CARACTÈRES DE DIRICHLET, SOMMES DE GAUSS ET THÉORÈME DE BOMBIERI-DAVENPORT.

Olivier Ramaré

Abstract. Nous rappelons rapidement ce que sont les caractères de Dirichlet et nous les exprimons en termes des caractères additifs de $\mathbb{Z}/q\mathbb{Z}$, introduisant ainsi les sommes de Gauss. Nous donnons alors l'extension grand crible de l'inégalité de Brun-Titchmarsh donnée par Bombieri & Davenport. Version du 25 Janvier 2000.

I. Les caractères de Dirichlet.

Nous supposons essentiellement que le lecteur est familier avec la dualité sur les groupes abéliens finis.

Le groupe multiplicatif de $\mathbb{Z}/q\mathbb{Z}$ sera noté $\mathcal{U}_q$ ou $\left(\mathbb{Z}/q\mathbb{Z}\right)^*$; il s'agit d'un groupe abélien fini. En ce qui concerne sa structure, rappelons que $\mathcal{U}_{p^k}$ est cyclique si $p \neq 2$ et $k \geq 1$ et que $\mathcal{U}_{2^{k+1}}$ est le produit direct de $\mathbb{Z}/2\mathbb{Z}$ par un 2-groupe cyclique.

Nous considérons alors $\widehat{\mathcal{U}_q}$ le groupe des caractères de $\mathcal{U}_q$, i.e. le groupe des morphismes de $(\mathcal{U}_q, \cdot)$ dans $(\mathbb{C} \setminus \{0\}, \cdot)$. Il est facile de voir qu'un tel morphisme prend ses valeurs dans les racines de l'unité et est donc de module 1. C'est un tel morphisme que l'on appelle *un caractère de Dirichlet*. La théorie générale nous apprend que $\widehat{\mathcal{U}_q}$ est isomorphe à $\mathcal{U}_q$ et en particulier est de cardinal $\phi(q)$.

Soit $\chi \in \widehat{\mathcal{U}_d}$ où d divise q. Nous pouvons bien sûr considérer χ sur $\mathcal{U}_q$ (en le composant avec la projection canonique) et le problème est de définir un d minimum tel que χ provienne de $\widehat{\mathcal{U}_d}$. Pour cela, notons le résultat suivant : si χ provient de $\widehat{\mathcal{U}_{d_1}}$ et de $\widehat{\mathcal{U}_{d_2}}$, alors χ provient de $\widehat{\mathcal{U}_{(d_1,d_2)}}$.

Preuve. Remarquons que χ provient de $\widehat{\mathcal{U}_d}$ si et seulement si l'ensemble $E_d = \{1 + kd, k \in \mathbb{Z}/q\mathbb{Z}\}$ est contenu dans $\operatorname{Ker}\chi$, tout simplement parce que E_d est le noyau de la projection canonique de $\mathcal{U}_q$ sur $\mathcal{U}_d$. Notre hypothèse nous dit donc que $E_{d_1} \subset \operatorname{Ker}\chi$ et similairement pour E_{d_2}. Mais il est facile de vérifier que $E_{d_1} \cdot E_{d_2} = E_{(d_1,d_2)}$, ce qui conclut la preuve. $\diamond\diamond\diamond$

Nous pouvons dès lors parler de *conducteur* d'un caractère, soit le plus petit f tel ce caractère provienne de $\widehat{\mathcal{U}_f}$. En particulier, le conducteur du caractère identiquement égal à 1, dit *principal*, est bien sûr 1. Un caractère modulo q de conducteur q est dit *primitif modulo q*

Si χ est un caractère de Dirichlet sur $\mathcal{U}_q$, nous l'étendons à $\mathbb{Z}/q\mathbb{Z}$ en posant $\chi(x) = 0$ si $(x, q) \neq 1$. Il est alors immédiat de vérifier que nous avons encore $\chi(xy) = \chi(x)\chi(y)$ pour tout x, y modulo q. De plus, nous étendons aussi χ à $\mathbb{Z}$ en le composant avec la surjection canonique. Il faut toutefois remarquer que même si χ modulo q provient de χ^* modulo f, en tant que fonction sur $\mathbb{Z}$, χ et χ^* sont distincts, tout simplement parce qu'ils ne prennent pas la même valeur sur les

entiers qui ne sont pas premiers à q. En particulier le caractère principal modulo q n'est pas, en tant que fonction sur $\mathbb{Z}$, la fonction identiquement égale à 1, ce qu'est pourtant le caractère principal modulo 1.

