Loi de réciprocité quadratique par le résultant

Développement pour les leçons 123 [1], 125 [2], 152 [3].

1 Introduction

Dans la suite, p et q seront deux nombres premiers impairs distincts. On considère le symbole de Jacobi $\left(\frac{q}{p}\right)$ comme étant le résidu quadratique de q modulo p. Le but de ce développement va être de montrer la loi de réciprocité quadratique, à savoir que

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

On utilisera pour cela la théorie du résultant appliquée à des polynômes bien choisis.

2 Développement

On va tout d'abord démontrer deux lemmes préliminaires avant de se lancer dans le développement.

Lemme 1 : Soit $P(X) = \sum_{k=-n}^{n} a_k X^k$ tel que $a_k = a_{-k}$. Alors il existe un unique polynôme V de degré n et de coefficient dominant a_n tel que $P(X) = V(X + \frac{1}{X})$.

Démonstration : Supposons dans un premier temps qu'un tel polynôme V existe. Alors en écrivant $V(X + \frac{1}{X}) = P(X)$, on obtient directement que $\deg V = n$ et que le coefficient dominant de V est a_n.

Montrons que V est unique. Supposons donc qu'il existe U et V vérifiant les conditions de l'énoncé. Alors $(U-V)(X+\frac{1}{X}) = 0$ et donc le coefficient dominant de $U - V$ est nul, ce qui n'est pas possible sauf si $U - V = 0$ et donc $U = V$.

Montrons maintenant l'existence de V. On procède par récurrence sur le degré de P. Si $\deg P = 0$, on a directement que $V = a_0$ convient. Supposons donc la propriété vraie au rang $n - 1$. On a alors par hypothèse de récurrence qu'il existe un polynôme $\tilde{V}$ tel que

$$P(X) - a_n(X + \frac{1}{X})^n = \tilde{V}(X + \frac{1}{X})$$

et ainsi, le polynôme $V = \tilde{V} + a_n X^n$ convient.

Lemme 2 : On considère V_p le polynôme vérifiant $V_p(X + \frac{1}{X}) = \sum_{k=-\frac{p-1}{2}}^{\frac{p-1}{2}} X^k$. Alors $\overline{V_p}(X) = (X-2)^{\frac{p-1}{2}}$ dans $\mathbb{F}_p[X]$.

Démonstration : On considère un corps de décomposition de $\overline{V_p}$ et soit x une racine de $\overline{V_p}$. Sans perte de généralité (quitte à prendre une extension de ce corps de décomposition), on peut supposer que $Y^2 - xY + 1$ possède une racine non-nulle. Ainsi, il existe y tel que $x = y + \frac{1}{y}$. On a donc

$$\overline{V_p}(x) = 0 = \overline{V_p}(y + \frac{1}{y}) = \sum_{k=-\frac{p-1}{2}}^{\frac{p-1}{2}} y^k = y^{-\frac{p-1}{2}} \sum_{k=0}^{\frac{p-1}{2}} y^k$$

Supposons que $y \neq 1$. Alors on obtient que $y^p - 1 = 0$ et en utilisant le morphisme de Frobenius et l'intégrité du corps, on obtient que $y = 1$, donc nécessairement $y = 1$ et donc $x = 2$. Ainsi, 2 est l'unique racine de $\overline{V_p}$ qui est unitaire de degré $\frac{p-1}{2}$.

Preuve du théorème : On va montrer que $A := \mathrm{Res}(V_p, V_q) = \left(\frac{q}{p}\right)$. Pour cela, on va réduire modulo p ce résultant. On a

1. Corps finis. Applications.
2. Extensions de corps. Exemples et applications.
3. Déterminant. Exemples et applications.

$$\begin{aligned}\overline{\mathrm{Res}(V_p, V_q)} &= \mathrm{Res}(\overline{V_p}, \overline{V_q}) \\ &= \mathrm{Res}((X-2)^{\frac{p-1}{2}}, \overline{V_q}) \\ &= \overline{V_q}(2)^{\frac{p-1}{2}} \\ &= \overline{V_q}(1+\frac{1}{1})^{\frac{p-1}{2}} \\ &= q^{\frac{p-1}{2}} \\ &= \left(\frac{q}{p}\right) \ [p]\end{aligned}$$

On va maintenant, afin de pouvoir remonter, montrer que $A = \pm 1$. Pour ce faire, on raisonne par l'absurde et on suppose qu'il existe un nombre premier ℓ tel que ℓ divise A. On a donc, modulo ℓ,

$$0 = A = \mathrm{Res}(\overline{V_p}, \overline{V_q})$$

Or, il existe une extension de $\mathbb{F}_\ell$ telle que $\overline{V_p}$ et $\overline{V_q}$ possèdent une racine commune que l'on note x. Comme précédemment, on peut supposer que l'extension contient aussi une racine de $Y^2 - xY + 1$. Ainsi, il existe y tel que $x = y + \frac{1}{y}$. Si $y \neq 1$, on obtient comme précédemment que $y^p = 1$ et $y^q = 1$. Mais p et q sont premiers entre eux donc par le théorème de Bézout, il existe des entiers u et v tels que $up + vq = 1$. On obtient donc

$$1 = y^{up} y^{vq} = y^{up+vq} = y$$

et donc nécessairement $y = 1$. Ainsi, on a que $x = 2$ et donc $\overline{V_p}(2) = 0 = p$ et $\overline{V_q}(2) = 0 = q$ et donc ℓ divise p et q, ce qui est absurde. D'où $A = \pm 1$.

Ainsi, on a que

$$\begin{aligned}\left(\frac{p}{q}\right) &= \mathrm{Res}(V_p, V_q) \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \mathrm{Res}(V_q, V_p) \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right)\end{aligned}$$

et on a ainsi terminé la preuve.

3 Bibliographie

C'est le Isenmann page 361. Y'a pas mal de coquilles cependant, faut faire gaffe...