# Loi de réciprocité de la puissance $d$-ième.

Réf : Rosen : Number theory in Function Fields.

$d \mid q-1$, $A = \mathbb{F}_q[T]$

**Thm :** Soient $a, P, Q \in A$, avec $P$ et $Q$ irréductibles unitaires de degrés $\delta$ et $\gamma$.
Alors :
(i) $\left(\frac{a}{P}\right)_d = 1$ ssi $x^d \equiv a \pmod P$ admet une solution

(ii) $\left(\frac{Q}{P}\right)_d = (-1)^{\frac{q-1}{d}\delta\gamma} \left(\frac{P}{Q}\right)_d$

**Lem :** (i) . Si $a \equiv b^d \pmod P$ alors $a^{\frac{|P|-1}{d}} = b^{|P|-1} = 1 \pmod P$
Donc les racines $d$-ièmes sont racines de $X^{\frac{|P|-1}{d}} - 1$.
Soit $\varphi : \left(\frac{A}{PA}\right)^* \to \left(\frac{A}{PA}\right)^*$
$x \mapsto x^d$
$|\ker\varphi| = d$, en effet $X^d - 1 \mid X^{q-1} - 1$ $(d \mid q-1)$ qui est scindé à racines simples : donc $X^d - 1$ a exactement $d$ solutions.
Ainsi il y a $\frac{|P|-1}{d}$ puissances $d$-ième qui sont les racines de $X^{\frac{|P|-1}{d}} - 1$ exactement □

(ii) Posons $\left(\frac{a}{P}\right) = \left(\frac{a}{P}\right)_{q-1}$. Alors $\left(\frac{a}{P}\right)_d = a^{\frac{|P|-1}{d}} = \left(a^{\frac{|P|-1}{q-1}}\right)^{\frac{q-1}{d}} = \left(\frac{a}{P}\right)^{\frac{q-1}{d}}$

Il suffit donc de prouver que $\left(\frac{P}{Q}\right) = (-1)^{\delta\gamma}\left(\frac{Q}{P}\right)$ (on élève ensuite à la puissance $\frac{q-1}{d}$)

Soient $\alpha$ une racine de $P$, $\beta$ une racine de $Q$ et $\mathbb{F}'$ un corps fini contenant $\mathbb{F}_q$, $\alpha$ et $\beta$.

$P(T) = (T-\alpha)\cdots(T-\alpha^{q^{\delta-1}})$, $Q(T) = (T-\beta)(T-\beta^q)\cdots(T-\beta^{q^{\gamma-1}})$ (*)

Posons $A' = \mathbb{F}'[T]$.

Rq : . Si $g \in A'$, $g(T) = g(\alpha) \pmod{(T-\alpha)}$
. Si $g \in A$ $g(T)^q = g(T^q)$ (les coefficients de $g$ sont dans $\mathbb{F}_q$)

Donc : $\left(\frac{Q}{P}\right) = Q^{\frac{|P|-1}{q-1}} = Q^{\frac{q^{\delta}-1}{q-1}} = Q(T)^{1+q+\cdots+q^{\delta-1}} \equiv Q(T)Q(T^q)\cdots Q(T^{q^{\delta-1}}) \equiv Q(\alpha)\cdots Q(\alpha^{q^{\delta-1}}) \pmod{(T-\alpha)}$

Par symétrie la congruence reste vraie modulo $T-\alpha^{q^i}$ donc modulo $P$.

Avec (*) : $\left(\frac{Q}{P}\right) \equiv \prod_{i=0}^{\delta-1}\prod_{j=0}^{\gamma-1}(\alpha^{q^i} - \beta^{q^j}) \pmod P$. Les deux membres sont dans $\mathbb{F}'$ donc sont égaux. D'où : $\left(\frac{Q}{P}\right) = \prod_{i=0}^{\delta-1}\prod_{j=0}^{\gamma-1}(\alpha^{q^i} - \beta^{q^j}) = (-1)^{\delta\gamma}\prod_{i=0}^{\delta-1}\prod_{j=0}^{\gamma-1}(\beta^{q^j} - \alpha^{q^i}) = (-1)^{\delta\gamma}\left(\frac{P}{Q}\right)$.