Nous ne souhaitons pas entrer dans les détails de la dualité de Pontrjagin dont le cadre naturel est la catégorie des groupes abéliens localement compact, mais il nous faut tout de même faire une remarque. Notre préoccupation ici est de déterminer le groupe des caractères de $\widehat{\mathcal{U}_q}$. Il se trouve qu'il est possible d'identifier naturellement ce "double-dual" avec $\mathcal{U}_q$ en remarquant que $\chi \mapsto \chi(x)$ est un caractère sur $\widehat{\mathcal{U}_q}$ dès que $x \in \mathcal{U}_q$. Un argument de comptage permet de montrer que nous avons bel et bien exhibé un isomorphisme entre $\widehat{\widehat{\mathcal{U}_q}}$ et $\mathcal{U}_q$.

II. Analyse de Fourier des caractères de Dirichlet.

Les caractères de Dirichlet présentent de remarquables propriétés L^2 qui viennent essentiellement de l'égalité suivante :

$$\sum_{x \mod {}^* q} \chi_1(x)\overline{\chi_2}(x) = \begin{cases} \phi(q) & \text{si} \quad \chi_1 = \chi_2, \\ 0 & \text{si} \quad \chi_1 \neq \chi_2, \end{cases}$$

dont la duale s'écrit :

$$\sum_{\chi \in \widehat{\mathcal{U}_q}} \chi(x_1)\overline{\chi}(x_2) = \begin{cases} \phi(q) & \text{si} \quad x_1 = x_2, \\ 0 & \text{si} \quad x_1 \neq x_2. \end{cases}$$

Preuve. Si $\chi_1 \neq \chi_2$, alors il existe x_0 tel que $\chi_1(x_0)\overline{\chi_2}(x_0) \neq 1$. Comme le produit par x_0 est un isomorphisme de $\mathcal{U}_q$, nous avons

$$\sum_{x \mod {}^* q} \chi_1(x)\overline{\chi_2}(x) = \sum_{x \mod {}^* q} \chi_1(x_0x)\overline{\chi_2}(x_0x)$$

d'où nous tirons

$$(1 - \chi_1(x_0)\overline{\chi_2}(x_0)) \sum_{x \mod {}^* q} \chi_1(x)\overline{\chi_2}(x) = 0.$$

Conclusion facile. $\diamond\diamond\diamond$

L'égalité duale se comprend mieux en notant que $\chi(x^{-1}) = \overline{\chi}(x)$.

Une fois ceci dûment noté, nous nous tournons vers la comparaison des structures additives et multiplicatives de $\mathbb{Z}/q\mathbb{Z}$. Les caractères de $(\mathbb{Z}/q\mathbb{Z}, +)$ sont les

$$x \mapsto e(ax/q)$$

et nous cherchons alors à exprimer les caractères multiplicatifs en termes de ces caractères additifs. Soit donc $\chi \in \widehat{\mathcal{U}_q}$. Regardons

$$\tau_q(\chi, a) = \sum_{x \mod {}^* q} \chi(x)e(ax/q).$$

L'inversion classique de Fourier (que l'on peut prouver ici directement) nous donne

$$\chi(n) = \frac{1}{q} \sum_{a \mod q} \tau_q(\chi, a)e(-an/q) \qquad (n \in \mathbb{Z}/q\mathbb{Z}).$$

Il nous faut à présent évaluer ces coefficients $\tau_q(\chi, a)$. L'égalité de Parseval nous donne

$$\sum_{a \mod q} |\tau_q(\chi, a)|^2 = q\phi(q).$$

Théorème 1. *Soit χ un caractère de Dirichlet modulo q et de conducteur f. Soit d un diviseur de q et soit $a' \in \mathbb{Z}/q\mathbb{Z}$ premier à d. Nous avons*

$$\tau_q(\chi, a'q/d) = \begin{cases} \mu(d/f)\overline{\chi^*(a')}\chi^*(d/f)\dfrac{\phi(q)}{\phi(d)}\tau_f(\chi,1) & \text{si} \quad f|d \quad \text{et} \quad (d/f, f) = 1, \\ 0 \qquad \text{sinon,} \end{cases}$$

où χ^* est le caractère induit par χ modulo f.

