

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  $\chi : G \rightarrow \mathbb{C}^*$ .

On appelle dual de  $G$ , et on note  $\hat{G}$ , l'ensemble des caractères de  $G$ .

**Prop 2 :** Pour tous  $\chi \in \hat{G}$  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  $\hat{G}$  de la loi  $\cdot$  définie par

$$\forall \chi_1, \chi_2 \in \hat{G}, \chi_1 \cdot \chi_2 : g \in G \mapsto \chi_1(g) \chi_2(g)$$

Pour cette loi,  $\hat{G}$  est un groupe abélien fini et  $\forall \chi \in \hat{G}, \chi^{-1} = \overline{\chi}$ .

**Prop 4 :** Si  $G$  est un groupe cyclique d'ordre  $n$  engendré par un élément  $g$ , alors l'application  $\mathbb{Z} \rightarrow \hat{G}$

$$k \mapsto \chi_k : jg \mapsto e^{\frac{2ij\pi}{n}}$$

se factorise en un isomorphisme  $\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \hat{G}$ .

En particulier  $\hat{G} \cong G$ . *ea*

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

### 2. Quelques isomorphismes

**Th 6 :** (Lemme de prolongement)

Si  $H$  est un sous-groupe de  $G$ , alors le morphisme

$$\begin{aligned} \hat{G} &\rightarrow \hat{H} \\ \chi &\mapsto \chi|_H \end{aligned}$$

DVPT  
④

**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  $\geq 2$  telle que  $m_1 \dots m_r = |G|$  et

$$G \cong \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \dots \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$$

*app / ea*

**Déf-Prop 8 :** Si  $H$  est un sous-groupe de  $G$ , on appelle orthogonal de  $H$ , et on note  $H^\perp$ ,

$$H^\perp = \{ \chi \in \hat{G} \mid \forall h \in H, \chi(h) = 1 \}$$

$H^\perp$  est un sous-groupe de  $\hat{G}$ .

**Prop 9 :** Soit  $H$  un sous-groupe de  $G$ . Considérons les morphismes

$$i : \hat{G}/H \rightarrow \hat{G} \quad \text{où } \pi : G \rightarrow G/H \text{ projection canonique et } P : \hat{G} \rightarrow \hat{H}$$

*ea*

Alors la suite  $1 \rightarrow \hat{G}/H \xrightarrow{i} \hat{G} \xrightarrow{P} \hat{H} \rightarrow 1$  est exacte,  $\hat{G}/H \cong H^\perp$  et  $\hat{G}/H^\perp \cong \hat{H}$ .

**Cor 10 :**  $|\hat{G}| = |G|$

**App 11 :** Si  $g \in G$  est d'ordre  $r$ , alors pour tout  $\omega \in \langle e^{2i\pi/r} \rangle$ ,

$$|\{ \chi \in \hat{G} \mid \chi(g) = \omega \}| = \frac{|G|}{r}$$

En particulier, on a  $\prod_{\chi \in \hat{G}} (1 - \chi(g)T) = (1 - T^r)^{|G|/r}$  dans  $\mathbb{C}[T]$ .

**Prop 12 :** Si  $G_1$  et  $G_2$  sont deux groupes abéliens finis, alors

$$\begin{aligned} \hat{G}_1 \times \hat{G}_2 &\rightarrow \widehat{G_1 \times G_2} && \text{est un isomorphisme.} \\ (\chi_1, \chi_2) &\mapsto ((g_1, g_2) \mapsto \chi_1(g_1) \chi_2(g_2)) \end{aligned}$$

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

**Cor 14 :**  $\hat{G} \cong G$

**Rem 15 :** Cet isomorphisme n'est pas canonique. *ea*

**Prop 16 :** On a un isomorphisme canonique  $\mathbb{Z} \xrightarrow{\sim} \hat{G}$

## 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

$$\forall f_1, f_2 \in \mathbb{C}[G], \langle f_1, f_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \overline{f_1(g)} f_2(g)$$

