Fiche sur les racines de l'unité : Sommes de Gauss et transformée de Fourier discrète

Dans toute cette fiche, $n \geq 2$ est un entier et $\zeta_n = e^{2i\pi/n}$ (mais un autre choix de racine n-ième primitive donnera un résulat équivalent).

Notation pratique Comme ζ_n^k ne dépend que de k modulo n pour k entier, on notera également ζ_n^k pour $k \in \mathbb{Z}/n\mathbb{Z}$, et cette notation puissance vérifie les propriétés habituelles.

Formule fondamentale (c'est le nom que je lui donne)

Pour tout entier $a \in \mathbb{Z}$,

$$\sum_{b=0}^{n-1} \zeta_n^{ab} = \sum_{b \in \mathbb{Z}/n\mathbb{Z}} \zeta_n^{ab} = \begin{cases} n & \text{si } a \equiv 0 \bmod n. \\ 0 & \text{sinon.} \end{cases}$$

Deux preuves équivalentes. On reconnaît une somme partielle de la suite géométrique de raison $\omega = \zeta_n^a$, ce qui donne $\frac{1-\omega^n}{1-\omega}$ si $\omega \neq 1$ et n sinon, puis on utilise le fait que ω est une racine n-ième de l'unité, soit on reconnaît directement

$$1 + X + \cdots + X^{n-1} = \frac{X^n - 1}{X - 1}$$

qu'il suffit ensuite d'évaluer soit en 1 soit en une autre racine n-ième de l'unité $\omega = \zeta_n^a$. □

1 Sommes de Gauss

1.1 Définition et propriétés des sommes de Gauss

Référence : Hindry, Arithmétique.

La version la plus simple des sommes de Gauss est la suivante. On fixe p un nombre premier impair, et on rappelle que $\left(\frac{a}{p}\right)$ est le symbole de Legendre d'un entier a modulo p.

La somme de Gauss est alors

$$G(a) := \sum_{x=0}^{p-1} e^{2i\pi a x^2/p} = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \zeta_p^{ax^2}.$$

Remarque 1.1. On peut toujours réécrire

$$G(a) = \sum_{y=0}^{p-1} \left(\frac{y}{p}\right) \zeta_p^{ay}. \tag{1}$$

En effet, dans cette expression, on compte 0 fois la racine 1 (symbole de Legendre nul), 1 fois les racines avec exposants de la forme ax^2 où $x \in (\mathbb{Z}/p\mathbb{Z})^*$ et -1 fois les autres. En ajoutant la somme de toutes les racines p-ièmes de l'unité qui est nulle, on comptera 1 fois la racine 1, 2 fois les racines avec exposants de la forme ax^2 et 0 fois les autres, ce qui revient exactement à l'expression initiale de $G(a)$.

Proposition 1.2 (Propriétés fondamentales)**.** *Pour tout $a \in \mathbb{Z}$ premier à p :*

(*a*) $G(a) = \left(\frac{a}{p}\right) G(1)$.

(*b*) *Si* $p \nmid a$, $|G(a)|^2 = p$.

(*c*) *Enfin,* $G(1)^2 = \left(\frac{-1}{p}\right) p$.

Démonstration. (*a*) Si a est un carré modulo p, on peut écrire $a = b^2$ et alors

$$G(a) = \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \zeta_p^{(bx)^2} = \sum_{y \in \mathbb{Z}/p\mathbb{Z}} \zeta_p^{y^2} = G(1).$$

avec le changement de variable $y = bx$. Sinon, les ax^2 pour $x \in (\mathbb{Z}/p\mathbb{Z})^*$ parcourent les non-carrés de $(\mathbb{Z}/p\mathbb{Z})^*$ (par multiplicativité du symbole de Legendre) et chacun est atteint deux fois car p est impair, et donc

$$G(a) = 1 + 2 \sum_{\substack{y \in (\mathbb{Z}/p\mathbb{Z})^* \\ y \text{ non carré}}} \zeta_p^y$$

de sorte que

$$\begin{aligned} G(a) + G(1) &= 2 + 2 \sum_{\substack{y \in (\mathbb{Z}/p\mathbb{Z})^* \\ y \text{ non carré}}} \zeta_p^y + 2 \sum_{\substack{y \in (\mathbb{Z}/p\mathbb{Z})^* \\ y \text{carré}}} \zeta_p^y \\ &= 2 \sum_{x \in (\mathbb{Z}/p\mathbb{Z})} \zeta_p^x = 0. \end{aligned}$$

