1 Lemme de Zolotarev

Si X est un ensemble fini quelconque, nous notons $\mathfrak{S}_X$ le groupe des permutations de X. Nous rappelons qu'il existe un unique morphisme surjectif $\epsilon : \mathfrak{S}_X \longrightarrow \{-1, 1\}$ appelé signature.

Théorème 1. *Il existe un unique morphisme signature de $\mathfrak{S}_X$.*

Proof. On commence par montrer l'existence. On note $n = |X|$ et on considère l'application suivante

$$\Delta : \begin{cases} \mathbb{Z}^n & \longrightarrow \{-1, 1\} \\ (x_1, \ldots, x_n) & \longmapsto \prod_{1 \leq i < j \leq n}^{n} x_j - x_i. \end{cases} \tag{1}$$

On peut faire agir $\mathfrak{S}_n$ sur l'ensemble des applications $\mathbb{Z}^n \to \mathbb{Z}$ par l'action suivante

$$\sigma \cdot f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}). \tag{2}$$

On remarque ensuite que l'action d'une transposition sur Δ est d'en changer le signe.

Lemme 1. *Soit τ une transposition, alors $\tau \cdot \Delta = -\Delta$.*

On peut ensuite définir le morphisme ϵ_n comme le signe de Δ. Celui-ci est bien un morphisme car pour une transposition τ, on a

$$\epsilon_n(\sigma\tau) = \epsilon_n(\sigma)\epsilon_n(\tau) = -\epsilon_n(\sigma). \tag{3}$$

Or $\mathfrak{S}_n$ est engendré par les transpositions, donc ϵ_n est bien un morphisme de groupes. Par ailleurs, il est bien surjectif puisque $\epsilon_n(\tau) = -1$.
Il existe un isomorphisme de groupes entre $\mathfrak{S}_X$ et $\mathfrak{S}_n$. On note f un isomorphisme entre ces deux groupes. On peut donc définir $\epsilon = f \circ \epsilon_n$ qui est un morphisme signature.

Montrons que ce morphisme est unique. Soit ϵ' un autre morphisme signature non trivial, i.e. $\epsilon'(\tau) = -1$. Puisque $\mathfrak{S}_X$ est engendré par les transpositions, il existe pour $\sigma \in \mathfrak{S}_X$ une suite de transpositions $\tau_1, \ldots, \tau_k$ telles que $\sigma = \tau_1 \ldots \tau_k$. On a alors

$$\epsilon'(\sigma) = \epsilon'(\tau_1) \ldots \epsilon'(\tau_k) = (-1)^k = \epsilon(\sigma). \tag{4}$$

□

Le lemme de Zolotarev est une conséquence directe de ce théorème.

Théorème 2. *Soit p premier et $a \in \mathbb{Z}/p\mathbb{Z}^\times$, on définit $\mathfrak{m}_a$ comme la multiplication par a dans $\mathbb{Z}/p\mathbb{Z}^\times$, i.e.*

$$\mathfrak{m}_a : \begin{cases} \mathbb{Z}/p\mathbb{Z}^\times & \longrightarrow \mathbb{Z}/p\mathbb{Z}^\times \\ x & \longmapsto ax. \end{cases} \tag{5}$$

Alors, $\mathfrak{m}_a$ *est une permutation de* $\mathbb{Z}/p\mathbb{Z}^\times$ *de signature* $\epsilon(\mathfrak{m}_a) = \left(\frac{a}{p}\right)$.

Proof. $\mathfrak{m}_a$ est une permutation car $\mathbb{Z}/p\mathbb{Z}$ est un corps, la bijection inverse est alors $\mathfrak{m}_{a^{-1}}$.