*ea*

**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

$$\forall f \in \mathbb{C}[G], f = \sum_{g \in G} f(g) \delta_g$$

**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  $\rightarrow$  *ea*

**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  $G \rightarrow \{ \delta_g \mid g \in G \}$  est un morphisme.

• 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  $\forall f_1, f_2 \in \mathbb{C}[G], f_1 * f_2 : g \in G \mapsto \sum_{h \in G} f_1(h) f_2(g-h)$

Prop 23: Si  $\chi$  est un caractère de  $G$ , alors il existe un unique morphisme d'algèbres  $\tilde{\chi} : (\mathbb{C}[G], *) \rightarrow \mathbb{C}$  qui prolonge  $\chi$ .

## 2. Quelques relations d'orthogonalité

Th 24:  $\hat{G}$  forme une base orthonormée de  $\mathbb{C}[G]$ . *(en)*

Rem 25: En particulier, les lignes de la table de caractères de  $G$  forment une base orthogonale de  $\mathbb{C}^{G^1}$  muni de son produit scalaire usuel.

Cor 26:  $\forall g_1, g_2 \in G, \frac{1}{|G|} \sum_{\chi \in \hat{G}} \overline{\chi(g_1)} \chi(g_2) = \begin{cases} 1 & \text{si } g_1 = g_2 \\ 0 & \text{sinon} \end{cases}$

Rem 27: En particulier, les colonnes de la table de caractères de  $G$  forment une base orthogonale de  $\mathbb{C}^{G^1}$  muni de son produit scalaire usuel. *(Appo)*

## III - TRANSFORMÉE DE FOURIER

### 1. Généralités

Def 28: On appelle transformée de Fourier sur  $G$  l'application  $\mathcal{F} : \mathbb{C}[G] \rightarrow \mathbb{C}[\hat{G}]$  où  $\hat{f}$  est définie par  $f \mapsto \hat{f} \quad \forall \chi \in \hat{G}, \hat{f}(\chi) = |G| \langle \chi, f \rangle = \sum_{g \in G} f(g) \chi(g)$

Prop 29: (Formule d'inversion)

$$\forall f \in \mathbb{C}[G], f = \frac{1}{|G|} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \bar{\chi} \quad \text{(en)}$$

Th 30:  $\mathcal{F}$  réalise un isomorphisme d'algèbres de  $(\mathbb{C}[G], *)$  vers  $(\mathbb{C}[\hat{G}], \cdot)$ .

Prop 31: (Formule de Plancherel)

$$\forall f_1, f_2 \in \mathbb{C}[G], \langle f_1, f_2 \rangle = \frac{1}{|G|} \langle \hat{f}_1, \hat{f}_2 \rangle \quad \text{(en)}$$

En particulier,  $\forall f \in \mathbb{C}[G], \|f\|^2 = \frac{1}{|G|} \|\hat{f}\|^2$ .

Appl 32: Si  $\mathbb{P}$  est une mesure de probabilité sur  $(G, \mathcal{P}(G))$ , alors  $\forall g \in G, \left| \mathbb{P}(g) - \frac{1}{|G|} \right|^2 \leq \frac{1}{|G|} \sum_{\chi \neq \chi_0} |\hat{\mathbb{P}}(\chi)|^2$  où  $\mathbb{P} : g \mapsto \mathbb{P}(g)$  et  $\chi_0$  est le caractère trivial.