(*b*) On obtient d'abord immédiatement que

$$\overline{G(a)} = \sum_{x=0}^{p-1} \overline{\zeta_p^{ax^2}} = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})} \zeta_p^{-ax^2} = G(-a).$$

On a d'un côté grâce au (*a*) que $\sum_{a=1}^{p-1} |G(a)|^2 = (p-1)G(1)^2$ et de l'autre que

$$\sum_{a=1}^{p-1} |G(a)|^2 = \sum_{a=1}^{p-1} \sum_{x,y \in (\mathbb{Z}/p\mathbb{Z})} \zeta_p^{a(x^2-y^2)} = \sum_{u,v \in (\mathbb{Z}/p\mathbb{Z})} \sum_{a=1}^{p-1} \zeta_p^{auv}$$

grâce au changement de variable $u = x + y, v = x - y$ dans $(\mathbb{Z}/p\mathbb{Z})^2$ (d'inverse $x = (u+v)/2, y = (u-v)/2$ comme p est impair). Maintenant, grâce à la formule fondamentale, à u et a fixés, la somme sur v vaut 0 sauf si $au = 0 \bmod p$ (donc $u = 0$ car a est inversible) et elle vaut alors p dans ce cas. On obtient donc

$$\sum_{a=1}^{p-1} |G(a)|^2 = \sum_{a=1}^{p-1} p = p(p-1),$$

ce qui montre bien que $|G(1)|^2 = p$.

(c) Pour finir, on a $|G(1)|^2 = G(1)G(-1) = \left(\frac{-1}{p}\right) G(1)^2$ et en conséquence $G(1)^2 = \left(\frac{-1}{p}\right) p$ d'après (a) et (b). □

Exercice 1.3. Redémontrer les trois propriétés avec l'expression alternative (1).

1.2 Preuve de la loi de réciprocité quadratique

Références : Hindry, Arithmétique et Serre, Cours d'arithmétique.

Le but est de montrer, pour p et q deux nombres premiers impairs distincts, la relation

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Pour cela, il faut faire des sommes de Gauss *mais* sur des corps finis.

On fixe donc $\omega_p \in \overline{\mathbb{F}_q}$ une racine p-ième primitive de l'unité (*attention* : il n'existe pas de racine p-ième primitive dans $\overline{\mathbb{F}_p}$, savoir pourquoi !), et on définit alors comme avant

$$G_q(a) = \sum_{x=0}^{p-1} \omega_p^{ax^2} \in \overline{\mathbb{F}_q}$$

pour tout a non multiple de p.

Si on souhaite dès le début démontrer la réciprocité quadratique, il vaut mieux commencer directement par ces expressions.

Exercice 1.4. Montrer que la formule fondamentale et la remarque qui suit est encore valide avec ω_p au lieu de ζ_p. En déduire que le (a) de la Proposition 1.2 est encore vrai également pour $G_q(a)$.

Remarque 1.5. La Proposition 1.2 (b) n'a a priori pas de sens comme on ne dispose plus de la conjugaison complexe, mais en fait en remplaçant $|G(a)|^2$ par $G_q(a)G_q(-a)$, on s'attend à retrouver le résultat. Mais on fait une division par $(p-1)$ à un moment (où ?) qui empêche de reproduire mot à mot la preuve si $q|p-1$.

On va donc redémontrer directement la proposition suivante.

Proposition 1.6. *Dans* $\mathbb{F}_q$, $G_q(1)^2 = \left(\frac{-1}{p}\right) p$. *De plus,* $G_q(1)^{q-1} = \left(\frac{q}{p}\right)$.

Démonstration. Cette fois, on utilise d'emblée l'égalité $G_q(a) = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) \omega_p^{ax}$, pour avoir

$$G_q(1)^2 = \sum_{0 \le x,y \le p-1} \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \omega_p^x \omega_p^y = \sum_{s \in (\mathbb{Z}/p\mathbb{Z})} \omega_p^s \sum_{\substack{x,y \in \mathbb{Z}/p\mathbb{Z} \\ x+y=u}} \left(\frac{xy}{p}\right)$$

en regroupant les termes selon la valeur $s = x + y$. On va noter $S(s)$ la somme auxiliaire sur x, y avec $x + y = s$ ci-dessus. Alors, pour $s = 0$,

$$S(0) = \sum_{x=0}^{p} \left(\frac{-1}{p}\right)\left(\frac{x}{p}\right)^2 = \left(\frac{-1}{p}\right)(p-1)$$

(attention au terme $x = 0$),et pour s non nul,

$$S(s) = \sum_{x\in(\mathbb{Z}/p\mathbb{Z})} \left(\frac{x(s-x)}{p}\right) = \left(\frac{-1}{p}\right) \sum_{x\in(\mathbb{Z}/p\mathbb{Z})^*} \left(\frac{1-sx^{-1}}{p}\right)$$

en enlevant le terme nul pour $x = 0$ et en factorisant par $\left(\frac{-x^2}{p}\right) = \left(\frac{-1}{p}\right)$.

