leçons :
123 : Corps finis
125 : Extensions de corps
143 : Résultant
144 : Racines d'un polynôme

Loi de réciprocité quadratique par le résultant

(35)

Références :
APERY "Elimination. Le cas d'une variable"

Thm : Soient p et q deux nombres premiers impairs distincts
Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

preuve :

① **lemme 1 :** Soit A un anneau intègre. Soit $P = \sum_{k=-n}^{n} a_k X^k \in A(X)$ tel que pour tout $k \in [\![1, n]\!]$ $a_k = a_{-k}$.
Alors il existe un unique $V \in A[X]$ tel que $P(X) = V\left(X + \frac{1}{X}\right)$
De plus, si $a_n \neq 0$, alors V est de degré n et de coefficient dominant a_n

preuve du lemme 1 : Soit $V = \sum_{k=0}^{n} b_k X^k \in A[X]$ tel que $b_n \neq 0$.
Alors $V\left(X + \frac{1}{X}\right) = b_n X^n + b_n X^{-n} + Q_1(X) + Q_2(X^{-1})$ où $Q_1, Q_2 \in A_{\leq n-1}[X]$

On obtient l'équivalence : $V = 0 \iff V\left(X + \frac{1}{X}\right) = 0$ (dans $A(X)$)
Si $P(X) = V_1\left(X + \frac{1}{X}\right) = V_2\left(X + \frac{1}{X}\right)$, alors $(V_1 - V_2)\left(X + \frac{1}{X}\right) = 0$ donc $V_1 = V_2$.
D'où l'unicité.

Existence : • Si $P = a_0$, alors $V = a_0$ convient.
• Sinon, $P = \sum_{k=-n}^{n} a_k X^k$ avec $n \geq 1$, $a_n \neq 0$

$P - a_n\left(X + \frac{1}{X}\right)^n$ est de la forme $\sum_{k=-(n-1)}^{(n-1)} b_k X^k$ avec $b_k = b_{-k}$ $\forall k$

et on conclut par récurrence sur n. □

Déf : On notera V_p l'unique élément de $\mathbb{Z}[X]$ tel que $V_p\left(X + \frac{1}{X}\right) = \sum_{k=-\frac{p-1}{2}}^{\frac{p-1}{2}} X^k$

② **lemme 2 :** $V_p = (X-2)^{\frac{p-1}{2}}$ dans $\mathbb{F}_p[X]$

preuve du lemme 2 : $\overline{V_p}$ est unitaire de degré $\frac{p-1}{2}$ par le lemme 1.
Soit $\mathbb{K}$ un corps de décomposition de $\overline{V_p}$ sur $\mathbb{F}_p$. Il suffit de montrer que 2 est l'unique racine de $\overline{V_p}$ dans $\mathbb{K}$. Soit $x \in \mathbb{K}$ tel que $\overline{V_p}(x) = 0$.
Quitte à se placer dans une extension $\mathbb{L}$ de $\mathbb{K}$ (corps de rupture de $Y^2 - xY + 1$ sur $\mathbb{K}$) on peut supposer qu'il existe $y \in \mathbb{K}^*$ tel que $x = y + \frac{1}{y}$.
On a alors $\overline{V_p}\left(y + \frac{1}{y}\right) = 0$.

On $\overline{V_p}\left(y+\frac{1}{y}\right) = \sum_{k=-\frac{p-1}{2}}^{\frac{p-1}{2}} y^k = \begin{cases} p & \text{si } y=1 \\ y^{-\frac{p-1}{2}} \dfrac{1-y^p}{1-y} & \text{sinon} \end{cases}$

Si $y \neq 1$, on a $y^p - 1 = 0$ dans $\mathbb{K}$ donc $(y-1)^p = 0$ par morphisme de Frobenius donc $y = 1$. Absurde. D'où $x = 1+1 = 2$.

③ MQ $\text{Rés}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q) = \left(\frac{q}{p}\right)$

Modulo p, on a $\overline{\text{Rés}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q)} = \text{Rés}_{\frac{p-1}{2},\frac{q-1}{2}}(\overline{V_p}, \overline{V_q})$ (car le résultant passe aux morphismes)

$= \text{Rés}_{\frac{p-1}{2},\frac{q-1}{2}}((X-2)^{\frac{p-1}{2}}, \overline{V_q})$ (par ②)

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

$= \overline{V_q}\left(1+\frac{1}{x}\right)^{\frac{p-1}{2}}$

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

$= \left(\frac{q}{p}\right)$ [p]

Pour avoir l'égalité voulue, il suffit de montrer que $\text{Rés}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q) \in \{-1, 1\}$. Il suffit donc de montrer que $\text{Rés}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q)$ n'est divisible par aucun nombre premier ℓ ie $\forall \ell$ premier $\text{Rés}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q) \neq 0$ dans $\mathbb{F}_\ell$