Preuve. Nous avons

$$\tau_q(\chi, a'q/d) = \sum_{b \mod q} e(a'b/d)\chi(b) = \sum_{c \mod d} e(a'c/d) \sum_{\substack{b \mod q \\ b \equiv c[d]}} \chi(b).$$

Introduisons le sous-groupe $E_d = \{b \mod q, b \equiv 1[d]\}$. Si $\operatorname{Ker}\chi \not\subset E_d$, alors les sommes intérieures sont nulles. Sinon, i.e. si $f|d$, χ est induit par un caractère modulo d que nous dénotons aussi par χ. Nous avons

$$\tau_q(\chi, a'q/d) = \frac{\phi(q)}{\phi(d)} \sum_{c \mod d} \chi(c)\, e(a'c/d) = \frac{\phi(q)}{\phi(d)}\tau_d(\chi, a').$$

Nous avons donc réduit notre problème initial au cas $d = q$. Comme alors $b \mapsto a'b$ est une bijection, nous avons

$$\tau_d(\chi, a') = \sum_{c \mod d} e(c/d)\chi(c)\overline{\chi(a')} = \overline{\chi(a')}\tau_d(\chi, 1).$$

Le conducteur de χ étant f, nous avons

$$\tau_d(\chi, 1) = \sum_{b \mod f} \chi(b) \sum_{\substack{c \mod {}^* d \\ c \equiv b[f]}} e(c/d)$$

La somme intérieure vaut 0 si $(d/f, f) \neq 1$ et $e(\nu b/f)\mu(d/f)$ sinon, où ν est l'inverse de d/f modulo f. Supposant dès lors que $(d/f, f) = 1$, nous constatons que l'expression ci-dessus égale $\mu(d/f)\chi^*(d/f)\tau_f(\chi)$ où χ^* est le caractère modulo f induit par χ. $\diamond\diamond\diamond$

Par conséquent seul $\tau_f(\chi, 1)$ importe vraiment. Pour ce qui est de son module, il nous suffit d'appliquer Parseval, et pour cela, de nous restreindre au cas $f = q$. Il vient alors

$$|\tau_f(\chi, 1)| = \sqrt{f} \qquad (\chi \text{ de conducteur } f).$$

Notons que lorsque χ est primitif, nous avons toujours

$$\begin{cases} \tau_q(\chi, a) = \overline{\chi}(a)\tau_q(\chi, 1) & (\forall a \in \mathbb{Z}/q\mathbb{Z}, \quad \chi \text{ primitif}), \\ \tau_q(\chi, a) = \overline{\chi}(a)\tau_q(\chi, 1) & (\forall a \in \mathcal{U}_q, \quad \chi \text{ quelconque}). \end{cases}$$

ce qui montre clairement que nous n'avons pas vraiment calculé la transformée de Fourier de χ, mais bien plutôt établi une équation reliant cette transformée à χ.

III. Le théorème de Bombieri-Davenport.

Rappelons l'inégalité du grand crible pour la suite de Farey :

$$\sum_{q\le Q}\sum_{a \bmod^* q} |S(a/q)|^2 \le \sum_{n\le N} |\varphi_n|^2 (N+Q^2) \tag{3.1}$$

où

$$S(\alpha) = \sum_{M<n\le M+N} \varphi_n\, e(n\alpha). \tag{3.2}$$

Ajoutons alors une hypothèse (H) sur la suite (φ_n) : nous supposons qu'elle est portée par $(\mathcal{U}_q)$ jusqu'au niveau Q, ou, dit autrement,

$$(H) \qquad \forall n \in]M, M+N] \quad \big[\varphi_n \neq 0 \implies \forall q \le Q (n,q)=1\big].$$

Dans ce cadre, nous définissons

$$G_q(Q/q) = \sum_{\substack{d\le Q/q\\(d,q)=1}} \frac{\mu^2(q)}{\phi(q)} \tag{3.3}$$

et rappelons que nous avons montré que $G_q(Q/q) \ge \frac{\phi(q)}{q}\operatorname{Log}(Q/q)$. Nous posons enfin

$$S(\chi) = \sum_{n\in]M,M+N]} \varphi_n\, \chi(n) \tag{3.4}$$

la distinction entre (3.2) et (3.4) étant clair d'après le contexte.

Théorème (Bombieri & Davenport –1968). *Si (φ_n) vérifie (H), alors*

$$\sum_{q\le Q} \frac{q}{\phi(q)} G_q(Q/q) \sum_{\chi\in\widehat{\mathcal{U}_q}^*} |S(\chi)|^2 \le \sum_{n\in]M,M+N]} |\varphi_n|^2 (N+Q^2)$$

où $\widehat{\mathcal{U}_q}^*$ est l'ensemble des caractères primitifs modulo q.

