0.1 Loi de réciprocité quadratique par les sommes de Gauss

Difficulté : Moyenne
Thèmes : Extension de corps, nombres premiers, racines de polynômes, racines de l'unité.
Leçons concernées: **120**, **104**, **121**, **123**
Références : Serre, Cours d'arithmétique

Enoncé 1. *Soient p et q deux nombres premiers impairs. Alors*

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

Considérons $\mathbb{L}$ le corps de décomposition de $X^q - 1$ sur $\mathbb{F}_p$ et soit ω une racine primitive q-ème de l'unité dans $\mathbb{L}$. Posons alors

$$y = \sum_{x\in\mathbb{F}_q} \left(\frac{x}{q}\right)\omega^x.$$

L'élément y a bien un sens, au sens où sa définition ne dépend pas du réprésentant des x choisis.

Lemme 1.

$$y^2 = (-1)^{\frac{q-1}{2}} q.$$

Démonstration. On a

$$y^2 = \sum_{t\in\mathbb{F}_q} \left(\frac{t}{q}\right) w^t \sum_{z\in\mathbb{F}_q} \left(\frac{z}{q}\right) w^z.$$

Comme le symbole de Legendre est multiplicatif,

$$y^2 = \sum_{t,z\in\mathbb{F}_q} \left(\frac{tz}{l}\right) w^{t+z}.$$

En effectuant le changement de variable $u = t + z$ (notons que u parcourt tous les éléments de $\mathbb{F}_q$), on obtient alors

$$y^2 = \sum_{u\in\mathbb{F}_q} \omega^u \left(\sum_{t\in\mathbb{F}_q^*} \left(\frac{t(u-t)}{q}\right)\right) \qquad \text{(Notons que si } t = 0\text{, tous les termes valent 0.)}$$

Donc, si $t \neq 0$,

$$\left(\frac{t(u-t)}{q}\right) = \left(\frac{-t^2}{q}\right)\left(\frac{1-ut^{-1}}{q}\right) = \left(\frac{t^2}{q}\right)\left(\frac{-1}{q}\right)\left(\frac{1-ut^{-1}}{q}\right) = 1\cdot(-1)^{\frac{q-1}{2}}\left(\frac{1-ut^{-1}}{q}\right).$$

On a alors

$$(-1)^{\frac{q-1}{2}} y^2 = \sum_{u\in\mathbb{F}_q} \mathrm{C}_u \omega^u$$

avec

$$\mathrm{C}_u = \sum_{t\in\mathbb{F}_q^*} \left(\frac{1-ut^{-1}}{q}\right).$$

Si $u = 0$, $\mathrm{C}_0 = \sum_{t\in\mathbb{F}_q^*} \left(\frac{1}{q}\right) = \sum_{t\in\mathbb{F}_q^*} 1 = l - 1$. Sinon, posons $s = 1 - ut^{-1}$.

Comme t parcourt $\mathbb{F}_q^*$, s atteint $\mathbb{F}_q \setminus \{1\}$. Or, comme dans $\mathbb{F}_q^*$, il y a autant d'éléments qui sont des carrés que d'éléments qui n'en sont pas, on a $\sum_{s\in\mathbb{F}_q} \left(\frac{s}{q}\right) = 0$. Ainsi

$$\mathrm{C}_u = \sum_{s\in\mathbb{F}_q} \left(\frac{s}{q}\right) - \left(\frac{1}{q}\right) = -\left(\frac{1}{q}\right) = -1.$$

Finalement, on obtient

$$(-1)^{\frac{q-1}{2}} y^2 = \sum_{u \in \mathbb{F}_q} \mathrm{C}_u \omega^u = q - 1 - \sum_{u \in \mathbb{F}_q^*} \omega^u = q.$$

En effet, soit $\mathrm{S} = \sum_{u \in \mathbb{F}_q} \omega^u$ et soit $y \in \mathbb{F}_q^*$. Comme $\mathbb{F}_q$ est un corps, la somme S est invariante par translation, *i.e.*, $\mathrm{S} = \sum_{x \in \mathbb{F}_q} \omega^{x+y} = \omega^y \sum_{x \in \mathbb{F}_q} \omega^x = \omega^y \, \mathrm{S}$. Comme ω et y sont non nuls, ω^y est non nul donc $\mathrm{S} = 0$. Dans notre cas, la somme est restreinte à $\mathbb{F}_q^*$. Il manque donc le terme en $w^0 = 1$. D'où $\sum_{u \in \mathbb{F}_q^*} \omega^u = -1$ □

Lemme 2.

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

Démonstration.

$$y^p = \left(\sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right) \omega^x \right)^p.$$

Comme l'équation a lieu dans $\mathbb{L}$ qui est un corps de caractéristique de p (comme extension de $\mathbb{F}_p$), il vient, en utilisant l'identité du première année $(x+y)^p = x^p + y^p$,

$$y^p = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right)^p \omega^{xp}.$$

De plus, comme p est impair

$$\left(\frac{x}{q}\right)^p = \left(\frac{x}{q}\right).$$

En effectuant alors le changement de variable $z = xp$, il vient

$$\begin{aligned} y^p = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right)^p \omega^{xp} &= \sum_{z \in \mathbb{F}_q} \left(\frac{zp^{-1}}{q}\right) \omega^z \\ &= \sum_{z \in \mathbb{F}_q^*} \left(\frac{z}{q}\right)\left(\frac{p^{-1}}{q}\right) \omega^z \\ &= \left(\frac{p^{-1}}{q}\right) \sum_{z \in \mathbb{F}_q^*} \left(\frac{z}{q}\right) \omega^z \\ &= \left(\frac{p^{-1}}{q}\right) y \\ &= \left(\frac{p}{q}\right) y. \end{aligned}$$

Comme y est non nul (invoquer le 1er lemme par exemple), en multipliant par y^{-1} de chaque côte, cela conclut. □

Enfin, pour conclure sur la loi de réciprocité quadratique

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

Remarque. Il existe une multitudes de preuves de ce résultat (autour de 80 il me semble), par exemple par le résultant ou encore les formes quadratiques. La difficulté de cette preuve se reflète au travers des calculs de somme en caractéristiques non nuls. Au delà de la preuve, il est aussi important de bien comprendre comment cet énoncé s'utilise. Pour cela, je conseille vivement la page wikipédia liée à la loi de réciprocité quadratique, où il est évoqué des exemples ainsi que de loi complémentaire.