f_1, f_2 \in \mathbb{C}[G]$, $\langle f_1, f_2\rangle = \frac{1}{|G|}\langle \widehat{f_1}, \widehat{f_2}\rangle$ (ex)
En particulier, $\forall f \in \mathbb{C}[G]$, $\|f\|^2 = \frac{1}{|G|}\|\widehat{f}\|^2$.

Appli32 : Si $\mathbb{P}$ est une mesure de probabilité sur $(G, \mathcal{P}(G))$, alors $\forall g\in G$, $\left|\mathbb{P}(g) - \frac{1}{|G|}\right|^2 \leq \frac{1}{|G|}\sum_{\chi\neq\chi_0} |\widehat{P}(\chi)|^2$ où $P : g \mapsto \mathbb{P}(g)$ et χ_0 est le caractère trivial.

Appli33 : (Formule de Poisson)
Si H est un sous-groupe de G et $f \in \mathbb{C}[G]$, alors
$\forall g\in G$, $\sum_{h\in H} f(g+h) = \frac{|H|}{|G|}\sum_{\chi\in H^\perp} \widehat{f}(\chi)\overline{\chi}(g)$

2. Transformée de Fourier discrète

Déf34 : Si $N\geq 1$ et $f = (f[n])_{n\in[\![0,N-1]\!]} \in \mathbb{C}^N$, on appelle transformée de Fourier discrète de f le vecteur $\widehat{f} = (\widehat{f}[n])_{n\in[\![0,N-1]\!]}$ défini par
$\forall n\in[\![0,N-1]\!]$, $\widehat{f}[n] = \sum_{k=0}^{N-1} f[k] e^{-2ikn\pi/N}$
ex de calcul linéaire

Prop35 : Si $N\geq 1$ et $f = (f[n]) \in \mathbb{C}^N$, alors $\forall n\in[\![0,N-1]\!]$, $\widehat{f}[n] = \widehat{f_0}(\chi_n)$
où $f_0 : \begin{vmatrix} \mathbb{Z}/N\mathbb{Z} \to \mathbb{C} \\ k+N\mathbb{Z} \mapsto f[k \bmod N] \end{vmatrix}$ et $\chi_n : \begin{vmatrix} \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{C}^* \\ k+N\mathbb{Z} \longmapsto \exp\left(\frac{-2ikn\pi}{N}\right) \end{vmatrix}$

Prop36 : Soit $N\geq 1$.
- (Formule d'inversion) $\forall f\in\mathbb{C}^N$, $\forall k\in[\![0,N-1]\!]$, $f[k] = \frac{1}{N}\sum_{n=0}^{N-1}\widehat{f}[n]e^{\frac{2ikn\pi}{N}}$
- (Formule de Plancherel) $\forall f_1, f_2\in\mathbb{C}^N$, $\langle f_1, f_2\rangle = \frac{1}{N}\langle\widehat{f_1}, \widehat{f_2}\rangle$
où $\langle\cdot,\cdot\rangle$ est le produit scalaire usuel sur $\mathbb{C}^N$.

Déf-Prop37 : Soit $N\geq 1$. Les lois $\cdot$ et $*$ définies sur $\mathbb{C}^N$ par
$\forall f_1, f_2\in\mathbb{C}^N$, $f_1 \cdot f_2 = (f_1[n]f_2[n])$ et $f_1 * f_2 = \left(\sum_{k=0}^{N-1} f_1[k] f_2[N-k \bmod N]\right)$
munissent $\mathbb{C}^N$ d'une structure d'algèbre commutative.

Prop38 : $\mathcal{F} : f\mapsto\widehat{f}$ réalise un isomorphisme d'algèbres de $(\mathbb{C}^N, *)$ vers $(\mathbb{C}^N, \cdot)$.