Maintenant, l'application $x \mapsto y = 1 - sx^{-1}$ est injective et donc bijective de $(\mathbb{Z}/p\mathbb{Z})^*$ dans $(\mathbb{Z}/p\mathbb{Z})\backslash\{1\}$, donc en faisant le changement de variable induit,

$$S(s) = \left(\frac{-1}{p}\right) \sum_{\substack{y\in(\mathbb{Z}/p\mathbb{Z}) \\ y\neq 1}} \left(\frac{y}{p}\right) = -\left(\frac{-1}{p}\right)$$

car il y a autant de carrés que de non-carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$. On obtient donc

$$G_q(1)^2 = \left(\frac{-1}{p}\right)(p-1) - \left(\frac{-1}{p}\right) \sum_{s\in(\mathbb{Z}/p\mathbb{Z})^*} \omega_p^s = \left(\frac{-1}{p}\right) p$$

car la somme des racines p-ièmes de l'unité sauf 1 vaut -1.

Maintenant, en utilisant le Frobenius sur $\overline{\mathbb{F}_q}$, et comme q est impair (donc $x \mapsto x^q$ fixe 0,1 et -1), on a

$$G_q(1)^q = \sum_{x\in(\mathbb{Z}/p\mathbb{Z})} \left(\frac{x}{p}\right) \omega_p^{qx} = G_q(q) = \left(\frac{q}{p}\right) G_q(1).$$

Le résultat précédent prouve en particulier que $G_q(1) \neq 0$ donc on peut diviser et on obtient bien $G_q(1)^{q-1} = \left(\frac{q}{p}\right)$. □

On peut maintenant montrer la réciprocité quadratique. Rappelons que pour tout $x \in \mathbb{F}_q$, $\left(\frac{x}{q}\right) = x^{(q-1)/2}$ (savoir pourquoi). Alors, dans $\mathbb{F}_q$,

$$\begin{aligned}
\left(\frac{p}{q}\right) &= p^{(q-1)/2} = \left(\left(\frac{-1}{p}\right) G_q(1)^2\right)^{(q-1)/2} \\
&= (-1)^{(p-1)(q-1)/4} G_q(1)^{q-1} \\
&= (-1)^{(p-1)(q-1)/4} \left(\frac{q}{p}\right).
\end{aligned}$$

grâce aux relations de la proposition.

On a donc une égalité d'éléments égaux à ± 1 dans $\mathbb{F}_q$ c'est-à-dire modulo q, qui est impair. On en déduit finalement que ces éléments sont égaux dans $\mathbb{Z}$, c'est-à-dire la loi de réciprocité quadratique.

1.3 Preuve du théorème de Polya-Vinogradov

TDF discrète. FFT.

2 Dualité

Les racines de l'unité sont également au coeur d'une notion importante de théorie des groupes, celle de dualité.

Définition 2.1 (Caractère abélien et groupe dual)**.**
Soit G un groupe. Un *caractère (abélien)* est un morphisme de groupes $\chi : G \to \mathbb{C}^*$.
Le *groupe dual* de G, noté $\widehat{G}$, est le groupe abélien formé par ses caractères.

Remarque 2.2. On précise caractère abélien car il ne faut pas confondre avec les caractères issus des représentations, qui ne sont en général pas des morphismes de groupes.

Proposition 2.3. *Les propriétés générales des caractères sont les suivantes :*
(a) Le groupe dual de G s'identifie à celui de $G/D(G)$ son abélianisé.
(b) Le groupe dual de $\mathbb{Z}/n\mathbb{Z}$ est canoniquement isomorphe à μ_n (lui-même isomorphe à $(\mathbb{Z}/n\mathbb{Z})$.
(c) En admettant le théorème des structure des groupes abéliens finis, on a $\widehat{G} \cong G$ pour tout G abélien fini et alors $\widehat{\widehat{G}}$ canoniquement isomorphe à G.

