

COURS 3 (24 janvier 2024)

③ La loi de réciprocité quadratique

Soit p un nombre premier. Notons

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

(c'est un corps à p éléments). Dans cette
 $\uparrow$ car p est premier

section on admettra le résultat qu'il existe un corps $\Omega \supset \mathbb{F}_p$ tel que tout polynôme $P \in \mathbb{F}_p[T]$ de degré ≥ 1 a une racine dans Ω . Un tel Ω s'appelle une clôture algébrique de $\mathbb{F}_p$. et tous les éléments de Ω sont racine d'un polynôme $P \in \mathbb{F}_p[T]$.

Question générale: Étant donné $x \in \mathbb{F}_p$,

comment décider si x est un carré, c'est-à-dire s'il existe $y \in \mathbb{F}_p$ tel que $y^2 = x$?

* Si $p=2$, tous les éléments de $\mathbb{F}_2$ sont des carrés. En effet, $0=0^2$ et $1=1^2$.

Proposition. Soit $p \geq 3$ un nombre premier.

Les carrés forment un sous-groupe d'indice 2 d'éléments $\uparrow$ non nuls de $\mathbb{F}_p$

de $\mathbb{F}_p^x$, qui est le noyau de l'homomorphisme

$$\begin{array}{ccc} \mathbb{F}_p^x & \longrightarrow & \{\pm 1\} \\ x & \longmapsto & x^{\frac{p-1}{2}} \end{array} \quad \leftarrow \begin{array}{l} \text{puisque} \\ x^{p-1} = 1 \\ \text{par le petit} \\ \text{théorème de} \\ \text{Fermat} \end{array}$$

Preuve: Pour $x \in \mathbb{F}_p^x$, soit $y \in \Omega$ un élément de la clôture algébrique tel que $y^2 = x$. On a alors:

$$y^{p-1} = x^{\frac{p-1}{2}} \in \{\pm 1\}$$

on en déduit:

$$x \text{ est un carré} \iff y \in \mathbb{F}_p^x$$

$\boxed{\Leftarrow}$ évident

$$\boxed{\Rightarrow} \text{ si } x = z^2, \text{ alors } y^{p-1} = z^{p-1} = 1,$$

donc $y \in \mathbb{F}_p^x$ car l'équation $y^{p-1} = 1$

a $\leq p-1$ solutions dans le corps Ω et elle en a déjà $p-1$ dans $\mathbb{F}_p^x$.

Par conséquent:

$$(\mathbb{F}_p^x)^2 = \ker \left(x \mapsto x^{\frac{p-1}{2}} \right)$$

Par ailleurs, $\mathbb{F}_p^x$ est cyclique d'ordre $p-1$.

(2)

Si x est un générateur, alors $x^{\frac{p-1}{2}} \neq 1$.

L'application $x \mapsto x^{\frac{p-1}{2}}$ est donc surjective,

d'où : $\mathbb{F}_p^x / (\mathbb{F}_p^x)^2 \cong \{\pm 1\}$ □

Définition : Soit $p \geq 3$ un nombre premier. Le symbole de Legendre de $x \in \mathbb{F}_p^x$ est l'entier

$$\left(\frac{x}{p}\right) = x^{\frac{p-1}{2}} \in \{\pm 1\}$$

$$= \begin{cases} 1 & \text{si } x \text{ est un carré} \\ -1 & \text{sinon} \end{cases}$$

On étend le symbole de Legendre à $\mathbb{F}_p$ en posant $\left(\frac{0}{p}\right) = 0$. Si $x \in \mathbb{Z}$, on définit

$$\left(\frac{x}{p}\right) = \left(\frac{x \bmod p}{p}\right) = \begin{cases} 0 & \text{si } p \mid x \\ 1 & \text{si } x \text{ est un carré mod } p \\ -1 & \text{si } x \text{ n'est pas un carré mod } p \end{cases}$$

le symbole de Legendre est multiplicatif :

$$\left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right) \left(\frac{y}{p}\right)$$

On a $\left(\frac{1}{p}\right) = 1$ et $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$,

c'est-à-dire

$$-1 \text{ est un carré mod } p \iff p \equiv 1 \pmod{4}$$

Proposition:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

c'est-à-dire 2 est un carré mod $p \iff$
 $p \equiv 1$ ou $p \equiv -1 \pmod{8}$

Preuve: Soit $\alpha \in \Omega$ une racine de $T^4 + 1$.
L'élément $y = \alpha + \frac{1}{\alpha}$ satisfait alors à

$$y^2 = \left(\alpha + \frac{1}{\alpha}\right)^2 = \alpha^2 + 2 + \frac{1}{\alpha^2} = 2$$

puisque $\alpha^4 = -1$ implique $\alpha^2 = -\frac{1}{\alpha^2}$.

$$\therefore 2 \text{ est un carré mod } p \iff y \in \mathbb{F}_p$$

Pour cela on calcule

$$y^p = \left(\alpha + \frac{1}{\alpha}\right)^p = \alpha^p + \frac{1}{\alpha^p}$$

Si $p \equiv 1$ ou $p \equiv -1 \pmod{8}$, alors $\alpha^p = \alpha$
car $\alpha^8 = 1$. Donc $y^p = y$, d'où $y \in \mathbb{F}_p$.