Appli39 : (Systèmes circulants)
Soient $C = \begin{pmatrix} c_0 & c_1 & \cdots & c_{N-1} \\ c_{N-1} & c_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & c_1 \\ c_1 & \cdots & c_{N-1} & c_0 \end{pmatrix}$ une matrice circulante et c son premier vecteur colonne. (ex)

Alors C est inversible ssi $\forall n\in[\![0,N-1]\!]$, $\widehat{c}[n]\neq 0$. Dans ce cas, pour tout $b\in\mathbb{C}^N$, l'unique solution de $Cx = b$ est donnée par $x = \mathcal{F}^{-1}\left(\left(\frac{\widehat{b}[n]}{\widehat{c}[n]}\right)\right)$

Algo40 : (Transformée de Fourier rapide)
Supposons que N est une puissance de 2. Soit $f\in\mathbb{C}^N$.
- On calcule récursivement $\widehat{f^0}$ et $\widehat{f^1}$ où $f^0 = (f[2n])_{n\in[\![0,N/2-1]\!]}$ et $f^1 \in (f[2n+1])_{n\in[\![0,N/2-1]\!]}$
- On calcule $S\widehat{f^1} = (e^{-2in\pi/N}\widehat{f^1}[n])_{n\in[\![0,N/2-1]\!]}$.
- On a $\widehat{f} = \begin{pmatrix} \widehat{f^0} + S\widehat{f^1} \\ \widehat{f^0} - S\widehat{f^1} \end{pmatrix}$.

en de calcul

Prop41 : La transformée de Fourier rapide permet de calculer la transformée de Fourier discrète en $O(N\log N)$ opérations, alors que le calcul naïf de la transformée de Fourier discrète nécessite $O(N^2)$ opérations.

Rem42 : La transformée de Fourier rapide permet aussi de calculer la transformée de Fourier inverse via la formule

$$\forall f \in \mathbb{C}^N,\ \mathcal{F}^{-1}(f) = \widehat{f_0} \quad \text{où} \quad f_0 = \left(\tfrac{1}{N} f[N-n \bmod N]\right)_{n \in [\![0, N-1]\!]}.$$

Rem43 : Si N est pair et $N/2$ est impair, on peut calculer $\hat{f}$ en calculant naïvement $\hat{f}^0$ et $\hat{f}^1$.

Appli44 : (Multiplication de polynômes)

Soient N une puissance de 2, A, B deux polynômes de degré $\leq N-1$ et $C = AB$. On note a (resp. b, c) $\in \mathbb{C}^{2N}$ le vecteur formé des coefficients de A (resp. B, C), complété avec des zéros.

- On calcule $\hat{a}$ et $\hat{b}$ par transformée de Fourier rapide.
- On calcule $\hat{a} \cdot \hat{b}$.
- On calcule $c = \mathcal{F}^{-1}(\hat{a} \cdot \hat{b})$ par transformée de Fourier rapide.

On obtient ainsi un algorithme de multiplication de polynômes en $O(N \log N)$ opérations, alors que l'algorithme naïf nécessite $O(N^2)$ opérations.

IV - APPLICATIONS AUX CORPS FINIS

ea

Soient p un nombre premier et $q = p^n$.

1. Caractères additifs et multiplicatifs

DéF45 : On appelle caractères additifs de $\mathbb{F}_q$ les éléments de $\widehat{\mathbb{F}_q}$. ea

DéF-Prop46 : Pour $x \in \mathbb{F}_q$, on appelle trace de x et on note $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)$ la trace de l'application $m_x : \left| \begin{array}{l} \mathbb{F}_q \to \mathbb{F}_q \\ y \mapsto xy \end{array} \right.$.

C'est une forme $\mathbb{F}_p$-linéaire non nulle sur $\mathbb{F}_q$, et

$$\forall x \in \mathbb{F}_q,\ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) = \sum_{k=0}^{n-1} x^{p^k}$$

ea

Prop47 : L'application $\left| \begin{array}{l} \mathbb{F}_q \longrightarrow \widehat{\mathbb{F}_q} \\ a \longmapsto \psi_a : x \mapsto e^{2i\pi \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)/p} \end{array} \right.$ app ?

est un isomorphisme de groupes.

