Chapitre 11

Caractères de Dirichlet

11.1 Caractères de groupes

Soit G un groupe abélien fini. Un caractère de G est un homomorphisme de G dans le groupe multiplicatif $\mathbb{C}^*$ des nombres complexes. On note $\hat{G}$ l'ensemble des caractères de G, que l'on munit de la structure naturelle de groupe multiplicatif (c'est à dire pour χ_1 et χ_2 deux caractères de G, $\chi_1\chi_2$ est l'homomorphisme $x \mapsto \chi_1(x)\chi_2(x)$) L'élément neutre de $\hat{G}$(l'identité sur G), appelé caractère principal de G, sera noté χ_0 ou 1. Il faut noter que l'inverse du caractère χ est $\overline{\chi} : x \mapsto \overline{\chi(x)}$.

11.2 Caractères sur $\mathbb{Z}/n\mathbb{Z}$

Déterminons les caractères de $(\mathbb{Z}/n\mathbb{Z}, +)$, pour n entier quelconque. Nous considèrons pour $a \in \mathbb{Z}/n\mathbb{Z}$:

$$\begin{array}{rccc} f_a : & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{C} \\ & x & \mapsto & e^{2i\pi ax/n} \end{array} \tag{11.1}$$

C'est un caractère de $(\mathbb{Z}/n\mathbb{Z}, +)$, et tout caractère de $(\mathbb{Z}/n\mathbb{Z}, +)$ est de ce type. En effet soit χ un tel caractère. On a : $\chi(1)^n = 1$ donc $\chi(1) = \omega$ est une racine n-ième de l'unité, et χ est alors tout simplement l'application $\mapsto \omega^x$.

L'application

$$\begin{array}{c} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ a \mapsto f_a \end{array} \tag{11.2}$$

est donc clairement un isomorphisme : le groupe des caractères de $\mathbb{Z}/n\mathbb{Z}$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

11.3 Caractères de groupes abéliens finis

Théorème 17. *Soit G un groupe abélien fini. Son groupe des caractères est isomorphe à G.*

Nous établissons ce résultat en deux étapes.

Première étape

Nous remarquons que :

$$\begin{array}{l} \hat{G}_1 \times \hat{G}_2 \to \widehat{G_1 \times G_2} \\ (\chi 1, \chi 2) \mapsto \chi_1 \times \chi_2 : G_1 \times G_2 \to \mathbb{C} \\ \qquad\qquad\qquad (x_1, x_2) \mapsto \chi_1(x_1)\chi_2(x_2) \end{array} \tag{11.3}$$

est une bijection.

Preuve. L'injectivité est triviale :

$$\chi_1\chi_2 = 1 \implies (\chi_1\chi_2)(x_1, 0) = 1 = \chi_1(x_1),$$

et cela pour tout $x_1 \in G_1$, donc $\chi_1 = 1$. De même $\chi_2 = 1$.

Pour la surjectivité, on voit que si χ est un caractère de $\widehat{G_1 \times G_2}$, $\chi_1 : x1 \mapsto \chi(x1, 0)$ est un caractère de G_1, de même on définit χ_2 ; on a bien $\chi_1(x_1)\chi_2(x_2) = \chi(x_1, x_2)$. ◇◇◇

Seconde étape

Pour montrer comme annoncé que $\hat{G} \simeq G$, on écrit G comme produit de groupes abéliens cycliques :

$$G \simeq \prod_{i=1} \mathbb{Z}/n_i\mathbb{Z}.$$

En appliquant le lemme ci-dessus par récurrence, on obtient

$$\hat{G} \simeq \prod_{i=1} \widehat{\mathbb{Z}/n_i\mathbb{Z}} \simeq \prod_{i=1} \mathbb{Z}/n_i\mathbb{Z} \simeq G.$$

Finissons cette partie par une digression. La transformation, dite de Gelfond,

$$\begin{aligned} G &\to \hat{\hat{G}} \\ x &\mapsto \hat{x} : \hat{G} \to G \\ &\qquad \chi \mapsto \chi(x) \end{aligned}$$

induit un isomorphime entre G et $\hat{\hat{G}}$. Nous laissons la démonstration aux soins du lecteur. Il faut noter que cet isomorphisme est parfaitement canonique, alors qu'il n'en existe pas de G à $\hat{G}$.

