Chapitre 2 : le théorème des nombres premiers

① Caractères des groupes abéliens finis

Soit G un groupe abélien fini.

Définition. Un caractère de G est un morphisme de groupes $\chi : G \to \mathbb{C}^\times$.
On note $\hat{G}$ l'ensemble des caractères de G.

* Si G est d'ordre n, alors $g^n = e$ pour tout $g \in G$, d'où $\chi(g)^n = \chi(g^n) = \chi(e) = 1$. Un caractère prend donc ses valeurs dans les racines de l'unité.

* $\hat{G}$ est un groupe, d'élément neutre le caractère trivial $\chi(g) = 1$ pour tout g. Comme

$$1 = |\chi(g)| = \chi(g)\,\overline{\chi(g)}$$

l'inverse d'un caractère est son conjugué $\overline{\chi}$.

Exemple : Si G est cyclique d'ordre n, alors $\hat{G}$ est isomorphe à $\mu_n(\mathbb{C}) = \{\xi \in \mathbb{C} \mid \xi^n = 1\}$.

En effet, comme tout élément de G est de la forme g^a, un caractère χ est déterminé par $\chi(g)$, qui est une racine n-ième de l'unité.

Réciproquement, si $\zeta \in \mu_n(\mathbb{C})$, alors

$$G \longrightarrow \mathbb{C}^\times \quad \text{pour } 0 \le a < n$$
$$g^a \longmapsto \zeta^a$$

est un caractère de G.

$\Rightarrow |\hat{G}| = |G|$ et ils sont même isomorphes.

En général :

Proposition : Soit G un groupe abélien fini. Alors $\hat{G}$ a le même cardinal que G.

(G et $\hat{G}$ sont en fait des groupes isomorphes)

La démonstration repose sur le lemme suivant :

Lemme : Soit H un sous-groupe de G. Pour tout caractère χ_1 de H, il existe un caractère χ de G tel que $\chi_{|H} = \chi_1$.

Preuve : Par récurrence sur l'indice $\frac{|G|}{|H|} = (G:H)$.

* Si $(G:H) = 1$, rien à démontrer.
* Sinon, soit $g \in G \setminus H$ et soit m le plus petit entier tel que $g^m \in H$. Soit

$$H \subset H' = \{ g^a h \mid 0 \le a < m, \ h \in H \} \subset G$$
$$\geq 2$$

C'est un sous-groupe car G est abélien. Si

$$g^a h = g^b h' \Rightarrow g^{b-a} = h h' \in H$$
$$0 \le a \le b < m$$
$$h, h' \in H$$

$\Rightarrow b = a$, $h = h'$ par minimalité de m.

∴ Tout élément de H' s'écrit de même sorte comme $g^q h$.

Soit $\xi \in \mathbb{C}$ tel que $\xi^m = \chi_1(g^m)$ ($g^m \in H$). Pour $x = g^a h$, posons $\chi'(x) = \xi^a \chi_1(h)$

c'est un caractère :

$$\chi'(xy) = \chi'(g^{a+b} hh')$$

($x = g^a h$, $y = g^b h'$)

Si $a+b < m$, $= \xi^{a+b} \chi_1(h)\chi_1(h')$

$$= \chi'(x)\chi'(y)$$

Si $a+b \geq m$, alors $a+b < 2m$,

$$= \chi'(g^{a+b-m} \underbrace{g^m hh'}_{\in H})$$

$$= \xi^{a+b-m} \underbrace{\chi_1(g^m)}_{\xi^m} \chi_1(h)\chi_1(h')$$

$$= \chi'(x)\chi'(y)$$

On a donc étendu le caractère à H', et

$$(G:H') = \frac{(G:H)}{m} < (G:H)$$

Par récurrence, il existe χ caractère de G tel que $\chi_{|H'} = \chi'$, donc $\chi_{|H} = \chi_1$ ▨

Preuve de la proposition : OK pour G cyclique.

Récurrence sur l'ordre $|G|$. Cas $|G| = 1, 2, 3$ OK.