DéF-Prop48 : On appelle caractères multiplicatifs de $\mathbb{F}_q$ les éléments de $\widehat{\mathbb{F}_q^\times}$.

L'application $\left| \begin{array}{l} \mathbb{Z} \longrightarrow \widehat{\mathbb{F}_q^\times} \\ k \longmapsto \chi_k : \zeta^j \mapsto e^{2ijk\pi/(q-1)} \end{array} \right.$, où ζ est un générateur de $\mathbb{F}_q^\times$

se factorise en un isomorphisme $\mathbb{Z}/(q-1)\mathbb{Z} \xrightarrow{\sim} \widehat{\mathbb{F}_q^\times}$.

Ex49 : L'application $\eta : x \in \mathbb{F}_q^\times \mapsto \begin{cases} 1 & \text{si } x \text{ est un carré} \\ -1 & \text{sinon} \end{cases}$

est un caractère multiplicatif de $\mathbb{F}_q$.

On a même $\eta = \begin{cases} \chi_0 & \text{si } p = 2 \\ \chi_{(q-1)/2} & \text{si } p \geq 3 \end{cases}$.

Dans le cas où q est premier impair, η coïncide avec le symbole de Legendre.

2. Sommes de Gauss

DéF-Prop50 : Si $\psi \in \widehat{\mathbb{F}_q}$ et $\chi \in \widehat{\mathbb{F}_q^\times}$, on appelle somme de Gauss associée à ces caractères $\quad G(\chi, \psi) = \sum_{x \in \mathbb{F}_q^\times} \chi(x) \psi(x)$

On a $G(\chi, \psi) = \widehat{\psi_{|\mathbb{F}_q^\times}}(\chi)$ et $G(\chi, \psi) = \hat{\tilde{\chi}}(\psi)$ où $\tilde{\chi} \in \mathbb{C}[\mathbb{F}_q]$ prolonge χ et vérifie $\tilde{\chi}(0) = 0$.

Prop51 : Soient $\psi \in \widehat{\mathbb{F}_q}$ et $\chi \in \widehat{\mathbb{F}_q^\times}$.

- $\forall a \in \mathbb{F}_q^\times, \forall b \in \mathbb{F}_q,\ G(\chi, \psi_{ab}) = \overline{\chi(a)}\, G(\chi, \psi_b)$
- $G(\chi, \bar{\psi}) = \chi(-1)\, G(\chi, \psi)$
- $G(\bar{\chi}, \psi) = \chi(-1)\, \overline{G(\chi, \psi)}$
- $G(\chi, \psi) = \begin{cases} q-1 & \text{si } \chi = \chi_0 \text{ et } \psi = \psi_0 \\ -1 & \text{si } \chi = \chi_0 \text{ et } \psi \neq \psi_0 \\ 0 & \text{si } \chi \neq \chi_0 \text{ et } \psi = \psi_0 \end{cases}$

Dans les autres cas, $|G(\chi, \psi)| = \sqrt{q}$.

Appli52 : (Sommes quadratiques de Gauss)

Supposons p impair et $q = p$.

Pour $a \in \mathbb{F}_p$, on pose $G(a) = G(\eta, \psi_a) = \sum_{k=0}^{p-1} \left(\frac{k}{p}\right) e^{2iak\pi/p}$

où η désigne le symbole de Legendre.

