Structure et dualité des groupes abéliens finis. Applications.

1/10

Soit G un groupe fini quelconque.

I - Dualité des groupes abéliens finis

1) Premières définitions et cas cyclique

Def 1 : Un caractère est un morphisme $\chi : G \to \mathbb{C}^*$.
On note $\hat{G}$ l'ensemble des caractères, qu'on appelle le dual du groupe G.

Prop 2 : $\hat{G}$ est un groupe pour la multiplication des applications définie par :
$\forall (\chi_1, \chi_2) \in \hat{G}^2$, $\chi_1 \chi_2 : x \longmapsto \chi_1(x)\chi_2(x)$.

Prop 3 : Si $|G| = n$, les éléments de $\hat{G}$ sont les morphismes de $G \longrightarrow \mathbb{U}_n$.
En particulier, $\forall g \in G$, $|\chi(g)| = 1$ et $\chi(g^{-1}) = \chi(g)^{-1} = \overline{\chi(g)}$.

Rem 4 : $\hat{G}$ est donc un groupe fini et commutatif.

Prop 5 : Soit $G = \{1, g_0, g_0^2, \dots, g_0^{n-1}\}$ un groupe cyclique de cardinal n et de générateur g_0. Soit ω une racine primitive même de l'unité (ex : $\omega = e^{\frac{2i\pi}{n}}$).
Alors, pour tout $j \in [\![0, n-1]\!]$, les éléments de $\hat{G}$ sont de la forme :

$$\chi_j : G \longrightarrow \mathbb{C}^*, \quad g = g_0^k \longmapsto (\omega^j)^k = e^{\frac{2i\pi jk}{n}}.$$

En particulier, $G \simeq \hat{G}$ et $|G| = |\hat{G}|$.

Rem 6 : Cet isomorphisme n'est pas canonique car il dépend du choix de la racine primitive de l'unité ω choisie.

Cor 7 : $\forall n \in \mathbb{N}^*$, $\widehat{\mathbb{Z}/n\mathbb{Z}} \simeq \mathbb{Z}/n\mathbb{Z}$.

2) Cas d'un groupe abélien fini quelconque

Lem 8 : (Prolongement des caractères) Soit G un groupe abélien fini et $H \subset G$ un sous-groupe. Tout caractère χ de H peut être prolongé en un caractère de G.

DEV 1

Lem 9 : Soit $p : \hat{G} \twoheadrightarrow \hat{H}$ le morphisme de restriction et $j : \widehat{G/H} \hookrightarrow \hat{G}$ avec $\tilde{\chi}(x) := \chi(xH)$, le morphisme $\chi \longmapsto \tilde{\chi}$ d'extension. On a alors la suite exacte :

$$\{1\} \longrightarrow \widehat{G/H} \xrightarrow{j} \hat{G} \xrightarrow{p} \hat{H} \longrightarrow \{1\}.$$

Cor 10 : Soit G un groupe abélien fini. Alors $|G| = |\hat{G}|$.

Thm 11 : (Théorème de structure des groupes abéliens) Soit G un groupe abélien fini. Il existe des entiers strictement positifs $n_1, \dots, n_s$ uniquement déterminés tq $n_1 | n_2 | \cdots | n_s$ et tels que :

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}.$$

Cor 12 : (Théorème d'isomorphisme) Soit G un groupe abélien fini. Alors, $\hat{G} \simeq G$ et $|G| = |\hat{G}|$.

Rem 13 : Cet isomorphisme n'est pas canonique.

Thm 14 : (Théorème chinois) Soit m et n deux entiers premiers entre eux. Alors,

$$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Prop 15: Tout groupe abélien fini est produit direct de ses sous-groupes de Sylow.

Ex 16: Le groupe $A = \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/90\mathbb{Z}$ est d'ordre $2250 = 2.3^2.5^3$.

$$A \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}).$$

$$\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3^2\mathbb{Z} \times (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}).$$

Def 17: Soit G un groupe fini abélien, alors $\hat{G}$ est un groupe fini abélien. On peut lui associer son dual noté $\hat{\hat{G}}$ et appelé bidual de G.