Fixons ℓ premier. $\text{Rés}_{\frac{p-1}{2},\frac{q-1}{2}}(V_p, V_q) \neq 0$ dans $\mathbb{F}_\ell$ ssi pour toute extension $\mathbb{K}$ de $\mathbb{F}_\ell$, V_p et V_q n'ont pas de racines communes dans $\mathbb{K}$. Raisonnons par l'absurde, si il existe $x \in \mathbb{K}$ tel que $V_p(x) = V_q(x) = 0$. Quitte à prendre une extension $\mathbb{L}$ de $\mathbb{K}$, il existe $y \in \mathbb{K}^*$ tel que $x = y + \frac{1}{y}$. En faisant le même raisonnement qu'en ②, si $y \neq 1$ alors $y^p = y^q = 1$. p et q sont premiers entre eux donc par Bezout $y = 1$. Absurde

Donc $y = 1$ et $x = 2$ et $\begin{cases} V_p(x) = p \\ V_q(x) = q \end{cases}$ $\begin{cases} p \equiv 0 \ [\ell] \\ q \equiv 0 \ [\ell] \end{cases}$ c'est absurde

④ Conclusion

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

Compléments sur les carrés dans $\mathbb{F}_p$ et la loi de réciprocité quadratique

Thm : p un nombre premier impair

Alors (i) $\mathbb{F}_p$ contient $\frac{p+1}{2}$ carrés, $\mathbb{F}_p^*$ contient $\frac{p-1}{2}$ carrés.

(ii) les carrés de $\mathbb{F}_p^*$ sont les zéros de $X^{\frac{p-1}{2}} - 1$

(iii) $\forall a \in \mathbb{F}_p^* \quad a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \end{cases}$

preuve : (i) On pose $\varphi : \begin{cases} \mathbb{F}_p^* \to \mathbb{F}_p^* \\ x \mapsto x^2 \end{cases}$ morphisme de groupes

$$\ker \varphi = \{ x \in \mathbb{F}_p^* \mid x^2 = 1 \} = \{ x \in \mathbb{F}_p^* \mid (x-1)(x+1) = 0 \} = \{-1, 1\}$$

D'où $\# \operatorname{Im} \varphi = \frac{1}{2} \# \mathbb{F}_p^* = \frac{p-1}{2}$

Les carrés de $\mathbb{F}_p$ sont donc au nombre de $\frac{p-1}{2} + 1 = \frac{p+1}{2}$

(puisqu'il faut aussi compter 0)

(ii) Soit $x \in \mathbb{F}_p^*$ un carré. Il existe $y \in \mathbb{F}_p^*$ tq $y^2 = x$

D'où $x^{\frac{p-1}{2}} = y^{p-1} = 1$ par le petit théorème de Fermat (ou par Lagrange ~)

Donc x racine de $X^{\frac{p-1}{2}} - 1$.

On vient de trouver $\frac{p-1}{2}$ racines de $X^{\frac{p-1}{2}} - 1$ donc on les a toutes.

(iii) Soit $a \in \mathbb{F}_p^*$. On a $\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} = 1$ donc $a^{\frac{p-1}{2}} = \pm 1$.

D'après (ii) $a^{\frac{p-1}{2}} = 1 \iff a$ est un carré dans $\mathbb{F}_p^*$ □

Corollaire : p un nombre premier impair

Alors (-1) est un carré dans $\mathbb{F}_p^*$ (ie modulo p) ssi $p \equiv 1 \ [4]$

preuve : dans d'après (iii) □

Définition : p nombre premier impair, $a \in \mathbb{F}_p$.

On pose $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \\ 0 & \text{si } a = 0 \end{cases}$

Prop : $\begin{cases} \mathbb{F}_p \longrightarrow \{-1, 0, 1\} \\ a \longmapsto \left(\frac{a}{p}\right) \end{cases}$ est multiplicative.

Prop : p premier impair, $a \in \mathbb{F}_p^*$

Alors $\#\{x \in \mathbb{F}_p \mid ax^2 = 1\} = 1 + \left(\frac{a}{p}\right)$

Prop : p premier impair

Alors 2 est un carré dans $\mathbb{F}_p^*$ ssi $p \equiv \pm 1 \ [8]$

preuve :

$\# \mathbb{F}_{p^2}^* = p^2 - 1 = (p-1)(p+1)$ donc $8 \mid \# \mathbb{F}_{p^2}^*$

$\mathbb{F}_{p^2}^*$ est cyclique donc il existe $y \in \mathbb{F}_{p^2}^*$ d'ordre 8

$\begin{cases} y^8 = 1 \\ y^4 \neq 1 \end{cases} \Rightarrow y^4 = -1 \Rightarrow y^2 = -\frac{1}{y^2}$ et $y \neq -\frac{1}{y}$

. On pose $x = y + \frac{1}{y}$, on a $x^2 = y^2 + 2 + \frac{1}{y^2} = 2$

$x \neq 0$ donc $x \neq -x$ et x et $-x$ sont les seules racines carrées de 2 dans $\mathbb{F}_{p^2}$

Ainsi 2 carré dans $\mathbb{F}_p^* \iff x \in \mathbb{F}_p \iff x^p = x$

Par le morphisme de Frobenius, $x^p = y^p + \frac{1}{y^p}$

. Si $p \equiv \pm 1 \ [8]$ $y^p = y^{\pm 1}$ donc $x^p = x$

. Si $p \equiv \pm 3 \ [8]$ $y^p = -y^{\pm 1}$ donc $x^p = -x \neq x$ □