Appl 33: (Formule de Poisson)

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

### 2. Transformée de Fourier discrète

Def 34: 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  $\hat{f} = (\hat{f}[n])_{n \in [0, N-1]}$  défini par  $\forall m \in [0, N-1], \hat{f}[m] = \sum_{k=0}^{N-1} f[k] e^{-2ikm\pi/N}$

ou *à l'inverse*  $\hat{f}[n] = \sum_{k=0}^{N-1} f[k] e^{-2ikn\pi/N}$   
 Prop 35: Si  $N \geq 1$  et  $f = (f[n]) \in \mathbb{C}^N$ , alors  $\forall m \in [0, N-1], \hat{f}[m] = \hat{f}_0(\chi_m)$   
 où  $\hat{f}_0 : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}$  et  $\chi_m : \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{C}^*$   
 $k+N\mathbb{Z} \mapsto f[k \bmod N]$  et  $k+N\mathbb{Z} \mapsto \exp\left(-\frac{2ikm\pi}{N}\right)$

Prop 36: Soit  $N \geq 1$ .

• (Formule d'inversion)  $\forall f \in \mathbb{C}^N, \forall k \in [0, N-1], f[k] = \frac{1}{N} \sum_{n=0}^{N-1} \hat{f}[n] e^{\frac{2ikn\pi}{N}}$   
 • (Formule de Plancherel)  $\forall f_1, f_2 \in \mathbb{C}^N, \langle f_1, f_2 \rangle = \frac{1}{N} \langle \hat{f}_1, \hat{f}_2 \rangle$   
 où  $\langle \cdot, \cdot \rangle$  est le produit scalaire usuel sur  $\mathbb{C}^N$ .

Def-Prop 37: 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.

Prop 38:  $\mathcal{F} : f \mapsto \hat{f}$  réalise un isomorphisme d'algèbres de  $(\mathbb{C}^N, *)$  vers  $(\mathbb{C}^N, \cdot)$ .

Appl 39: (Systèmes circulants)

Soient  $C = \begin{pmatrix} c_0 & c_1 & \dots & c_{N-1} \\ c_{N-1} & c_0 & \dots & c_1 \\ \vdots & \vdots & \ddots & \vdots \\ c_1 & \dots & c_{N-1} & c_0 \end{pmatrix}$  une matrice circulante et  $c$  son premier vecteur colonne. *(en)*

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

Algo 40: (Transformée de Fourier rapide)

Supposons que  $N$  est une puissance de 2. Soit  $f \in \mathbb{C}^N$ .

• On calcule récursivement  $\hat{f}^0$  et  $\hat{f}^1$  où  $\hat{f}^0 = (f[2m])_{m \in [0, N/2-1]}$  et  $\hat{f}^1 = (f[2m+1])_{m \in [0, N/2-1]}$   
 • On calcule  $S \hat{f}^1 = (e^{-2im\pi/N} \hat{f}^1[n])_{n \in [0, N/2-1]}$   
 • On a  $\hat{f} = \begin{pmatrix} \hat{f}^0 + S \hat{f}^1 \\ \hat{f}^0 - S \hat{f}^1 \end{pmatrix}$  *en 2 calcul*

Prop 41: 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

$$\forall f \in \mathbb{C}^N, \mathcal{F}^{-1}(f) = \hat{f}_0 \text{ où } f_0 = \left( \frac{1}{N} f[N-n \bmod N] \right)_{n \in \{0, N-1\}}$$

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

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

##### 1. Caractères additifs et multiplicatifs

DEF45: On appelle caractères additifs de  $\mathbb{F}_q$  les éléments de  $\hat{\mathbb{F}}_q$ .

DEF-Prop46: Pour  $x \in \mathbb{F}_q$ , on appelle trace de x et on note  $\text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)$  la trace de l'application

$$m_x: \mathbb{F}_q \rightarrow \mathbb{F}_q, y \mapsto xy$$

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

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

Prop47: L'application

$$\mathbb{F}_q \rightarrow \hat{\mathbb{F}}_q, a \mapsto \psi_a: x \mapsto e^{2i\pi \text{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(ax)/p}$$

est un isomorphisme de groupes.