Démonstration. (a) Comme tout caractère abélien sur G est à valeurs dans $\mathbb{C}^*$ commutatif, il est nul sur le groupe dérivé donc se factorise par $G/D(G)$ (et réciproquement, tout caractère abélien sur $G/D(G)$ se relève à G).
(b) L'isomorphisme est donné par

$$\begin{array}{ccc} \widehat{\mathbb{Z}/n\mathbb{Z}} & \longrightarrow & \mu_n \\ \chi & \longmapsto & \chi(\overline{1}) \end{array}.$$

En effet, on doit avoir $\chi(\overline{1})^n = \chi(\overline{n}) = \chi(0) = 1$ donc il est bien défini et clairement un morphisme, et réciproquement pour toute racine n-ième de l'unité ζ, on peut définir un unique χ tel que $\chi(\overline{1}) = \zeta$, qui à $\overline{k}$ associe ζ^k.
(c) Pour deux groupes finis G et G', on prouve directement que $\widehat{G \times G'} \cong \widehat{G} \times \widehat{G'}$ par restriction. En effet, si χ est un caractère sur $G \times G'$, les fonctions $g \mapsto \chi(g, 1)$ et $g' \mapsto \chi(1, g')$ définissent des caractères sur G et G' et réciproquement pour deux caractères χ_G et $\chi_{G'}$, on définit

$$\chi(g, g') := \chi_G(g)\chi_{G'}(g').$$

Ces constructions sont réciproques d'où l'isomorphisme.

En conséquence, avec le théorème de structure des groupes abéliens finis, si G est abélien fini, $G \bigoplus_i (\mathbb{Z}/n_i\mathbb{Z})$ et alors

$$\widehat{G} \cong \bigoplus_i \widehat{\mathbb{Z}/n_i\mathbb{Z}} \cong \bigoplus_i (\mathbb{Z}/n_i\mathbb{Z}) \cong G.$$

En particulier, $\widehat{G}$ a le même ordre que G. Ceci permet de conclure grâce à un plongement canonique de G dans $\widehat{\widehat{G}}$: à $g \in G$ on associe $\chi \mapsto \chi(g)$ et si g est non nul ce morphisme est non trivial (par exemple en réutilisant la décomposition plus haut et un caractère d'une composante où g est non nul). On a donc un morphisme de groupes injectif de G dans son bidual, et les cardinaux sont les mêmes grâce à l'argument précédent, donc un isomorphisme. □

3 Transformée de Fourier discrète

La transformée de Fourier discrète, qui a plusieurs formes (donc attention aux notations à chaque fois), consiste à associer à un ensenble de n valeurs (réelles ou complexes) un autre ensemble de n valeurs, via les racines de l'unité.

En pratique, les n valeurs sont indexées par $\{0, \cdots, n-1\}$ mais pour la théorie il va être très utile de se rappeler que cet ensemble correspond également à $\mathbb{Z}/n\mathbb{Z}$.

On se place dans un corps K contenant une racine n-ième primitive de l'unité ω_N (on prendra $e^{2i\pi/n}$ sur $\mathbb{C}$).

On se sert intuitivement des correspondances suivantes :

Suites périodiques de période n	Familles indexées par $\{0, \cdots, n-1\}$	Familles indexées par $\mathbb{Z}/n\mathbb{Z}$
$(x_k)_{k\geq 0}$	$(x_0, \cdots, x_{n-1})$	$(x_{\overline{k}})_{k\in\mathbb{Z}/n\mathbb{Z}}$

Alors, à toute suite x périodique de période N, on associe la transformée de Fourier discrète $F_N(x)$ de x définie par

$$F_n(x)_k = \sum_{j\in(\mathbb{Z}/n\mathbb{Z})} x_j \omega_n^{-jk} = \sum_{j\in(\mathbb{Z}/n\mathbb{Z})} x_j e^{-2i\pi jk/n}.$$

On définit de même $\overline{F_n}$ en remplaçant $-jk$ par jk dans l'exposant de ω_n.

Le lien avec la transformée de Fourier habituelle est que si $x_k = f(k/N)$ où f est une fonction 1-périodique intégrable sur $\mathbb{R}$, alors $F_N(x)$ tend vers la transformée de Fourier de f.

