Développement : loi de réciprocité quadratique

Référence : *Cours d'algèbre*, Demazure

Janvier 2021

1 Introduction

La loi de réciprocité quadratique, incontournable pour calculer le symbole de Legendre $\left(\frac{p}{q}\right)$, constitue un développement d'arithmétique ni particulièrement original ni d'un niveau particulièrement élevé, mais tout à fait envisageable pour des candidats qui, comme moi, ne comptent pas sur l'algèbre pour briller à l'oral. Elle s'énonce généralement avec le lemme de Gauss, qui permet de traiter le cas $p = 2$. Elle possède énormément de démonstrations possibles (dont au moins 8 par Gauss lui-même), certaines anecdotiques, certaines amusantes, et d'autres plus profondes. Celle qui suit utilise la cyclotomie et m'a été recommandée par Lionel Fourquaux au titre qu'elle se généralise pour la loi de réciprocité cubique (je ne sais pas comment).

2 Le développement

Théorème 1 (Loi de réciprocité quadratique)**.** *Soit p et q des nombres premiers impairs distincts. On a*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \times (-1)^{(q-1)(p-1)/4}.$$

On va montrer ce résultat en passant par le lemme suivant, qui permet de calculer une racine carrée de $\pm q$ dans un corps de caractéristique p.

Lemme 1. *Soit K un corps de caractéristique p, et $\alpha \in K$ vérifiant $\alpha^{q-1} + \alpha^{q-2} + \ldots + 1 = 0$. On a $\alpha^q = 1$. De plus, soit $\tau \in K$ défini par*

$$\tau := \sum_{i=0}^{q-1} \left(\frac{i}{q}\right)\alpha^i = \sum_{i=1}^{q-1} \left(\frac{i}{q}\right)\alpha^i.$$

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

Observons qu'on a une racine carrée de $\pm q$ dans K sous la forme d'une racine de l'unité. C'est dans le lemme que se fait la majeure partie des calculs.

Preuve du lemme. La propriété $\alpha^q = 1$ est claire en multipliant par $(\alpha - 1)$ l'égalité vérifiée par α. Calculons $\tau^2 \times \left(\frac{-1}{q}\right)$.

$$\left(\frac{-1}{q}\right)\tau^2 = \sum_{0 \leqslant i,j \leqslant q-1} \left(\frac{-ij}{q}\right)\alpha^{i+j} = \sum_{k=0}^{q-1} s_k \alpha^k$$

où le coefficient s_k est défini par :

$$s_k = \sum_{i=1}^{q-1} \left(\frac{-i(k-i)}{q}\right) = \sum_{i=1}^{q-1} \left(\frac{i(i-k)}{q}\right).$$

Si $k=0$, puisque $\left(\frac{i^2}{q}\right)=1$, on obtient $s_0=q-1$. Explicitions s_k pour $k\neq 0$. Pour tout $1\leqslant i\leqslant q-1$, notons i^{-1} l'inverse de i modulo q, qui existe car q est premier avec i. Remarquons d'ailleurs que $i\mapsto i^{-1}$ est une bijection de $\{1,\dots,q-1\}$ dans lui-même. On a

$$s_k=\sum_{i=1}^{q-1}\Big(\frac{i(i-k)}{q}\Big)=\sum_{i=1}^{q-1}\Big(\frac{i^2(1-ki^{-1})}{q}\Big)=\sum_{i=1}^{q-1}1\times\Big(\frac{1-ki^{-1}}{q}\Big).$$

La fonction $i\mapsto 1-ki^{-1}$ étant une bijection de $\{1,\dots,q-1\}$ dans $\{0,2,3,\dots,q-1\}$, on effectue un changement de variable dans la somme :

$$s_k=\sum_{i=1}^{q-1}\Big(\frac{1-ki^{-1}}{q}\Big)=\sum_{j\in\{0,2,3,\dots,q-1\}}\Big(\frac{j}{q}\Big)=\sum_{j=0}^{q-1}\Big(\frac{j}{q}\Big)-1.$$

Or une propriété connue de $(\mathbb{Z}/q\mathbb{Z})^*$ est de contenir autant de carrés que de non-carrés. Donc la somme des $\left(\frac{j}{q}\right)$ contient exactement $\frac{q-1}{2}$ termes égaux à -1 et $\frac{q-1}{2}$ termes égaux à 1 (et un terme nul, en $j=0$), donc est nulle ! Finalement, $s_k=-1$. On a donc

$$\Big(\frac{-1}{q}\Big)\tau^2=q-1-\sum_{k=1}^{q-1}\alpha^k=q-1-(-1)=q.$$

Calculons maintenant $\left(\frac{p}{q}\right)\tau^p$. Le corps K est de caractéristique p donc par morphisme de Frobénius,

$$\tau^p=\left(\sum_{i=1}^{q-1}\Big(\frac{i}{q}\Big)\alpha^i\right)^p=\sum_{i=1}^{q-1}\Big(\frac{i}{q}\Big)^p\alpha^{pi}.$$

Comme $\left(\frac{i}{q}\right)\in\{\pm 1\}$ et p est impair, on a $\left(\frac{i}{q}\right)^p=\left(\frac{i}{q}\right)$, donc

$$\Big(\frac{p}{q}\Big)\tau^p=\sum_{i=1}^{q-1}\Big(\frac{pi}{q}\Big)\alpha^{pi}=\sum_{j=1}^{q-1}\Big(\frac{j}{q}\Big)\alpha^j=\tau$$

car $i\mapsto pi$ est une bijection de $\{1,\dots,q\}$ dans lui-même. □

Preuve du théorème. On cherche à se placer dans le cadre du lemme. Il nous faut pour cela un corps K de caractéristique p contenant une racine α de $\Phi_{q-1}=X^{q-1}+\dots+1$. Si $\mathbb{F}_p$ en contient une, on prend $K=\mathbb{F}_p$, et sinon il suffit de prendre le corps de décomposition de Φ_p sur $\mathbb{F}_p$. Dans ce nouveau corps K, on peut poser τ comme dans le lemme. Alors, dans ce corps K,

$$\Big(\frac{q}{p}\Big)=\left(\frac{\left(\frac{-1}{q}\right)\tau^2}{p}\right)=\left(\Big(\frac{-1}{q}\Big)\tau^2\right)^{\frac{p-1}{2}}=\Big(\frac{-1}{q}\Big)^{\frac{p-1}{2}}\tau^{p-1}=(-1)^{\frac{(p-1)(q-1)}{4}}\tau^{p-1}.$$

De plus, on a par le lemme $\tau^p=\left(\frac{p}{q}\right)\tau$. Comme τ est inversible dans K (puisque $\tau^2=\pm q$ l'est), on a donc $\tau^{p-1}=\left(\frac{p}{q}\right)$. Donc finalement,

$$\Big(\frac{q}{p}\Big)=(-1)^{\frac{(p-1)(q-1)}{4}}\tau^{p-1}=(-1)^{\frac{(p-1)(q-1)}{4}}\Big(\frac{p}{q}\Big).$$

□