En restreignant le membre de gauche à $q=1$, nous obtenons :

Corollaire. *Si (φ_n) vérifie (H), alors*

$$\big|S(0)\big|^2 \le \sum_{n\in]M,M+N]} |\varphi_n|^2 \frac{N+Q^2}{G_1(Q)}.$$

Preuve. Soit $e_{\mathcal{U}_d}(\cdot a/d)$ la fonction définie par

$$e_{\mathcal{U}_d}(na/d) = \begin{cases} e(na/d) & \text{si} \quad n\in\mathcal{U}_d,\\ 0 & \text{sinon.}\end{cases}$$

Comme $\widehat{\mathcal{U}_d}$ forme une base orthogonale de l'espace vectoriels des fonctions sur $\mathcal{U}_d$, nous pouvons exprimer $e_{\mathcal{U}_d}(\cdot a/d)$ en termes des caractères odulo d et plus précisément :

$$e_{\mathcal{U}_d}(na/d) = \sum_{\chi\in\widehat{\mathcal{U}_d}} [e_{\mathcal{U}_d}(\cdot a/d)|\chi]\,\chi(n) \quad \text{avec} \quad [e_{\mathcal{U}_d}(\cdot a/d)|\chi] = \frac{1}{\phi(d)}\sum_{k\in\mathcal{U}_d} e(ka/d)\overline{\chi}(k).$$

Par ailleurs, par (H), nous avons

$$S(a/d) = \sum_{n\leq N} \varphi_n\, e_{\mathcal{U}_d}(na/d) = \sum_{\chi\in\widehat{\mathcal{U}_d}} [e_{\mathcal{U}_d}(\cdot a/d)|\chi]\, S(\chi).$$

Il vient

$$\sum_{a \mod d} |S(a/d)|^2 = \sum_{\chi_1,\chi_2\in\widehat{\mathcal{U}_d}} S(\chi_1)\overline{S(\chi_2)} \sum_{a \mod d} [e_{\mathcal{U}_d}(\cdot a/d)|\chi_1]\,\overline{[a/d|\chi_2]}$$

où l'on reconnaît en somme intérieure le produit scalaire (à normalisation près) de χ_1 et χ_2 exprimé dans la base $(e(\cdot a/d))$. Par conséquent

$$\sum_{a \mod d} |S(a/d)|^2 = \frac{d}{\phi(d)} \sum_{\chi\in\widehat{\mathcal{U}_d}} |S(\chi)|^2.$$

En posant

$$W(f) = \sum_{\chi\in\widehat{\mathcal{U}_q}^*} |S(\chi)|^2$$

nous avons donc établi

$$\sum_{q|d} \sum_{a \mod {}^* q} |S(a/q)|^2 = \frac{d}{\phi(d)} \sum_{f|d} W(f).$$

Nous utilisons alors la formule d'inversion de Mœbius pour obtenir

$$\begin{aligned}\sum_{a \mod {}^* q} |S(a/q)|^2 &= \sum_{d|q} \mu(q/d)\frac{d}{\phi(d)} \sum_{f|d} W(f) \\ &= \sum_{f|q} \left(\sum_{f|d|q} \mu(q/d)\frac{d}{\phi(d)} \right) W(f)\end{aligned}$$

et il nous suffit à présent de calculer la somme interne. Par multiplicativité, nous vérifions que

$$\sum_{f|d|q} \mu(q/d)\frac{d}{\phi(d)} = \prod_p \left(\sum_{p^{|v_p(f)}|p^a|p^{v_p(q)}} \mu(p^{v_p(q)-a})\frac{p^a}{\phi(p^a)} \right).$$

Il nous reste à évaluer les facteurs locaux. Or

(1) Si $v_p(f) \geq 1$ et $v_p(q) - v_p(f) \geq 1$ alors ce facteur vaut 0.
(2) Si $v_p(f) \geq 1$ et $v_p(q) = v_p(f)$ alors ce facteur vaut $\frac{p^{v_p(f)}}{\phi(p^{v_p(f)})}$.
(3) Si $v_p(f) = 0$ et $v_p(q) \geq 2$ alors ce facteur vaut 0.
(4) Si $v_p(f) = 0$ et $v_p(q) = 1$ alors ce facteur vaut $1/\phi(p)$.

Nous en tirons une expression globale qui nous donne

$$\sum_{a \mod {}^*q} |S(a/d)|^2 = \sum_{\substack{f|q \\ (f,q/f)=1}} \frac{f}{\phi(f)} \mu^2(q/f)\phi(q/f)W(f)$$

qu'il nous suffit alors d'insérer dans (3.1) pour obtenir l'inégalité annoncée. $\diamond\diamond\diamond$

Remarquons que contrairement à la preuve usuelle (comme elle est par exemple reprise dans le livre de Bombieri cité ci-dessous), celle que nous avons présentée n'utilise pas la valeur des sommes de Gauss et en particulier ignore le fait que les χ soient multiplicatifs.

References

E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Astérisque **18** (1974/1987), 103pp.

E. Bombieri & H. Davenport, *On the large sieve method*, Deut. Verlag Wiss., Berlin (1968), 11–22.

P.X. Gallagher, *Sieving by prime powers*, Acta Arith. **24** (1974), 491–497.