Prop 18: On a un isomorphisme canonique $G \simeq \hat{\hat{G}}$, donné par $\varphi : G \longrightarrow \hat{\hat{G}}$, $g \longmapsto \varphi(g) : \chi \mapsto \chi(g)$

Cor 19: $|G| = |\hat{G}| = |\hat{\hat{G}}|$.

3) Ouverture aux groupes non abéliens

Prop 20: Soit G un groupe fini. On a $\hat{G} \simeq G/D(G)$.

Ex 21: Pour $n \geq 3$, on a $D(\mathfrak{S}_n) = \mathcal{A}_n$ et donc $\hat{\mathfrak{S}}_n \simeq \mathfrak{S}_n/\mathcal{A}_n \simeq \mathbb{Z}/2\mathbb{Z}$.

II - L'algèbre $\mathbb{C}[G]$ et transformée de Fourier

1) Structure de $\mathbb{C}[G]$ et relations d'orthogonalité

Def 22: On note $\mathbb{C}[G]$ l'ensemble des fonctions de G dans $\mathbb{C}$. C'est un espace vectoriel sur $\mathbb{C}$, muni d'un produit scalaire hermitien :

$$\forall (f,g) \in \mathbb{C}[G]^2, \quad \langle f, g \rangle := \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}.$$

Ainsi qu'une norme $\|f\|_2 = \sqrt{\langle f, f \rangle}$, pour tout $f \in \mathbb{C}[G]$.

Lem 23: Soit G un groupe abélien fini. Pour $\chi \in \hat{G}$, on a : $\sum_{g \in G} \chi(g) = \begin{cases} 0 \text{ si } \chi \neq 1 \\ |G| \text{ si } \chi = 1 \end{cases}$.

Prop 24: (orthogonalité des caractères) Soit G un groupe abélien fini. Alors $\hat{G}$ est une famille orthonormale et $\forall (\chi_1, \chi_2) \in \hat{G}^2$, $\langle \chi_1, \chi_2 \rangle = \begin{cases} 0 \text{ si } \chi_1 \neq \chi_2 \\ 1 \text{ si } \chi_1 = \chi_2 \end{cases}$.

Cor 25: Soit G un groupe abélien fini, alors $\hat{G}$ est une base orthonormale de $\mathbb{C}[G]$.

Prop 26: Soit $g, h \in G$. Alors $\sum_{\chi \in \hat{G}} \chi(g)\overline{\chi(h)} = \begin{cases} 0 \text{ si } g \neq h \\ |G| \text{ si } g = h \end{cases}$

App 27: Soit G un groupe abélien fini et $\varphi : G^n \longrightarrow G$. Pour $h \in G$, on note $N(h)$ le nombre de n-uplets $(g_1, \dots, g_n)$ tq $\varphi(g_1, \dots, g_n) = h$. Alors, $N(h) = \frac{1}{|G|} \sum_{g_1 \in G} \cdots \sum_{g_n \in G} \sum_{\chi \in \hat{G}} \chi(\varphi(g_1, \dots, g_n))\overline{\chi(h)}$.

2) Transformée de Fourier

Def 28: Soit G un groupe abélien fini. On définit la transformée de Fourier $\mathcal{F} : \mathbb{C}[G] \longrightarrow \mathbb{C}[\hat{G}]$ ou $f \longmapsto \hat{f}$

$$\forall \chi \in \hat{G}, \quad \hat{f}(\chi) = \sum_{x \in G} f(x)\chi(x).$$

Prop 29: (Formule d'inversion) Pour $f \in \mathbb{C}[G]$, on a :

$$f = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \hat{f}(\chi)\, \chi^{-1}.$$

Prop 30: (Formule de Plancherel) Soit $f, g \in \mathbb{C}[G]^2$, alors

$$\sum_{s \in G} f(s)\, \overline{g(s)} = \frac{1}{|G|} \sum_{\chi \in \widehat{G}} \hat{f}(\chi)\, \overline{\hat{g}(\chi)}.$$

III - Applications sur les corps finis

Soit p un nombre premier et $q = p^m$.