* Soit $h \in G \setminus \{e\}$, $H = \langle h \rangle \subset G$ le sous-groupe cyclique qu'il engendre, $n = |H|$. On a $n > 1$.

* H cyclique $\Rightarrow$ pour toute racine $\zeta \in \mu_n(\mathbb{C})$, il existe un unique caractère $\tilde{\chi}_\zeta$ de H avec $\tilde{\chi}_\zeta(h) = \zeta$.

* Par le lemme, on peut les prolonger en des caractères χ_ζ de G.

* G/H est d'ordre $k = \frac{|G|}{n} < |G|$ Par récurrence, $\bar{\theta}_1, \dots, \bar{\theta}_k$ caractères distincts de G/H

$\theta_i : G \longrightarrow G/H \xrightarrow{\bar{\theta}_i} \mathbb{C}^\times$

satisfaisant à $\theta_i|_H = 1$.

* Introduisons

$$\chi_\zeta \theta_i : G \longrightarrow \mathbb{C}^\times \qquad i = 1, \dots, k \quad \zeta \in \mu_n(\mathbb{C})$$

Ils sont deux à deux distincts :

$\chi_\zeta \theta_i = \chi_{\zeta'} \theta_j$ donne $\zeta = \zeta'$ par restriction à H, puis $\theta_i = \theta_j$

$\therefore$ $k n = |G|$ caractères distincts

Réciproquement, si χ est un caractère de G, $\chi_{|H}$ est de la forme $\tilde{\chi}_\xi$ pour $\xi \in \mu_m(\mathbb{C})$.

Alors $\chi \chi_\xi^{-1}$ vaut 1 sur H, donc donne lieu à un caractère de G/H, donc il est égal à θ_i pour un $i = 1, \dots, k$.

$$\Rightarrow \chi = \chi_\xi \theta_i$$

et on a trouvé tous les caractères □

Remarque : Dans la preuve, on a vu que si h est un élément d'un groupe abélien fini G et $h \neq e$, alors il existe un caractère χ de G tel que $\chi(h) \neq 1$. (« les caractères séparent les points »)

Proposition : Soit G abélien fini.

(1) Pour tout caractère χ de G,

$$\sum_{g \in G} \chi(g) = \begin{cases} 0 & \text{si } \chi \neq 1 \\ |G| & \text{si } \chi = 1 \end{cases}$$

(2) Pour tout élément $g \in G$,

$$\sum_{\chi \in \hat{G}} \chi(g) = \begin{cases} 0 & \text{si } g \neq e \\ |G| & \text{si } g = e \end{cases}$$

Preuve : ① le cas $\chi = 1$ est évident.

Si $\chi \neq 1$, soit h tel que $\chi(h) \neq 1$. Alors :

$$\sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(hg) = \chi(h) \sum_{g \in G} \chi(g)$$

□

donc $\sum_{g \in G} \chi(g) = 0$

② Si $g \neq e$, il existe $\Psi \in \hat{G}$ tel que $\Psi(g) \neq 1$.

Alors

$$\sum_{\chi \in \hat{G}} \chi(g) = \sum_{\chi \in \hat{G}} (\Psi\chi)(g) = \Psi(g) \sum_{\chi \in \hat{G}} \chi(g)$$

d'où $\sum_{\chi \in \hat{G}} \chi(g) = 0$. Dans le cas $g = e$,

$$\sum_{\chi \in \hat{G}} \chi(g) = |\hat{G}| = |G|$$

par la proposition

□

② Caractères modulaires

Soit $N \geq 1$ un entier. On considère

$G = (\mathbb{Z}/N\mathbb{Z})^\times$ groupe abélien fini à $\varphi(N)$ éléments

Définition : Un caractère de Dirichet modulo N est un caractère de $(\mathbb{Z}/N\mathbb{Z})^\times$, i.e.

un homomorphisme de groupes $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$.

