XI

Loi(s) de réciprocité quadratique :

Soit p un nombre premier impair. Soit z une racine primitive $p-$ième de l'unité.

Soit $\delta := \prod_{1\leq i<j\leq p-1}(z^i - z^j)$. On a $\delta \in \mathbb{Q}(z)$ et $\delta^2 = \Delta_{\Phi_p(X)} = (-1)^{p-2}(p^{(p-3)/2})^2 p$.

Donc si t est une racine carrée de $(-1)^{(p-1)/2}p$, t est de degré 2 sur $\mathbb{Q}$ et $t \in \mathbb{Q}(z)$.

Or $\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ contient un unique sous-groupe d'indice 2 : c'est le sous-groupe des carrés de $\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q})$.

Donc $\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q}(t))$ est formé des carrés de $\mathrm{Gal}(\mathbb{Q}(z)/\mathbb{Q})$.

Or, $s_q(t^2) = t^2 \Rightarrow s_q(t) = \pm t$.

On en déduit que si $q \neq p$ est un nombre premier impair, alors $s_q(t) = (q/p)t \bmod p$ dans $\mathbb{Z}[z]$.

Or, si $a_0 + ... + a_{p-2}z^{p-2} \in \mathbb{Z}[z]$, $a_i \in \mathbb{Z}$, on a :

$$\begin{aligned} s_q(a_0 + ... + a_{p-2}z^{p-2}) &= a_0 + ... + a_{p-2}z^{q(p-2)} \\ &= a_0^q + ... + a_{p-2}^q z^{q(p-2)} \bmod q \\ &= (a_0 + ... + a_{p-2}z^{p-2})^q \bmod q \end{aligned}$$

dans $\mathbb{Z}[z]$. On a donc :

$$s_q(t) = (q/p)t = t^q \bmod q$$

dans $\mathbb{Z}[z]$. Or, t est inversible $\bmod q$ (en effet dans $\mathbb{Z}[z]$, l'idéal engendré par t et q contient p et q (car $t^2 = \pm p$) et on a une relation de Bézout : $ap + bq = 1$ pour certains $a, b \in \mathbb{Z}$).

Donc :

$$t^{q-1} = (q/p) \bmod q \ .$$

Or : $t^{q-1} = (-1)^{(p-1)/2(q-1)/2}p^{(q-1)/2} = (-1)^{(p-1)/2(q-1)/2}(p/q) \bmod q$ (*remarque : comme $\mathbb{Z}$ est intégralement clos, pour deux entiers x, y, $x = y \bmod q\mathbb{Z}[z] \Leftrightarrow x = y \bmod q\mathbb{Z}$.*) On a donc :

$$(p/q)(q/p) = (-1)^{(p-1)/2(q-1)/2} \ .$$

Loi complémentaire :

Soit z une racine primitive $8-$i-ème de l'unité. On a $(y+y^{-1})^2 = y^2 + y^{-2} + 2 = 2$ car $y^2 = y^{-6} = y^{-4}y^{-2} = -y^{-2}$.

On a donc comme précédemment, pour tout p premier impair :

$$\begin{aligned} (y + y^{-1})2^{(p-1)/2} &= (y + y^{-1})^p \\ &= y^p + y^{-p} \bmod p \end{aligned}$$

dans $\mathbb{Z}[z]$. Or, $(y + y^{-1})$ est inversible $\bmod p$. Donc :

$$2^{(p-1)/2} = \frac{y^p + y^{-p}}{y + y^{-1}} \bmod p \ .$$

Comme y est une racine primitive $8-$ième de l'unité, $y^{\pm p}$ ne dépend que de $p \bmod 8$. On a :

$$y^p + y^{-p} = \begin{cases} y + y^{-1} & \text{si } p = \pm 1 \bmod 8, \\ -y - y^{-1} & \text{si } p = \pm 3 \bmod 8. \end{cases}$$

On en déduit : $(2/p) = (-1)^{(p^2-1)/8}$.

Anneau des entiers d'un corps de nombres.

Soit $K/\mathbb{Q}$ une extension finie. Soient $s_1, ..., s_n$ les plongements de K dans $\mathbb{C}$. Notons A l'anneau des entiers de K.

Si $x \in K$, alors $dx \in A$ pour un certain $d \neq 0$.

En effet, si $a_r x^r + ... + a_0 = 0$ pour certains $a_i \in \mathbb{Z}$ avec $a_r \neq 0$, alors on a une relation de dépendance unitaire à coefficients entiers :

$$(a_r x)^r + ... + a_0 a_r^{r-1} = 0 \ .$$

Soit $x_1, ..., x_n$ une $\mathbb{Q}-$ base de K. Quitte à multiplier chaque x_i par un entier $\neq 0$, on peut supposer que les x_i sont dans A. Soit $y_1, ..., y_n$ la base duale de $x_1, ..., x_n$ relativement à la forme bilinéaire :

$$(x, y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(xy)$$

(cette forme bilinéaire est non dégénérée car $\det(\mathrm{Tr}(x_i x_j)) = \det(s_i(x_j))^2 \neq 0$). Par définition : $\mathrm{Tr}(x_i y_j) = \delta_{i,j}$. Par conséquent, si $a \in A$, $a = t_1 y_1 + ... + t_n y_n$ avec $t_i = \mathrm{Tr}(a x_i) \in \mathbb{Z}$.

Donc : $A \subseteq \mathbb{Z}x_1 \oplus ... \oplus \mathbb{Z}x_n$. Le $\mathbb{Z}-$module A est donc libre de rang $\leq n$. Le rang est exactement n car une $\mathbb{Z}-$base de A est une $\mathbb{Q}-$base de K.

Par exemple si d est un entier sans facteur carré, $K = \mathbb{Q}(\sqrt{d})$ est une extension quadratique dont l'anneau des entiers est libre de base :

$$1, \sqrt{d}$$

si $d \neq 1 \bmod 4$ et de base :

$$1, \frac{1+\sqrt{d}}{2}$$

si $d = 1 \bmod 4$.