On a :
- $\forall a \in \mathbb{F}_p,\ G(a) = \sum_{k=0}^{p-1} e^{2iak^2\pi/p}$
- $\forall a \in \mathbb{F}_p^\times,\ G(a) = \left(\frac{a}{p}\right) G(1)$
- $G(1)^2 = (-1)^{(p-1)/2}\, p$

ea

Appli53 : (Nombre de vecteurs isotropes d'une forme quadratique non dégénérée sur $\mathbb{F}_p^n$)

Supposons p impair. Soit q une forme quadratique non dégénérée sur $\mathbb{F}_p^n$. Alors le nombre de vecteurs isotropes de q vaut

$$p^{n-1} + \varepsilon (p-1) p^{\frac{n}{2}-1} \quad \text{où} \quad \varepsilon = \begin{cases} 0 & \text{si } n \text{ est impair} \\ \left(\frac{(-1)^{n/2} \operatorname{disc}(q)}{p}\right) & \text{si } n \text{ est pair} \end{cases}$$

Appli54 : (Loi de réciprocité quadratique)

Soient p et q premiers impairs distincts.

Alors $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}}$ et $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

DVPT ②

ea

ANNEXE

- Table de caractères de $\mathbb{Z}/3\mathbb{Z}$

$\mathbb{Z}/3\mathbb{Z}$	0	1	2
χ_0	1	1	1
χ_1	1	j	j^2
χ_2	1	j^2	j

- Table de caractères de $(\mathbb{Z}/5\mathbb{Z})^\times$

$(\mathbb{Z}/5\mathbb{Z})^\times$	1	2	3	4
χ_0	1	1	1	1
χ_1	1	i	$-i$	-1
χ_2	1	-1	-1	1
χ_3	1	$-i$	i	-1

- Table de caractères de $(\mathbb{Z}/15\mathbb{Z})^\times$

$(\mathbb{Z}/15\mathbb{Z})^\times$	1	2	4	7	8	11	13	14
χ_0	1	1	1	1	1	1	1	1
χ_1	1	i	-1	i	$-i$	1	$-i$	-1
χ_2	1	-1	1	-1	-1	1	-1	1
χ_3	1	$-i$	-1	$-i$	i	1	i	-1
χ_4	1	-1	1	1	-1	-1	1	-1
χ_5	1	$-i$	-1	i	i	-1	$-i$	1
χ_6	1	1	1	-1	1	-1	-1	-1
χ_7	1	i	-1	$-i$	$-i$	-1	i	1

RÉFÉRENCES

- L'algèbre discrète de la transformée de Fourier - Peyré
- Arithmétique - Hindry

THÉORÈME DE STRUCTURE DES GROUPES ABÉLIENS FINIS

<u>Théorème.</u> Si G est un groupe abélien fini et H est un sous-groupe de G, alors le morphisme $\begin{array}{rcl}\hat{G} & \longrightarrow & \hat{H} \\ \chi & \longmapsto & \chi_{|H}\end{array}$ est surjectif.

<u>Preuve.</u> Soit G un groupe abélien fini.
Raisonnons par l'absurde et considérons un sous-groupe H de G d'ordre maximal tel que $\begin{array}{rcl}\hat{G} & \rightarrow & \hat{H} \\ \chi & \mapsto & \chi_{|H}\end{array}$ n'est pas surjectif.

Alors il existe $x \in G \setminus H$ et notons $n = o(x+H)$ dans G/H et $K = \langle H, x\rangle$.
Soit $\varphi \in \hat{H}$.
Considérons une racine n-ième $\rho \in \mathbb{C}^*$ de $\varphi(nx)$ et $\begin{array}{rcl}\chi : K & \longrightarrow & \mathbb{C}^* \\ mx+h & \mapsto & \rho^m \varphi(h)\end{array}$

Si $mx+h = m'x+h'$ avec $m,m' \in \mathbb{Z}$ et $h,h' \in H$, alors $(m-m')x = h'-h \in H$ et donc $n \mid m-m'$ et $\dfrac{\rho^m \varphi(h)}{\rho^{m'}\varphi(h')} = (\rho^n)^{\frac{m-m'}{n}} \varphi(h-h') = \varphi((m-m')x+h-h') = 1$, ce qui prouve que χ est bien défini.
De plus, χ est un caractère de K qui prolonge φ.
Ainsi tout caractère de H se prolonge en un caractère de G. Absurde.