Proposition 3.1. *La transformée de Fourier discrète est un automorphisme linéaire de K^N tel que*

$$F_n^{-1} = \frac{1}{n}\overline{F_n}, \text{ autrement dit } (F_n \circ F_n(x))_k = n \cdot x_{-k}.$$

Démonstration. La linéarité est claire, il suffit de démontrer la deuxième formule. Pour tout $x \in K^{\mathbb{Z}/N\mathbb{Z}}$,

$$\begin{aligned}(F_N \circ \overline{F_N})(x)_k &= \sum_{j=0}^{N-1} (\overline{F_N}(x))_j \omega_N^{-jk} \\ &= \sum_{j=0}^{N-1}\sum_{\ell=0}^{N-1} x_\ell \omega_N^{j\ell}\omega_N^{-jk} \\ &= \sum_{\ell=0}^{N-1} x_\ell \sum_{j=0}^{N-1} \omega_N^{j(k-\ell)}.\end{aligned}$$

et la somme interne vaut 0 si $k \neq \ell$ et n si $k = \ell$ par la formule fondamentale. □

A priori, le calcul de la DFT de $x \in K^n$ (en ayant déjà précalculé les racines n-ièmes de l'unité dans K) est assez lent puisqu'il demande $O(n^2)$ opérations pris tel quel.

D'autre part (et cela sera crucial pour la suite), ce calcul revient en fait à calculer la valeur du polynôme

$$P(X) = \sum_{j=0}^{N-1} x_j X^j$$

en les ω_N^j (soit les racines N-ièmes de l'unité), plus précisément $F_N(x)_k = P(\omega_N^{-k})$.

Réciproquement, la transformée de Fourier inverse F_N^{-1}, qui a un temps comparable comme c'est $1/N \cdot \overline{F_N}$, revient à déterminere x elle-mêmeà partir des $P(\omega_N^k)$, autrement dit retrouver P à partir de son évaluation en les racines N-ièmes de l'unité.

Pour N une puissance de 2, nous allons voir la *transformée de Fourier rapide* (FFT), qui permet de calculer beaucoup plus rapidement F_N. Pour ceci, avec $N = 2M$, on écrit

$$P(X) = Q(X^2) + XR(X^2)$$

c'est-à-dire que Q regroupe les coefficients pairs et R les coefficients impairs, et alors, en prenant bien sûr $\omega_M = \omega_N^2$:

$$P(\omega_N^k) = Q(\omega_M^k) + \omega_N^k R(\omega_M^k)$$

Si on connaît les DFT de Q et R, on a donc simplement ensuite à calculer un produit et une somme pour chaque k pour évaluer la DFT de P, autrement dit le coût C_N de calcul de la DFT de P par cette réduction vérifie

$$C_N \leq 2C_M + 2N$$

(on peut même économiser des multiplications avec $\omega_N^{k+M} = -\omega_k$).

Cela mène donc à la complexité suivante.

Proposition 3.2. *Pour $N = 2^n$ et un corps K contenant une racine N-ième primitive et ses puissances déjà stockées, le coût de la FFT pour un $x \in K^N$ (et de la FFT inverse pour $P \in K_{N-1}[X]$) est en $O(N \ln(N))$ opérations élémentaires sur K.*

Cela fonctionne aussi pour N général en complétant par des zéros jusqu'à la prochaine puissance de 2.

Démonstration. Avec le calcul précédent, on a

$$C_{2^n} \leq 2C_{2^{n-1}} + 2^{n+1}$$

La suite $D_n = C_{2^n}/2^n$ vérifie donc $D_n \leq D_{n-1} + 2$, donc $D_n = O(n)$, et n est proportionnel à $\log_2 N$, ce qui prouve le résultat. □

Corollaire 3.3. *Avec les mêmes hypothèses sur N et K, la FFt permet de calculer le produit de deux polynômes $P, Q \in K[X]$ de degré au plus N avec un coût $O(N \ln(N))$.*

Démonstration. Tout d'abord, on utilise deux FFT pour évaluer les $P(\omega_{2N}^k), Q(\omega_{2N}^k)$, puis on fait les produits termes à termes ce qui nous donne $(PQ)(\omega_{2N}^k) = P(\omega_{2N}^k)Q(\omega_{2N}^k)$, et PQ étant de degré au plus $2N$, la FFT inverse appliquée à ces valeurs permet de déterminer PQ. On a utilisé un produit terme à terme ($O(2N)$) et trois FFT sur des polynômes de degrés au plus $2N$ $O(3N \ln(3N))$, soit un coût total en $O(N \ln(N))$. □

Remarque 3.4. Il existe un découpage différent de la forme $P(X) = X^M Q(X) + R(X)$ (plus présent dans les références), qui permet de calculer la FFT de manière similaire mais a l'avantage d'autoriser les calculs « en place » dans la mémoire, en écrasant le polynôme initial.

Définition 3.5.

3.1 Transformée de Fourier discrète, définitions et propriétés

3.2 Transformée de Fourier rapide et applications