1) Caractères additifs et multiplicatifs

Def 31: 1) Les éléments de $\widehat{\mathbb{F}_q}$ sont les morphismes $\psi : (\mathbb{F}_q, +) \longrightarrow (\mathbb{C}^*, \times)$ appelés caractères additifs.

2) Les éléments de $\widehat{\mathbb{F}_q^*}$ sont les morphismes $\chi : (\mathbb{F}_q^*, \times) \longrightarrow (\mathbb{C}^*, \times)$ appelés caractères multiplicatifs.

Rem 32: Les caractères les plus simples à déterminer sont ceux de $\widehat{\mathbb{F}_q^*}$. Soit ζ un générateur du groupe cyclique $\mathbb{F}_q^*$, alors les caractères multiplicatifs sont :

$$\forall j \in [\![0, q-1]\!],\quad \chi_j : \begin{array}{ccc} \mathbb{F}_q^* & \longrightarrow & \mathbb{C}^* \\ \zeta^k & \longmapsto & e^{\frac{2i\pi}{q-1} jk} \end{array}.$$

Def 33: On définit le caractère additif canonique $\psi_1 \in \widehat{\mathbb{F}_q}$ par : $\psi_1 : \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{C}^* \\ x & \longmapsto & e^{\frac{2i\pi}{p} \mathrm{Tr}(x)} \end{array}$.

Prop 34: Les caractères additifs sont les applications définies pour $a \in \mathbb{F}_q$ par : $\psi_a : \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{C}^* \\ x & \longmapsto & \psi_1(ax) \end{array}$.

Rem 35: On note $\psi_0 = 1$, le caractère additif trivial.

Ex 36: (Caractère quadratique) Soit q un entier impair. On définit $\eta \in \widehat{\mathbb{F}_q^*}$ par : $\forall x \in \mathbb{F}_q^*$, $\eta(x) = \begin{cases} 1 & \text{si } x \text{ est un carré dans } \mathbb{F}_q \\ -1 & \text{sinon.} \end{cases}$

Alors $\eta = \chi_0^{\frac{q-1}{2}}$. Si $q = p$ premier alors $\eta(x) = \left(\frac{x}{p}\right)$.

2) Sommes de Gauss

Def 37: Soit $\chi \in \widehat{\mathbb{F}_q^*}$ et $\psi \in \widehat{\mathbb{F}_q}$. On définit la somme de Gauss associée à ces deux caractères par :

$$G(\chi, \psi) = \sum_{x \in \mathbb{F}_q^*} \psi(x)\, \chi(x).$$

Prop 38: Soit $\chi \in \widehat{\mathbb{F}_q^*}$. Alors, $\chi = \frac{1}{q} \sum_{\psi \in \widehat{\mathbb{F}_q}} G(\chi, \overline{\psi})\, \psi$.

Rem 39: En général, on est incapable de calculer les valeurs de ces sommes de Gauss, on disposera juste d'information sur son module.

Prop 40: (Calcul des sommes de Gauss)

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

Dans les autres cas, $|G(\chi, \psi)| = q^{\frac{1}{2}}$.

De plus, $G(\chi, \psi)\, G(\overline{\chi}, \psi) = q\, \chi(-1)$ pour $\chi \neq \chi_0$ et $\psi \neq \psi_0$.

Prop 41: Soit χ un caractère multiplicatif d'ordre m dans $\mathbb{F}_q^*$ (i.e. $\chi^m = \chi_0$). Alors $\chi(-1) = -1$ si et seulement si m pair et $\frac{q-1}{m}$ impair.