11.4 Une structure quadratique

Lemme 18. *On a les relations suivantes, dites d'orthogonalité :*

$$\sum_{x\in G}\chi(x) = \begin{cases} |G| & si\ \chi = \chi_0 \\ 0 & sinon \end{cases}, \sum_{\chi\in\hat{G}}\chi(x) = \begin{cases} |G| & si\ x = 0 \\ 0 & sinon \end{cases}$$

et

$$\sum_{x\in G}\chi_1(x)\overline{\chi_2(x)} = \begin{cases} |G| & si\ \chi_1 = \chi_2 \\ 0 & sinon \end{cases}$$

$$\sum_{\chi\in\hat{G}}\chi(x)\overline{\chi(y)} = \begin{cases} |G| & si\ x = y \\ 0 & sinon. \end{cases}$$

Preuve. Comme $\chi \neq \chi_0$, il existe un y tel que $\chi(y) \neq 0$. Il vient alors

$$\sum_{x\in G}\chi(x) = \sum_{x\in G}\chi(x+y) = \chi(y)\sum_{x\in G}\chi(x).$$

Nous laissons les autres vérifications au lecteur. De façon notiore, il faut montrer que, si $x \neq 0$, il existe $\chi \in \hat{G}$ tel que $\chi(x) \neq 1$. ◇◇◇

Lemme 19 (Décomposition de Fourier)**.** *Pour une fonction $f : G \to \mathbb{C}$, on a :*

$$f(x) = \sum_{\chi \in \hat{G}} \hat{f}(\chi)\chi(x)$$

avec

$$\hat{f}(\chi) = \sum_{y \in G} f(y)\overline{\chi(y)}/|G|.$$

Pour $G = (\mathbb{Z}/n\mathbb{Z}, +)$, cette décomposition est tout simplement :

$$f(x) = \sum_{a \bmod n} \hat{f}(a)e^{2i\pi a/n} \quad \text{où} \quad \hat{f}(a) = \sum_{y \bmod n} f(y)e^{-2i\pi y/n}/n.$$

11.5 Caractères de Dirichlet

On applique le cas précédent à $G = ((\mathbb{Z}/q\mathbb{Z})^*, x)$. Si χ est un caractère de $(\mathbb{Z}/q\mathbb{Z})^*$, on l'étend à $\mathbb{Z}/q\mathbb{Z}$ en posant $\chi(x) = 0$ si $(x, q) \neq 1$. On étend ensuite χ à $\mathbb{Z}$, en composant avec la projection canonique $\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$; on remarquera que l'on obtient alors une fonction arithmétique complètement multiplicative.

Nous disposons donc de trois fonctions que nous notons toutes χ et que nous appelons toutes des *caractères de Dirichlet* :

1. une qui va de $(\mathbb{Z}/q\mathbb{Z})^*$ dans $\mathbb{C}$.
2. une qui va de $\mathbb{Z}/q\mathbb{Z}$ dans $\mathbb{C}$.
3. une qui va de $\mathbb{Z}$ dans $\mathbb{C}$.

La distinction est claire d'après le contexte.

Dans la suite de cette section, on se restreint à q premier

Exemples :

1. Un caractère général. Soit g un générateur de $(\mathbb{Z}/q\mathbb{Z})^*$. Un tel générateur existe car ce groupe est cyclique. Considérons

$$\begin{aligned} \chi : \mathbb{Z}/q\mathbb{Z} &\to \mathbb{C} \\ x = g^t &\mapsto \exp(2i\pi t/(q-1)) \\ 0 &\mapsto 0 \end{aligned} \tag{11.4}$$

   Il s'agit là de la forme générale des caractères de Dirichlet modulo q.

2. Caractère quadratique. Soit H le sous-groupe des carrés de $(\mathbb{Z}/q\mathbb{Z})^*$, on a $|H| = \frac{q-1}{2}$.

$$\begin{aligned} \chi : \mathbb{Z}/q\mathbb{Z} &\to \mathbb{Z}/q\mathbb{Z} \\ x &\mapsto x^{(q-1)/2} \\ 0 &\mapsto 0 \end{aligned} \tag{11.5}$$

   Ce caractère arrive dans $\{0, \pm 1\}$: il nous est facile de voir ces valeurs dans $\mathbb{C}$. Ce caractère est tout simplement du symbole de Legendre $(\frac{x}{q})$; il est quadratique ($\chi^2 = 1$).

Dans le premier cas, la difficulté vient de ce que nous ne savons pas déterminer de générateur g, et ensuite nous ne savons pas déterminer un logarithme en base g (i.e. déterminer le t tel que $x = g^t$). Dans le second cas, la définition évite la notion de générateur est évitée, mais nous ne savons pas plus comment nous y prendre. Ce dernier cas est crucial.