On peut ensuite remarquer que le symbole de Legendre est un morphisme de groupes de $\mathbb{Z}/p\mathbb{Z}^\times$ dans $\{-1, 1\}$ non trivial et surjectif. Cela conclut la preuve : $\epsilon(\mathfrak{m}_a) = \left(\frac{a}{p}\right)$. □

Le lemme de Zolotarev permet de faire un pont entre la théorie des nombres et la théorie des permutations. Si on considère, par exemple, $\mathfrak{m}_2$ peut se représenter comme la permutation suivante

$$\begin{pmatrix} 1 & 2 & \dots & \frac{p-1}{2} & \frac{p+1}{2} & \dots & p-2 & p-1 \\ 2 & 4 & \dots & p-1 & p+1 & \dots & p-4 & p-2 \end{pmatrix}. \tag{6}$$

On remarque que l'inversion se fait à partir de $\frac{p+1}{2}$ et $\epsilon(\mathfrak{m}_2) = (-1)^{\text{nb d'inversion}}$ donc

$$\epsilon(\mathfrak{m}_2) = (-1)^{\frac{p-1}{2}+\dots+2+1}. \tag{7}$$

Il ne suffit que de calculer, $\frac{p-1}{2} + \dots + 2 + 1 = \frac{p^2-1}{8}$, d'où

$$\left(\frac{2}{p}\right) = \epsilon(\mathfrak{m}_2) = (-1)^{\frac{p^2-1}{8}}. \tag{8}$$

Une application

On peut utiliser le lemme de Zolotarev pour démontrer la loi de réciprocité quadratique.

Théorème 3. *Soit* p *et* q *deux nombres premiers impairs, alors*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{9}$$

Proof. D'abord, nous considérons l'isomorphisme $\phi : \mathbb{Z}_{pq} \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_q$. On considère les deux permutations suivantes

$$\sigma : \begin{cases} \mathbb{Z}_p \times \mathbb{Z}_q & \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_q \\ (x, y) & \longmapsto (qx + y, y) \end{cases} \tag{10}$$

$$\tau : \begin{cases} \mathbb{Z}_p \times \mathbb{Z}_q & \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_q \\ (x, y) & \longmapsto (x, py + x) \end{cases}. \tag{11}$$

On définit ensuite ρ sur $\mathbb{Z}_{pq}$ par $\rho(x + qy) = px + y$. On peut alors remarquer que

$$\phi(qx + y) = (qx + y, y) = \sigma(x, y) \text{ et } \phi(px + y) = (x, py + x) = \tau(x, y). \tag{12}$$

Ainsi, $qx + y = \phi^{-1}(\sigma(x, y))$ et en appliquant ρ, on obtient $\rho(\phi^{-1}(\sigma(x, y))) = px + y$. Finalement, en appliquant ϕ, déduit l'égalité suivante

$$\phi \circ \rho \circ \phi^{-1} \circ \sigma = \tau. \tag{13}$$

Désormais, on peut considère les signatures de ces permutations.

$$\epsilon(\phi \circ \rho \circ \phi^{-1})\epsilon(\sigma) = \epsilon(\tau). \tag{14}$$

On sait que $\epsilon(\sigma) = \left(\frac{q}{p}\right)$ et $\epsilon(\tau) = \left(\frac{p}{q}\right)$. (A faire) De plus, $\epsilon(\phi \circ \rho \circ \phi^{-1}) = (-1)^{\frac{(p-1)(q-1)}{4}}$, d'où la loi de réciprocité

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{15}$$

□

Une généralisation

Théorème 4. *Soit E un espace vectoriel sur un corps fini $\mathbb{F}_p$, alors pour tout automorphisme u de E, on a*

$$\epsilon(u) = \left(\frac{\det(u)}{p}\right). \tag{16}$$

où ϵ est le morphisme signature de $GL(E)$.

Proof. Remarquons que $SL(E)$ est le groupe dérivé de $GL(E)$. On en déduit que tout morphisme de $GL(E)$ vers un groupe abélien se factorise à travers l'abélianisé $GL(E)/SL(E)$. En particulier, si nous considérons le morphisme signature de $\mathfrak{S}_E$, nous avons l'existence de $f : \mathbb{F}_p^\times \longrightarrow \{-1, 1\}$ tel que $\epsilon = f \circ \det$ sur $GL(E)$.

De plus, f n'est pas un morphisme trivial, on peut, par exemple, prendre la multiplication par un élément générateur de $\mathbb{F}_p^\times$. Cet automorphisme est une permutation circulaire, ce qui permet simplement de déterminer que sa signature est -1. On en déduit que f n'est pas le morphisme trivial, donc $f = \left(\frac{\cdot}{p}\right)$ par unicité du symbole de Legendre. D'où

$$\epsilon(u) = \left(\frac{\det(u)}{p}\right). \tag{17}$$

□