Réciprocité quadratique (par le résultant)

Théorème : Soient p, q deux nombres premiers différents de 2. On a $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$.

Démonstration :

• **Lemme 1 :** Soient $n \in \mathbb{N}$ et $P(X) = \sum_{i=-n}^{n} a_i X^i \in \mathbb{Z}[X, X^{-1}]$ avec $a_i = a_{-i}$ pour tout $i \in [\![-n, n]\!]$. Il existe un unique $Q \in \mathbb{Z}[X]$ de degré n tel que $P(X) = Q(X + X^{-1})$.

→ **Preuve du lemme 1 :**

- **Existence :** On raisonne par récurrence sur n. Le cas $n = 0$ est immédiat. Soit $n \in \mathbb{N}$. On suppose le résultat vrai au rang n. Soit $P(X) = \sum_{i=-(n+1)}^{n+1} a_i X^i \in \mathbb{Z}[X, X^{-1}]$ avec $a_i = a_{-i}$ pour tout $i \in [\![-(n+1), n+1]\!]$. On écrit alors $P(X) - a_{n+1}\left(X + \frac{1}{X}\right)^{n+1} = \sum_{i=-n}^{n} b_i X^i$ avec $b_i = b_{-i}$ pour tout $i \in [\![-n, n]\!]$. Par hypothèse de récurrence, on fixe $R \in \mathbb{Z}[X]$ de degré n tel que $P(X) - a_{n+1}\left(X + \frac{1}{X}\right)^{n+1} = R\left(X + \frac{1}{X}\right)$. On pose alors $Q(X) = R(X) + a_{n+1} X^{n+1}$, qui est de degré $n+1$ et vérifie $P(X) = Q\left(X + \frac{1}{X}\right)$.

- **Unicité :** Soit $U \in \mathbb{Z}[X]$ de degré n, que l'on écrit $U(X) = \sum_{k=0}^{n} b_k X^k \neq 0$. On a $U\left(X + \frac{1}{X}\right) = b_n X^n + b_n X^{-n} + \underbrace{\text{termes de degré} \leq n-1 \text{ en } X \text{ et } X^{-1}}_{\neq 0}$. Soient alors $R, Q \in \mathbb{Z}[X]$ de degré n tels que $R\left(X + \frac{1}{X}\right) = P(X) = Q\left(X + \frac{1}{X}\right)$. On a $(R - Q)\left(X + \frac{1}{X}\right) = 0$, donc $R = Q$.

Pour tout nombre premier $p > 2$, on note alors V_p l'unique élément de $\mathbb{Z}[X]$ de degré $\frac{p-1}{2}$ tel que $V_p\left(X + \frac{1}{X}\right) = X^{-\frac{p-1}{2}} \sum_{k=0}^{p-1} X^k$.

• **Lemme 2 :** Pour tout nombre premier $p > 2$, on a $\overline{V_p} = (X-2)^{\frac{p-1}{2}}$ dans $\mathbb{F}_p[X]$.

→ **Preuve du lemme 2 :** On commence par fixer Ω une clôture algébrique de $\mathbb{F}_p$. On va montrer que 2 est la seule racine de $\overline{V_p}$ dans Ω. Soit $x \in \Omega$ tel que $\overline{V_p}(x) = 0$. Le polynôme $Y^2 - xY + 1$ étant scindé sur Ω, on en fixe $y \in \Omega$ une racine.

On a $0 = \overline{V_p}(x) = \overline{V_p}\left(y + \frac{1}{y}\right) = y^{-\frac{p-1}{2}} \sum_{k=0}^{p-1} y^k$, donc $\sum_{k=0}^{p-1} y^k = 0$, donc $y^p = 1$,

donc $y^p - 1 = 0$, d'où $(y-1)^p = 0$ (Ω est de caractéristique p), ce qui donne $y = 1$,

donc $x = y + \frac{1}{y} = 2$. Comme de plus $\overline{V_p}$ est scindé sur Ω, on a $\overline{V_p} = (X-2)^{\frac{p-1}{2}}$ dans $\Omega[X]$,

donc dans $\mathbb{F}_p[X]$.

On peut à présent poursuivre la preuve du théorème.

On a, dans $\mathbb{F}_p$, $\overline{\mathrm{Res}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q)} = \mathrm{Res}_{\frac{p-1}{2},\frac{q-1}{2}}(\overline{V_p}, \overline{V_q})$

$= \mathrm{Res}_{\frac{p-1}{2},\frac{q-1}{2}}\left((X-2)^{\frac{p-1}{2}}, \overline{V_q}\right)$

$= \overline{V_q}(2)^{\frac{p-1}{2}}$

$= q^{\frac{p-1}{2}}$

$= \left(\frac{q}{p}\right)$ (dans $\mathbb{F}_p$).

Il reste enfin à vérifier que $\mathrm{Res}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q) \in \{\pm 1\}$, pour remonter le résultat précédent dans $\mathbb{Z}$. Ceci revient à montrer qu'aucun nombre premier ne divise $\mathrm{Res}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q)$.

On raisonne par l'absurde, et on fixe un tel nombre premier ℓ.

On fixe une clôture algébrique Ω de $\mathbb{F}_\ell$. Soit alors $x \in \Omega$ une racine commune à $\overline{V_p}$ et $\overline{V_q}$.

Soit $y \in \Omega$ tel que $x = y + \frac{1}{y}$. On a $\overline{V_p}\left(y + \frac{1}{y}\right) = 0$, donc $y^p = 1$.

De même, on a $y^q = 1$. L'ordre de y dans Ω^* vaut donc 1, car divise p et q, ce qui donne $y = 1$.

On a alors $\overline{V_p}(2) = 0$ dans $\mathbb{F}_\ell$, ce qui est absurde car $V_p(2) = p$, et p, q sont deux

$\overline{V_q}(2) = 0$ $\qquad$ $V_q(2) = q$

nombres premiers distincts.

On a donc $\mathrm{Res}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q) = \left(\frac{q}{p}\right)$ (dans $\mathbb{Z}$),

donc $\left(\frac{p}{q}\right) = \mathrm{Res}_{\frac{q-1}{2},\frac{p-1}{2}}(V_q, V_p) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \mathrm{Res}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q)$

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

ce qui achève la preuve.