App 42 Soit $q = p^m$, $d \mid q-1$ et $a_1, \dots, a_m \in \mathbb{F}_p^*$. On définit

$F : \begin{array}{ccc} (\mathbb{F}_q)^m & \longrightarrow & \mathbb{F}_q \\ (x_1, \dots, x_m) & \longmapsto & \sum_{i=1}^m a_i x_i^d \end{array}$ et $G_d = \left\{ \chi \in \widehat{\mathbb{F}_q^*},\ \chi^d = \chi_0 \right\}$ et

$S_d = \left\{ (x_1, \dots, x_m) \in (G_d \setminus \{0\})^m,\ x_1 \cdots x_m = \chi_0 \right\}$. On pose

$N = \mathrm{Card} \left\{ x = (x_1, \dots, x_m) \in (\mathbb{F}_q)^m,\ F(x) = 0 \right\}$.

Alors, $N = q^{m-1} + \frac{q-1}{q} \sum_{(\chi_1, \dots, \chi_m) \in S_d} \overline{\chi_1}(a_1) \cdots \overline{\chi_m}(a_m)\, G(\chi_1, \psi) \cdots G(\chi_m, \psi)$.

DEV 2

Développement 1 : Prolongement de caractères

Cadre : On considère G un groupe abélien fini.

Théorème (Prolongement de caractères). *Soit H un sous-groupe de G. Alors tout caractère de H se prolonge en un caractère de G.*

Preuve.
On démontre cela par récurrence sur l'indice de H dans G.
Le résultat est bien sûr vrai pour $[G : H] = 1$, ie $G = H$.
Soit $m > 1$, supposons que $[G : H] = m$ et que la propriété est vraie pour tout sous-groupe d'indice strictement inférieur à m.
On considère $x \in G$ tel que $x \notin H$ et $K = \langle H, x\rangle$. Soit n l'ordre de xH dans G/H.
On a alors une décomposition unique de tout $z \in K$ sous la forme $z = yx^k$, avec $y \in H$ et $k \in \{0, ..., n-1\}$. En effet, si $yx^k = y'x^l$, $0 \leq k \leq l \leq n-1$, alors $x^{l-k} \in H$, donc $l = k$ car $l - k < n$.
Soit maintenant $\chi \in \widehat{H}$ On va procéder par analyse synthèse pour démontrer l'existence d'un prolongement $\tilde{\chi}$ sur K.
Analyse : Si l'on dispose d'un tel prolongement $\tilde{\chi}$, alors on pose $\xi = \tilde{\chi}(x)$ et ξ vérifie $\xi^n = \tilde{\chi}(x^n) = \chi(x^n)$ car $x^n \in H$. Donc ξ est une racine n-ème de $\chi(x^n)$.
Le prolongement $\tilde{\chi}$ est ainsi défini par $\tilde{\chi}(yx^k) = \chi(y)\xi^k$ $(*)$ pour $z = yx^k, y \in H, 0 \leq k \leq n-1$.
Synthèse : Soit ξ une racine n-ème de $\chi(x^n)$ et $\tilde{\chi}$ défini par $(*)$.
Montrons que $\tilde{\chi} \in \widehat{K}$. Premièrement, $\tilde{\chi}$ est bien défini, par unicité de la décomposition du type $z = yx^k$. Soient $h = yx^k, h' = y'x^{k'} \in K$. Deux cas sont à distinguer :
• Si $0 \leq k + k' \leq n-1$, alors

$$\tilde{\chi}(hh') = \tilde{\chi}(yy'x^{k+k'}) = \chi(yy')\xi^{k+k'} = (\chi(y)\xi^k)(\chi(y')\xi^{k'}) = \tilde{\chi}(h)\tilde{\chi}(h').$$

• Si $n \leq k + k' \leq 2n-2$, alors

$$\tilde{\chi}(hh') = \tilde{\chi}(yy'x^n x^{k+k'-n}) = \chi(y)\chi(y')\underbrace{\chi(x^n)}_{=\xi^n}\xi^{k+k'-n} = (\chi(y)\xi^k)(\chi(y')\xi^{k'}) = \tilde{\chi}(h)\tilde{\chi}(h')$$