11.6 Inégalité de Polya-Vinogradov

Théorème 18 (Polya-Vinogradov)**.** *Soit χ un caractère de Dirichlet non principal modulo q, avec q premier. On a :*

$$\forall N \geq 1, \quad \Big| \sum_{1 \leq n \leq N} \chi(n) \Big| \leq \sqrt{q} \operatorname{Log} q.$$

La majoration donnée par le théorème pour $N \leq q \operatorname{Log} q$ est moins bonne que la majoration triviale $|\sum_{n \leq N} \chi(n)| \leq N$ (car $|\chi(n)| \leq 1$).

Par contre, pour $N > q \operatorname{Log} q$, la majoration implique que les $\chi(n)$ ne peuvent pas être tous égaux à 1 : des compensations doivent se produire pour avoir une telle majoration. On trouve ainsi, pour χ caractère réel non principal, que le plus petit n tel que $\chi(n) = -1$ est $\leq \sqrt{q} \operatorname{Log} q$. Nous renvoyons le lecteur à la section 17.3 pour d'autres renseignements sur ce problème.

Pour étendre cette inégalité au cas d'un caractère modulo un module qui ne soit pas nécessairement premier, le lecteur est encouragé à d'abord lire la section 24.

Preuve. On développe χ en caractères additifs :

$$\chi(n) = \sum_{a \bmod q} \hat{\chi}(a) e(na/q) \quad \text{avec} \quad \hat{\chi}(a) = \sum_{b \bmod {}^* q} \chi(b) e(-ab/q)/q.$$

Par changement de variable $c = ab$ dans la somme pour $a \neq 0$, on obtient

$$\hat{\chi}(a) = \overline{\chi}(a) \sum_{c \bmod^* q} \chi(c) e(-c/q)/q$$

et par conséquent, pour tout $a \bmod^* q$, nous avons $|\hat{\chi}(a)| = |\hat{\chi}(1)|$, alors que $\hat{\chi}(0) = 0$. On vérifie par ailleurs directement que

$$\sum_{n \bmod q} |\chi(n)|^2 = q \sum_{a \bmod q} |\hat{\chi}(a)|^2.$$

d'où $q - 1 = q(q-1)|\hat{\chi}(1)|^2$ ce qui résulte en

$$|\hat{\chi}(1)| = 1/\sqrt{q}.$$

Nous reprenons ici le cours de la preuve principale :

$$\sum_{1 \leq n \leq N} \chi(n) = \sum_{b \bmod^* q} \chi(b) \sum_{1 \leq n \leq N} e(-nb/q)/q.$$

Cette technique porte le nom de *passage à une somme complète*. En effet, la somme initiale pour sur les valeurs $\chi(n)$ pour n dans un intervalle alors que la somme finale porte sur les valeurs $\chi(b)$ où b parcourt un système complet de résidus modulo q.

Or $|(e(Nb/q)-1)/(e(b/q)-1)| = 1/|\sin(\pi b/q)| \leq q/(2b)$. Donc la somme ci-dessus est majorée par :

$$\sum_{\substack{-q/2 < b \leq q/2 \\ b \neq 0}} \frac{1}{\sqrt{q}} \frac{q}{2b} \leq \sqrt{q} \operatorname{Log} q.$$

En effet puisque q est premier, il s'agit de montrer que

$$\sum_{1 \leq b \leq (q-1)/2} 1/b \leq \operatorname{Log} q$$

ce que nous laissons au lecteur. ◇◇◇

11.7 Conducteurs et caractères primitifs

Ici, nous ne nous restreignons plus à q premier.

Soit $\chi : \mathbb{Z} \to \mathbb{C}$ un caractère de Dirichlet. Lorsque nous regardons un caractère ainsi, il lui est associé un *module*. En effet ce caractère vient de $\mathbb{Z}/q\mathbb{Z}$ mais ce q semble avoir disparu de la définition de χ. Il n'est d'ailleurs pas évident que deux caractères, l'un modulo q_1 et l'autre modulo q_2 ne soient pas égaux vu sur $\mathbb{Z}$. Et c'est effectivement faux ! En effet, prenons un caractère χ modulo un nombre premier p et remontons le en un caractère χ' modulo p^2. Nous notons encore χ et χ' les caractères associés sur $\mathbb{Z}$. Si x est premier à p, nous avons $\chi(x) = \chi'(x)$ et si $p|x$, $\chi'(x) = 0 = \chi(x)$.

Nous ne pouvons donc pas parler du *module* d'un caractère de Dirichlet sans ambigüités, mais nous pouvons parler *d'un* module. Nous pourrions montrer que tous ces modules admissibles sont en fait les multiples d'un plus petit module commun, mais nous préférons nous concentrer sur une notion plus efficace. En effet les valeurs où χ est non nulle sont les plus importantes. Aussi définissons nous la relation d'équivalence suivant :

> *Deux caractères χ_1 modulo q_1 et χ_2 modulo q_2 sont dits équivalents si, dès que $(n, q_1q_2) = 1$, on a $\chi_1(n) = \chi_2(n)$.*

Il s'agit bien d'une relation d'équivalence. Et ici, quand nous disons "χ_1 modulo q_1", nous entendons "χ_1 dont un module est q_1".

