# Loi de réciprocité quadratique.

2013 – 2014

Il s'agit ici de démontrer la loi de réciprocité quadratique :

**Théorème.**
*Si $p$ et $q$ sont deux nombres premiers impairs distincts, alors*

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

On commence par deux résultats préliminaires.

**Définition.** Soit $A$ un anneau commutatif. On appelle polynôme de Laurent toute fraction rationnelle de la forme $\sum_{i\in\mathbb{Z}} a_i X^i \in A(X)$ telle que les $a_i$ soient presque tous nuls. Les polynômes de Laurent forment un sous-anneau de $A(X)$.

**Proposition.**
*Tout polynôme de Laurent de la forme $P := \sum_{i=-n}^{n} a_i X^i$ avec $a_{-i} = a_i$ pour tout $i$ et $a_n \neq 0$ s'écrit de manière unique sous la forme $Q(X + \frac{1}{X})$ avec $Q \in A[X]$ de degré $n$.*

*Démonstration.* Si $Q = b_0 + b_1 X + \cdots + b_n X^n$ avec $b_n \neq 0$, alors $Q(1 + \frac{1}{X}) = b_n X^{-n} + \cdots + b_n X^n$ où les monômes dans les $\cdots$ ont un exposant compris entre $-(n-1)$ et $n-1$. On en déduit que si $Q$ est non nul, alors $Q(X + \frac{1}{X})$ aussi, ce qui montre l'unicité de $Q$.

Montrons l'existence de $Q$ par récurrence sur $n$.
Si $P = a_0$, $Q := a_0$ convient.
Supposons le résultat connu pour des polynômes de Laurent faisant intervenir des exposants compris entre $-(n-1)$ et $n-1$. Soit $P := \sum_{i=-n}^{n} a_i X^i$ avec $a_{-i} = a_i$ et $a_n \neq 0$. Le polynôme de Laurent $P - a_n(X + \frac{1}{X})^n$ a des coefficients symétriques donc, par hypothèse de récurrence, il existe $R \in A[X]$ de degré inférieur à $n-1$ tel que $P - a_n(X + \frac{1}{X})^n = R(X + \frac{1}{X})$. Le polynôme $Q := R + a_n X^n$ vérifie $P = Q(X + \frac{1}{X})$ et est de degré $n$. □

**Proposition.**
*Pour $p$ un nombre premier impair, on note $V_p \in \mathbb{Z}[X]$ le polynôme de degré $\frac{p-1}{2}$*

*tel que*

$$V_p\left(X+\frac{1}{X}\right)=\sum_{i=-\frac{p-1}{2}}^{\frac{p-1}{2}}X^i.$$

*Son existence et son unicité sont garanties par la proposition précédente.*

*Si $q$ est un autre nombre premier impair distinct de $p$, alors*

$$\left(\frac{q}{p}\right)=Res(V_p,V_q).$$

*Démonstration.* Montrons que ces deux quantités sont congrues modulo $p$. Pour cela, établissons d'abord que $V_p$ est congru à $(X-2)^{\frac{p-1}{2}}$ modulo $p$.

$V_p$ étant unitaire, un représentant $\overline{V_p}$ de la classe de $V_p$ dans $\mathbb{F}_p[X]$ est un polynôme unitaire de degré $\frac{p-1}{2}$. Pour montrer que $\overline{V_p}=(X-2)^{\frac{p-1}{2}}$, il suffit de montrer que si $K$ est un corps de décomposition de $\overline{V_p}$ sur $\mathbb{F}_p$, alors 2 est l'unique racine de $\overline{V_p}$ dans $K$.
Soit $x\in K$ tel que $\overline{V_p}(x)=0$. Dans une certaine extension $L$ de $K$, il existe $\zeta$ tel que $x=\zeta+\frac{1}{\zeta}$ ($\zeta$ vérifie $\zeta^2-x\zeta+1=0$). On a alors

$$\overline{V_p}(x)=\overline{V_p}\left(\zeta+\frac{1}{\zeta}\right)=\sum_{i=-\frac{p-1}{2}}^{\frac{p-1}{2}}\zeta^i=0.$$

D'où

$$\sum_{i=0}^{p-1}\zeta^i=0\quad\text{et}\quad\sum_{i=1}^{p}\zeta^i=0,$$

d'où $\zeta^p-1=0$. On en déduit $(\zeta-1)^p=0$ et donc $\zeta=1$ et $x=2$.

La réduction modulo $p$ de $\mathrm{Res}(V_p,V_q)$ donne

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

dans $\mathbb{F}_p$.

Il reste à montrer que $\mathrm{Res}(V_p,V_q)$ est égal à $\pm1$. Pour cela, il suffit de montrer que pour tout nombre premier $l$, $l$ ne divise pas $\mathrm{Res}(V_p,V_q)$, c'est-à-dire que $V_p$ et $V_q$ n'ont pas de racine commune dans une extension finie $K$ de $\mathbb{F}_l$.
Soit $x\in K$ une racine commune de $V_p$ et $V_q$ dans $K$. Comme précédemment, on peut écrire $x=\zeta+\frac{1}{\zeta}$ avec $\zeta$ appartenant à une extension $L$ de $K$. $V_p(x)=0$ donc $\zeta^p=1$ et $V_q(x)=0$ donc $\zeta^q=1$. Or $p$ et $q$ sont premiers entre eux donc

$\zeta = 1$. Quitte à échanger les rôles de $p$ et $q$, on peut supposer que $p \neq l$, on a alors

$$V_p(x) = \sum_{i=-\frac{p-1}{2}}^{\frac{p-1}{2}} \zeta^i = p \neq 0$$

dans $\mathbb{F}_l$. □

Par la formule $\mathrm{Res}(V_q, V_p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\mathrm{Res}(V_p, V_q)$, on en déduit la loi de réciprocité quadratique.