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

L'application  $\mathbb{Z} \rightarrow \hat{\mathbb{F}}_q^\times, k \mapsto \chi_k: \mathbb{Z} \mapsto e^{2ij k \pi / (q-1)}$ , où  $\mathbb{Z}$  est un générateur de  $\hat{\mathbb{F}}_q^\times$

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

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,  $\eta$  coïncide avec le symbole de Legendre.

##### 2. Sommes de Gauss

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

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

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

•  $\forall a \in \mathbb{F}_q^\times, \forall b \in \mathbb{F}_q, G(\chi, \psi_{ab}) = \chi(a) G(\chi, \psi_b)$

•  $G(\chi, \overline{\psi}) = \chi(-1) G(\chi, \psi)$

•  $G(\overline{\chi}, \psi) = \chi(-1) \overline{G(\chi, \psi)}$

•  $G(\chi, \psi) = \begin{cases} q-1 & \text{si } \chi = \chi_0 \text{ et } \psi = \psi_0 \\ -1 & \text{si } \chi = \chi_0 \text{ et } \psi \neq \psi_0 \\ 0 & \text{si } \chi \neq \chi_0 \text{ et } \psi = \psi_0 \end{cases}$

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  $\eta$  désigne le symbole de Legendre.

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

•  $\forall a \in \mathbb{F}_p^\times, G(a) = \left( \frac{a}{p} \right) G(1)$

•  $G(1) = (-1)^{(p-1)/2} p$

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

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

Appli54: (Loi de réciprocité quadratique)

Soient p et q premiers impairs distincts.

Alors  $\left( \frac{q}{p} \right) = \left( \frac{p}{q} \right) (-1)^{\frac{(p-1)(q-1)}{4}}$  et  $\left( \frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}}$ .

DVPT

②

ca

## ANNEXE

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

$\mathbb{Z}/3\mathbb{Z}$	0	1	2
$\chi_0$	1	1	1
$\chi_1$	1	$j$	$j^2$
$\chi_2$	1	$j^2$	$j$

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

$(\mathbb{Z}/5\mathbb{Z})^\times$	1	2	3	4
$\chi_0$	1	1	1	1
$\chi_1$	1	$i$	$-i$	-1
$\chi_2$	1	-1	-1	1
$\chi_3$	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
$\chi_0$	1	1	1	1	1	1	1	1
$\chi_1$	1	$i$	-1	$-i$	$-i$	1	$-i$	-1
$\chi_2$	1	-1	1	-1	-1	1	-1	1
$\chi_3$	1	$-i$	-1	$-i$	$i$	1	$i$	-1
$\chi_4$	1	-1	1	1	-1	-1	1	-1
$\chi_5$	1	$-i$	-1	$i$	$i$	-1	$-i$	1
$\chi_6$	1	1	1	-1	1	-1	-1	-1
$\chi_7$	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

Théorème. Si  $G$  est un groupe abélien fini et  $H$  est un sous-groupe de  $G$ , alors le morphisme  $\hat{G} \rightarrow \hat{H}$  est surjectif.  

$$x \mapsto x|_H$$

Preuve. Soit  $G$  un groupe abélien fini.

Raisonnons par l'absurde et considérons un sous-groupe  $H$  de  $G$  d'ordre maximal tel que  $\hat{G} \rightarrow \hat{H}$  n'est pas surjectif.  

$$x \mapsto x|_H$$

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  $\varphi(x)$  et  $\chi: K \rightarrow \mathbb{C}^*$   

$$mz+th \mapsto \rho^m \varphi(h)$$

Si  $mz+th = m'z'+th'$  avec  $m, m' \in \mathbb{Z}$  et  $h, h' \in H$ , alors  $(m-m')z = h'-h \in H$  et donc  $n | (m-m')$  et  $\frac{\rho^m \varphi(h)}{\rho^{m'} \varphi(h')} = (\rho^n)^{\frac{m-m'}{n}} \varphi(h-h') = \varphi((m-m')z + h-h') = 1$ , ce qui prouve que  $\chi$  est bien défini.