<u>Théorème.</u> Si G est un groupe abélien fini non trivial, alors il existe une unique suite finie $(m_1, \dots, m_r)$ d'entiers ≥ 2 telle que $m_r \mid \dots \mid m_1$ et $G \simeq \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$.

<u>Preuve.</u>
<u>Etape 1</u>: Existence
Raisonnons par récurrence sur $n = |G|$.
* Immédiat pour $n=2$.
* Soit $n \geq 3$. Supposons le résultat vrai pour tout $k \leq n-1$.
Soit G un groupe abélien d'ordre n.
Alors il existe $x \in G$ d'ordre l'exposant m de G et considérons $\begin{array}{rcl}\varphi : \langle x\rangle & \longrightarrow & \mathbb{C}^* \\ kx & \longmapsto & e^{\frac{2ik\pi}{m}}\end{array}$.

D'après le lemme, φ se prolonge en un caractère χ de G.
- Si $g \in G$, alors $\chi(g)^m = 1$ et donc $\chi(g) \in \langle e^{\frac{2i\pi}{m}}\rangle = \chi(\langle x\rangle)$.
Ainsi $G = \ker(\chi) + \langle x\rangle$.
- Par ailleurs, $\ker(\chi) \cap \langle x\rangle = \ker(\varphi) = \{0\}$.

Donc $G = \ker(\chi) \oplus \langle x\rangle \simeq \ker(\chi) \times \mathbb{Z}/m\mathbb{Z}$.

Étape 2 : Unicité

- Pour tous $n \geq 1$ et $d \in \mathbb{Z}$, $\{x \in \mathbb{Z}/n\mathbb{Z},\ dx = 0\} = \dfrac{\frac{n}{n \wedge d}\mathbb{Z}}{n\mathbb{Z}}$.

- Supposons qu'il existe une suite finie $(n_1, \dots, n_s) \neq (m_1, \dots, m_r)$ vérifiant les conditions du théorème.

On peut supposer $r \geq s$.

Alors $|\{x \in G,\ m_r x = 0\}| = \begin{cases} m_r^r \\ \prod_{i=1}^{s} (m_r \wedge n_i) \leq m_r^s \end{cases}$ et donc $r = s$.

Sit $k \geq 1$ maximal tel que $m_k \neq n_k$.

Alors $|\{x \in G,\ m_k x = 0\}| = \begin{cases} m_k^k \times \prod_{i=k+1}^{r} m_i \\ \prod_{i=1}^{k} (m_k \wedge n_i) \times \prod_{i=k+1}^{r} m_i \end{cases}$ et donc $m_k^k = \prod_{i=1}^{k} (m_k \wedge n_i)$.

Ainsi $m_k | n_k$ et par symétrie, $m_k = n_k$. Absurde.

Loi de réciprocité quadratique

Soient p, q deux nombres premiers impairs distincts, $\zeta = e^{2i\pi/p}$ et $\xi = e^{2i\pi/8}$.

Définition : . On appelle somme de Gauss relative à p : $G_p = \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) \zeta^a$.

. On appelle somme de Gauss relative à 2 : $G_2 = \xi + \xi^{-1} = \sqrt{2}$.

Proposition : $G_p^2 = (-1)^{\frac{p-1}{2}} p$

Démonstration :

$$G_p^2 = \sum_{a,b \in \mathbb{F}_p} \left(\frac{ab}{p}\right) \zeta^{a+b} \underset{b=at}{=} \sum_{a,t \in \mathbb{F}_p} \left(\frac{a^2 t}{p}\right) \zeta^{(1+t)a} \underset{\left(\frac{a^2t}{p}\right) = \left(\frac{t}{p}\right) \text{ si } a \neq 0}{=} \sum_{t \in \mathbb{F}_p^\times} \left(\frac{t}{p}\right) \sum_{a \in \mathbb{F}_p^\times} \zeta^{(1+t)a}$$

d'où $G_p^2 = \left(\frac{-1}{p}\right)(p-1) + \sum_{t \in \mathbb{F}_p^\times \setminus \{-1\}} \left(\frac{t}{p}\right) \sum_{a \in \mathbb{F}_p^\times} \zeta^{(1+t)a}$