Finalement, $\tilde{\chi}$ est bien un morphisme de groupes, d'où $\tilde{\chi} \in \widehat{K}$. La multiplicativité des indices nous donne, comme $[K : H] > 1$,

$$[G : K] = \frac{[G : H]}{[K : H]} < [G : H].$$

L'hypothèse de récurrence nous permet de conclure que $\tilde{\chi}$, donc χ, se prolonge sur G, ce qui conclut la preuve du théorème. □

Théorème (Théorème de structure des groupes abéliens finis).
Soit G un groupe abélien fini. Alors il existe $r \in \mathbb{N}$ et $n_1, ..., n_r \in \mathbb{N}$ tels que $n_r | n_{r-1} | ... | n_1$ et

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_r\mathbb{Z}.$$

En particulier, n_1 est l'exposant de G.

Preuve.
On va démontrer le résultat par récurrence sur l'ordre de G.
Le résultat est vrai pour $|G| = 2$, car dans ce cas $G \simeq \mathbb{Z}/2\mathbb{Z}$.
Soit $n \geq 3$ et supposons que $|G| = n$ et que le résultat est vrai pour tout groupe d'ordre

strictement inférieur à n.
Soit n_1 l'exposant de G. Comme G est abélien, il existe $x \in G$ d'ordre n_1. On considère le groupe cyclique $H = \langle x \rangle \simeq \mathbb{Z}/n_1\mathbb{Z} \simeq \mathbb{U}_{n_1}$. Soit $\chi \in \widehat{H}$ l'isomorphisme en question.
On peut supposer que $H \neq G$ car si $H = G$, alors $G \simeq \mathbb{Z}/n_1\mathbb{Z}$ et le résultat est démontré.
Par le lemme de prolongement, il existe un prolongement $\tilde{\chi}$ de χ sur G.
Comme pour tout $g \in G, g^{n_1} = 1$, par définition de l'exposant, alors $\tilde{\chi}$ est à valeurs dans $\mathbb{U}_{n_1}$.
Cette remarque assure que l'application

$$\begin{aligned} \varphi : G &\to H \times G/H \\ g &\mapsto (\chi^{-1} \circ \tilde{\chi}(g), gH) \end{aligned}$$

est bien définie. C'est de plus un isomorphisme de groupes.
En effet, si $g \in Ker(\varphi)$, alors $g \in H$, d'où $\chi^{-1} \circ \tilde{\chi}(g) = \chi^{-1} \circ \chi(g) = g$ et donc $g = 1$. Donc φ est injectif, et surjectif pour des raisons de cardinal. D'où $G \simeq H \times G/H \simeq \mathbb{Z}/n_1\mathbb{Z} \times G/H$.
On applique l'hypothèse de récurrence à G/H : il existe des entiers $n_2, ..., n_r$ tels que $n_r | n_{r-1} | ... | n_2$ et

$$G/H \simeq \mathbb{Z}/n_2\mathbb{Z} \times ... \times \mathbb{Z}/n_r\mathbb{Z}$$

Pour conclure, il reste à vérifier que n_2 divise n_1.
Pour cela, remarquons que $(0, 1, 0, ..., 0) \in \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_r\mathbb{Z}$ est d'ordre n_2, qui divise donc l'exposant du groupe. □

Développement 2 : Dénombrement de solutions à des équations polynômiales sur $\mathbb{F}_q$

Cadre : Soit p premier, $q = p^m$ et $\mathbb{F}_q$ le corps à q éléments.
On considère $d \in \mathbb{N}$ tel que d divise $q - 1$, des éléments $a_1, ..., a_n \in \mathbb{F}_p$ et l'application

$$\begin{aligned} F : (\mathbb{F}_q)^n &\to \mathbb{F}_q \\ (x_1, ..., x_n) &\mapsto \sum_{i=1}^{n} a_i x_i^d. \end{aligned}$$

On considère également $G_d = \{\chi \in \widehat{\mathbb{F}_q^*}, \chi^d = \chi_0\}$ un sous-groupe cyclique d'ordre d de $\widehat{\mathbb{F}_q^*}$ et $S_d = \{(\chi_1, ..., \chi_n) \in (G_d \setminus \{\chi_0\})^n, \chi_1 ... \chi_n = \chi_0\}$.