De plus,  $\chi$  est un caractère de  $K$  qui prolonge  $\varphi$ .

Ainsi tout caractère de  $H$  se prolonge en un caractère de  $G$ . Absurde.

Théorème. Si  $G$  est un groupe abélien fini non trivial, alors il existe une unique suite finie  $(m_1, \dots, m_r)$  d'entiers  $\geq 2$  telle que  $m_i | m_{i+1}$  et  $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \dots \times \mathbb{Z}/m_r\mathbb{Z}$ .

Preuve.

Étape 1: 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  $\varphi: \langle x \rangle \rightarrow \mathbb{C}^*$   

$$x^2 \mapsto e^{\frac{2i\pi k}{m}}$$

D'après le lemme,  $\varphi$  se prolonge en un caractère  $\chi$  de  $G$ .

• Si  $g \in G$ , alors  $\chi(g)^m = 1$  et donc  $\chi(g) \in \langle e^{\frac{2i\pi k}{m}} \rangle = \chi(\langle x \rangle)$ .

Ainsi  $G = \ker(\chi) + \langle x \rangle$ .

• Par ailleurs,  $\ker(\chi) \cap \langle x \rangle = \ker(\varphi) = \{0\}$ .

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

## Étape 2: Unité

• Pour tous  $n \geq 1$  et  $d \in \mathbb{Z}$ ,  $\{z \in \frac{\mathbb{Z}}{n\mathbb{Z}}, dz=0\} = \frac{n}{nd} \frac{\mathbb{Z}}{n\mathbb{Z}}$ .

• 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  $|\{x \in \mathbb{G}, m_r x = 0\}| = \left| m_r^r \prod_{i=1}^s (m_r \wedge n_i) \right| \leq m_r^s$  et donc  $r=s$ .

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

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

Ainsi  $m_k \mid n_k$  et par symétrie,  $m_k = n_k$ . Absurde.

## Loi de réciprocity quadratique

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

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:  $G_2 = \zeta + \zeta^{-1} = \sqrt{2}$ .

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

Démonstration:

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

$\xrightarrow{b=at} \quad \left(\frac{a^2 t}{p}\right) = \left(\frac{t}{p}\right) \text{ si } a \neq 0$

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

Or si  $t \neq -1$ ,  $\begin{cases} \mathbb{F}_p^\times \rightarrow \mathbb{F}_p^\times \\ a \mapsto (1+t)a \end{cases}$  est une bijection, donc  $\sum_{a \in \mathbb{F}_p^\times} \zeta^{(1+t)a} = \sum_{a \in \mathbb{F}_p^\times} \zeta^a = -1$

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

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

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,  $G_p^q = \left( \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) \zeta^a \right)^q \equiv \sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) \zeta^{aq} \pmod{q\mathbb{Z}}$

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

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

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

• On a donc  $(-1)^{\frac{(p-1)}{2} \cdot \frac{(q-1)}{2}} \left(\frac{p}{q}\right) G_p \equiv \left(\frac{q}{p}\right) G_p \pmod{q\mathbb{Z}}$

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

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

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

Démonstration:

• D'une part,  $G_2^p = (\xi + \xi^{-1})^p \equiv \xi^p + \xi^{-p} \pmod{p\overline{\mathbb{Z}}}$ .

- Si  $p \equiv 1$  ou  $7 \pmod{8}$ ,  $G_2^p \equiv \xi + \xi^{-1} \equiv G_2 \pmod{p\overline{\mathbb{Z}}}$

- Si  $p \equiv 3$  ou  $5 \pmod{8}$ ,  $G_2^p \equiv \xi^5 + \xi^{-5} \equiv -(\xi + \xi^{-1}) \equiv -G_2 \pmod{p\overline{\mathbb{Z}}}$   
car  $\xi^4 = -1$ .

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

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

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

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

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