On peut le voir comme une fonction

$$\chi : \mathbb{Z} \to \mathbb{C}$$

en définissant

$$\chi(a) = \begin{cases} 0 & \text{si } a \text{ et } N \text{ ne sont pas premiers entre eux} \\ \chi(a \bmod N) & \text{si } a \text{ et } N \text{ sont premiers entre eux} \end{cases}$$

Cette fonction satisfait à

$$\chi(ab) = \chi(a)\chi(b)$$

pour tous $a, b \in \mathbb{Z}$

Exemple : Si $N = p$ est premier, alors $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$, donc le groupe de caractères aussi. Si $p \geq 3$, il existe un unique caractère $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ d'ordre 2 (qui prend donc des valeurs dans $\{\pm 1\}$) : c'est le caractère de Legendre

$$\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \{\pm 1\}$$
$$a \longmapsto \left(\frac{a}{p}\right)$$

Il est non trivial car il prend (autant de fois que la valeur 1) la valeur -1.

Lemme : Soit a un entier non nul sans facteur carré (c'est-à-dire $v_p(a) \in \{0,1\}$ pour tout nombre premier p). Soit $N = 4|a|$. Il existe un unique caractère χ_a modulo n tel que $\chi_a(p) = \left(\frac{a}{p}\right)$ pour tout p qui ne divise pas a. Il vérifie $\chi_a^2 = 1$ et $\chi_a \neq 1$ si $a \neq 1$.

Preuve : Comme tous les éléments de $(\mathbb{Z}/n\mathbb{Z})^\times$ sont des produits de premiers qui ne divisent pas n, s'il existe χ_a est unique et satisfait $\chi_a^2 = 1$.

Existence : si $a = \ell_1 \dots \ell_k$, où les ℓ_i sont des premiers impairs distincts, on pose

$$\chi_a(x) = (-1)^{\varepsilon(x)\varepsilon(a)} \left(\frac{x}{\ell_1}\right) \cdots \left(\frac{x}{\ell_k}\right)$$

Si p est différent de 2 et des ℓ_i, alors

$$\chi_a(p) = (-1)^{\varepsilon(p)\varepsilon(a)} \left(\frac{p}{\ell_1}\right) \cdots \left(\frac{p}{\ell_k}\right)$$

$$= (-1)^{\varepsilon(p)\varepsilon(a)} (-1)^{\varepsilon(p)(\varepsilon(\ell_1)+\cdots+\varepsilon(\ell_k))} \left(\frac{\ell_1}{p}\right) \cdots \left(\frac{\ell_k}{p}\right)$$

loi de réciprocité quadratique

$$= \left(\frac{a}{p}\right)$$

car $\varepsilon(a) = \varepsilon(\ell_1) + \cdots + \varepsilon(\ell_k) \bmod 2$. En effet, la fonction est donnée par

$$\varepsilon(m) \equiv \begin{cases} 0 & m \equiv 1 \bmod 4 \\ 1 & m \equiv -1 \bmod 4 \end{cases} \bmod 2.$$

On a $\chi_a \neq 1$ car si on choisit x de sorte que $\left(\frac{x}{\ell_1}\right) = -1$ et $x \equiv 1 \bmod 4\ell_2 \cdots \ell_k$, alors on a $\chi_a(x) = -1$.

Si a est de la forme (avec b comme avant)

$-b$ $\quad \chi_b \cdot (-1)^{\varepsilon(x)}$

$2b$ $\quad \chi_b \cdot (-1)^{w(x)}$

$-2b$ $\quad \chi_b (-1)^{\varepsilon(x)+w(x)}$

avec $w(m) = \dfrac{m^2-1}{8} \bmod 2 = \begin{cases} 0 & m \equiv \pm 1 \\ 1 & m \equiv \pm 5 \end{cases} \bmod 8$

et on fait le même type de vérifications. □

Un tel x existe par le lemme chinois

$$(\mathbb{Z}/N\mathbb{Z})^\times \simeq (\mathbb{Z}/\ell_1\mathbb{Z})^\times \times (\mathbb{Z}/4\ell_2 \cdots \ell_2)^\times$$

et on prend une préimage de $(y, 1)$ avec y non carré modulo ℓ_1.