Théorème. *Soit* $N = Card\{x = (x_1, ..., x_n) \in (\mathbb{F}_q)^n, F(x) = 0\}$. *Alors*

$$N = q^{n-1} + \frac{q-1}{q} \sum_{(\chi_1,...,\chi_n) \in S_d} \overline{\chi_1}(a_1) ... \overline{\chi_n}(a_n) G(\chi_1, \psi) ... G(\chi_n, \psi).$$

Preuve.
Pour tout $b = F(x) \in \mathbb{F}_q$, la relation d'orthogonalité pour le caractère additif ψ_b nous donne

$$\sum_{a \in \mathbb{F}_q} \psi_b(a) = \begin{cases} q & si \ \ b = F(x) = 0 \\ 0 & si \ \ b = F(x) \neq 0 \end{cases}$$

Donc on a la relation

$$\sum_{x \in (\mathbb{F}_q)^n} \sum_{a \in \mathbb{F}_q} \psi_{F(x)}(a) = qN.$$

D'où

$$\begin{aligned} qN &= \underbrace{\sum_{x\in(\mathbb{F}_q)^n} \psi_{F(x)}(0)}_{=q^n} + \sum_{x\in(\mathbb{F}_q)^n}\sum_{a\in\mathbb{F}_q^*} \psi_{F(x)}(a) \\ &= q^n + \sum_{a\in\mathbb{F}_q^*}\sum_{x\in(\mathbb{F}_q)^n} \exp\left(\frac{2i\pi}{p} Tr\left(a\sum_{j=1}^n a_j x_j^d\right)\right) \\ &= q^n + \sum_{a\in\mathbb{F}_q^*}\sum_{x\in(\mathbb{F}_q)^n} \underbrace{\exp\left(\frac{2i\pi}{p}\sum_{j=1}^n a_j Tr\left(ax_j^d\right)\right)}_{=\prod_{j=1}^n \psi_{aa_j}(x_j^d)} \\ &= q^n + \sum_{a\in\mathbb{F}_q^*}\prod_{j=1}^n \underbrace{\sum_{y\in\mathbb{F}_q} \psi_{aa_j}(y^d)}_{:=T(d,aa_j)} \end{aligned}$$

où l'on note pour tout $a \in \mathbb{F}_q, T(d,a) = \sum_{y\in\mathbb{F}_q} \psi_a(y^d)$.
Il s'agit maintenant de calculer ces sommes $T(d,a)$ pour conclure :

Lemme. *Pour tout $a \in \mathbb{F}_q$, on a*

$$T(d,a) = \sum_{\chi\in G_d\setminus\{\chi_0\}} \overline{\chi}(a) G(\chi,\psi).$$

Preuve du lemme.
On montre tout d'abord l'égalité suivante : pour tout $x \in \mathbb{F}_q$

$$\sum_{\chi\in G_d} \chi(x) = \begin{cases} d & si\ \ x\in\mathbb{F}_q^{*d} \\ 1 & si\ \ x=0 \\ 0 & sinon \end{cases}$$

- Si $x = y^d \in \mathbb{F}_q^{*d}$, alors

$$\sum_{\chi\in G_d} \chi(x) = \sum_{\chi\in G_d} \underbrace{\chi(y)^d}_{=1} = |G_d| = d$$