Si $d|q$, un caractère χ sur $(\mathbb{Z}/d\mathbb{Z})^*$ se remonte à $(\mathbb{Z}/q\mathbb{Z})^*$ en un caractère χ' tout simplement en posant $\chi'(x) = \chi(x \bmod d)$. Nous pouvons ensuite remonter χ et χ' à $\mathbb{Z}$ et nous obtenons deux caractères de Dirichlet a priori différents (mais pas toujours come nous l'avons remarqué plus haut). Toutefois, l'essentiel de l'information est contenue dans le plus caractère de plus petit module. Nous disons que χ' *vient* de χ.

Étant donné un caractère χ', il s'agit de définir si possible un caractère de module minimal dont χ' viendrait, c'est à dire de déterminer un plus petit élément dans la chaque classe de la relation d'équivalence définie ci-dessus.

Le lemme essentiel ici est le suivant.

Lemme 20. *Si χ_1 modulo q_1 est équivalent à χ_2 modulo q_2, il existe un caractère χ modulo $q = (q_1, q_2)$ qui leur est équivalent.*

Preuve. Remarquons tout d'abord que dans toute progression $(x + \ell q_1)_\ell$ où x et q_1 sont premiers entre eux, nous pouvons trouver x' qui est premier à tout entier fixé par avance. En particulier, il existe des points dans cette

progressions qui sont premiers q_2. Une fois cela établi, notons qu'il existe a et b des entiers tels que $q = aq_1 + bq_2$. Nous en arrivons au point central : si $x \equiv y[q]$ et si $(xy, q_1) = 1$, alors $\chi_1(x) = \chi_1(y)$. En effet il existe u et v tels que $x = y + uq_1 + vq_2$ et l'on a $\chi_1(x) = \chi_1(x - uq_1)$. Par ailleurs nous pouvons ajouter disons wq_1 de sorte que $x - uq_1 + wq_1$ soit premier à q_2. Par conséquent

$$\begin{aligned}\chi_1(x) = \chi_1(x - uq_1 + wq_1) &= \chi_2(x - uq_1 + wq_1)\\ &= \chi_2(y + vq_2 + wq_1) = \chi_2(y + wq_1) = \chi_1(y + wq_1) = \chi_1(y)\end{aligned}$$

ce qu'il nous fallait. Ceci nous permet de définir un caractère χ modulo q qui coincide avec χ_1 sur les entiers premiers à q_1 et avec χ_2 sur les entiers premiers à q_2. ◇◇◇

Pour un caractère χ donné, le plus petit entier $\mathfrak{f}$ tel que χ est équivalent à un caractère modulo $\mathfrak{f}$ [1] est appelé le conducteur de χ. Un caractère modulo $\mathfrak{f}$ est dit primitif si son conducteur est $\mathfrak{f}$.

La situation est alors la suivante : nous partons d'un caractère χ modulo q et lui associons un caractère primitif χ^* modulo $\mathfrak{f}|q$ de telle sorte que

$$\chi(x) = \begin{cases}\chi^*(x) & \text{si } (x,q) = 1,\\ 0 & \text{sinon.}\end{cases}$$

Il est facile de dénombrer les caractères primitifs modulo q. Soit $H(q)$ un tel nombre. Nous avons $\sum_{\mathfrak{f}|q} H(\mathfrak{f}) = \phi(q)$ ce qui se traduit par $H = \mu \star \phi$, ou encore par $H(q) = \prod_{p^\alpha \| q} H(p^\alpha)$ et

$$H(p) = p - 2, \quad H(p^\alpha) = p^{\alpha-2}(p-1)^2 \quad \text{si } \alpha \geq 2.$$

Nous laissons le lecteur déterminer la série de Dirichlet associée, ainsi que l'ordre moyen de cette fonction multiplicative positive.

Dans la suite, nous aurons l'occasion d'utiliser des notations comme

$$\mathbb{1}_{n\equiv a[q]} = \sum_{\chi \bmod q} \overline{\chi}(a)\chi(a) \tag{11.6}$$

où $\sum_{\chi \bmod q}$ désigne une somme sur tous les *caractères multiplicatifs* modulo q, et non une somme sur une système entier de résidu modulo q. Et $\sum_{\chi \bmod^* q}$ désignera une somme sur tous les caractères primitifs modulo q.

1. La lettre $\mathfrak{f}$ provient de l'allemand Führer, qui signifie "conducteur".