Or si $t \neq -1$, $\left| \begin{array}{l} \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times \\ a \longmapsto (1+t)a \end{array} \right.$ est une bijection, donc $\sum_{a \in \mathbb{F}_p^\times} \zeta^{(1+t)a} = \sum_{a \in \mathbb{F}_p^\times} \zeta^a = -1$

donc $G_p^2 = \left(\frac{-1}{p}\right)(p-1) - \Big[\underbrace{\sum_{t \in \mathbb{F}_p^\times} \left(\frac{t}{p}\right)}_{=0} - \left(\frac{-1}{p}\right) \Big]$

donc $G_p^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p$.

Théorème : $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) (-1)^{\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}}$

Démonstration :

. D'une part, $G_p^q = \left(\sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) \zeta^a \right)^q \equiv \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) \zeta^{aq} \mod q\overline{\mathbb{Z}}$

d'où $G_p^q \equiv \sum_{a \in \mathbb{F}_p} \left(\frac{q}{p}\right)\left(\frac{aq}{p}\right) \zeta^{aq} \equiv \left(\frac{q}{p}\right) \sum_{b \in \mathbb{F}_p} \left(\frac{b}{p}\right) \zeta^b \equiv \left(\frac{q}{p}\right) G_p \mod q\overline{\mathbb{Z}}$.

. D'autre part $G_p^q = (G_p^2)^{\frac{q-1}{2}} G_p = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}} p^{\frac{q-1}{2}} G$.

Par le critère d'Euler, $G_p^q \equiv (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}} \left(\frac{p}{q}\right) G \mod q\overline{\mathbb{Z}}$.

. On a donc $(-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}} \left(\frac{p}{q}\right) G_p \equiv \left(\frac{q}{p}\right) G_p \mod q\overline{\mathbb{Z}}$

d'où, en multipliant par $(-1)^{\frac{p-1}{2}} G_p$, $(-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}} \left(\frac{p}{q}\right) p \equiv \left(\frac{q}{p}\right) p \mod q\mathbb{Z}$.

Or $p \in \mathbb{F}_q^\times$ et $q \neq 2$, donc $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$.

Théorème : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Démonstration :

- D'une part, $G_2^p = (\xi + \xi^{-1})^p \equiv \xi^p + \xi^{-p} \mod p\overline{\mathbb{Z}}$.
  - Si $p \equiv 1$ ou $7 \mod 8$, $G_2^p \equiv \xi + \xi^{-1} \equiv G_2 \mod p\overline{\mathbb{Z}}$
  - Si $p \equiv 3$ ou $5 \mod 8$, $G_2^p \equiv \xi^5 + \xi^{-5} \equiv -(\xi + \xi^{-1}) \equiv -G_2 \mod p\overline{\mathbb{Z}}$

    car $\xi^4 = -1$.

  Donc $G_2^p \equiv (-1)^{\frac{p^2-1}{8}} G_2 \mod p\overline{\mathbb{Z}}$.

- D'autre part, selon le critère d'Euler,

$$G_2^p = (G_2^2)^{\frac{p-1}{2}} G_2 = 2^{\frac{p-1}{2}} G_2 \equiv \left(\frac{2}{p}\right) G_2 \mod p\overline{\mathbb{Z}}$$

- On a donc $\left(\frac{2}{p}\right) G_2 \equiv (-1)^{\frac{p^2-1}{8}} G_2 \mod p\overline{\mathbb{Z}}$.

  En multipliant par G_2, et comme $p \neq 2$, on obtient $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.