- On a $\sum_{\chi\in G_d} \chi(0) = \chi_0(0) = 1$.
- Sinon, on considère $\tilde{\chi}$ un générateur de G_d. Alors on a $\tilde{\chi}(x) \neq 1$ donc

$$\sum_{\chi\in G_d} \chi(x) = \sum_{i=0}^{d-1} \tilde{\chi}(x)^i = \frac{\tilde{\chi}^d(x)-1}{\tilde{\chi}(x)-1} = 0,$$

ce qui conclut la preuve de la première égalité. On a alors

$$T(d,a) = \sum_{y\in\mathbb{F}_q} \psi_a(y^d) = \psi_a(0) + \sum_{y\in\mathbb{F}_q^*} \psi_a(y^d).$$

Soit maintenant ξ un générateur de $\mathbb{F}_q^*$. On a $\mathbb{F}_q^{*d} = \{\xi^d, ..., \xi^{\frac{q-1}{d}.d} = 1\}$ et la partition

$$\mathbb{F}_q^* = \mathbb{F}_q^{*d} \sqcup \xi\mathbb{F}_q^{*d} \sqcup ... \sqcup \xi^{d-1}\mathbb{F}_q^{*d}.$$

D'où

$$\begin{aligned}\sum_{y\in\mathbb{F}_q^*} \psi_a(y^d) = d \sum_{t\in\mathbb{F}_q^{*d}} \psi_a(t) &= \sum_{t\in\mathbb{F}_q^{*d}} \left(\sum_{\chi\in G_d} \chi(t)\right) \psi_a(t) \\ &= \sum_{t\in\mathbb{F}_q^*} \left(\sum_{\chi\in G_d} \chi(t)\right) \psi_a(t)\end{aligned}$$

et donc

$$T(d,a) = \sum_{t\in\mathbb{F}_q} \sum_{\chi\in G_d} \chi(t)\psi(at).$$

En effectuant un changement de variable en $x = at$, on obtient

$$\begin{aligned}T(d,a) &= \sum_{\chi\in G_d} \chi(a^{-1}) \underbrace{\sum_{x\in\mathbb{F}_q} \chi(x)\psi(x)}_{= G(\chi,\psi)} \\ &= \sum_{\chi\in G_d\setminus\{\chi_0\}} \overline{\chi}(a) G(\chi,\psi)\end{aligned}$$

car $G(\chi_0, \psi) = 0$, ce qui conclut la preuve du lemme. □

Il reste maintenant à utiliser le résultat du lemme dans les calculs le précédant. Nous avions établi que

$$qN = q^n + \sum_{a\in\mathbb{F}_q^*} \prod_{j=1}^n T(d, aa_j).$$

D'où

$$\begin{aligned}qN &= q^n + \sum_{a\in\mathbb{F}_q^*} \prod_{j=1}^n \sum_{\chi\in G_d\setminus\{\chi_0\}} \overline{\chi}(aa_j) G(\chi,\psi) \\ &= q^n + \sum_{a\in\mathbb{F}_q^*} \sum_{(\chi_1,...,\chi_n)\in(G_d\setminus\{\chi_0\})^n} \prod_{j=1}^n \overline{\chi_j}(aa_j) G(\chi_j,\psi) \\ &= q^n + \sum_{(\chi_1,...,\chi_n)\in(G_d\setminus\{\chi_0\})^n} \underbrace{\sum_{a\in\mathbb{F}_q^*} \overline{\chi_1}(a)...\overline{\chi_n}(a)}_{A} \prod_{j=1}^n \overline{\chi_j}(a_j) G(\chi_j,\psi)\end{aligned}$$

où $A = \begin{cases} q-1 & si\ \ \chi_1...\chi_n = \chi_0 \\ 0 & sinon \end{cases}$. D'où finalement

$$qN = q^n + (q-1) \sum_{(\chi_1,...,\chi_n)\in S_d} \prod_{j=1}^n \overline{\chi_j}(a_j) G(\chi_j,\psi),$$

ce qui conclut la preuve du théorème. □