Si $p \equiv 5$ ou $p \equiv -5 \pmod{8}$, alors $\alpha^p = -\alpha$
car $\alpha = -1$. Donc $y^p = -y$, d'où $y \notin \mathbb{F}_p$ $\square$

(3)

Théorème (loi de réciprocité quadratique)

Soient l et p deux premiers impairs distincts.
Alors on a l'égalité

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

Très utile pour calculer !

$$\begin{aligned} \left(\frac{29}{43}\right) &= \left(\frac{43}{29}\right) (-1)^{21} = \left(\frac{14}{29}\right) = \left(\frac{2}{29}\right) \left(\frac{7}{29}\right) \\ &= (-1) \left(\frac{7}{29}\right) = - \left(\frac{29}{7}\right) (-1)^{3 \cdot 14} = - \left(\frac{1}{7}\right) \\ &= -1 \end{aligned}$$

$\nearrow$
 $29 \equiv 5 \pmod{8}$

$\Rightarrow 29$ n'est pas un carré mod 43

Démonstration de la loi de réciprocité

Notation: $\varepsilon(n) = \frac{n-1}{2}$ pour n impair

Soit $\alpha \in \Omega$ une racine primitive l -ième de l'unité, c'est-à-dire une racine de

$$T^{l-1} + T^{l-2} + \dots + T + 1.$$

Considérons la somme de Gauss

$$y = \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell} \right) \alpha^x$$

↖ lin défini
puisque $\alpha^\ell = 1$

lemme: (1) $y^2 = (-1)^{\frac{\ell-1}{2}} \ell$

(2) $y^{p-1} = \left(\frac{p}{\ell} \right)$

Voyons comment conclure en supposant le lemme déjà démontré.

$$\left(\frac{(-1)^{\frac{\ell-1}{2}} \ell}{p} \right) = y^{p-1} = \left(\frac{p}{\ell} \right)$$

Mais, d'autre part,

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

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

□

Preuve du lemme (1)

$$y^2 = \sum_{x, z \in \mathbb{F}_\ell} \left(\frac{xz}{\ell} \right) \alpha^{x+z} = \sum_{u \in \mathbb{F}_\ell} S(u) \alpha^u$$

(4)

$$\text{avec } S(u) = \sum_{X+Z=u} \left(\frac{x^2}{l} \right) = \sum_{x \in \mathbb{F}_l} \left(\frac{x(u-x)}{l} \right)$$

Si $u=0$,

$$S(0) = \sum_{x \in \mathbb{F}_l} \left(\frac{-x^2}{l} \right) = \underbrace{\left(\frac{-1}{l} \right)}_{(-1)^{\varepsilon(l)}} (l-1)$$

Si $u \neq 0$,

$$\begin{aligned} S(u) &= \sum_{x \in \mathbb{F}_l^*} \left(\frac{x(u-x)}{l} \right) \\ &= \underbrace{\left(\frac{-x^2(1-ux^{-1})}{l} \right)}_{(-1)^{\varepsilon(l)}} \sum_{x \in \mathbb{F}_l^*} \left(\frac{1-ux^{-1}}{l} \right) \end{aligned}$$

et $1-ux^{-1}$ parcourt tous les éléments de $\mathbb{F}_l$ sauf 1. Donc

$$\begin{aligned} \sum_{x \in \mathbb{F}_l^*} \left(\frac{1-ux^{-1}}{l} \right) &= \sum_{x \in \mathbb{F}_l} \left(\frac{x}{l} \right) - 1 \\ &= -1 \end{aligned}$$

↑
autant de carrés qe de
non carrés dans $\mathbb{F}_l^*$!

Mettre tout ensemble:

$$\begin{aligned}
 y^2 &= \sum_{u \in \mathbb{F}_\ell} S(u) \alpha^u = \underbrace{\left(-\frac{1}{\ell}\right)}_{u=0} \left[(1-1) - \underbrace{\sum_{u=1}^{p-1} \alpha^u}_{-1} \right] \\
 &= \left(-\frac{1}{\ell}\right) \ell \\
 &= (-1)^{\varepsilon(\ell)} \ell
 \end{aligned}$$

Preuve du lemme (2)

$$\begin{aligned}
 y^p &= \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right)^p \alpha^{px} = \sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right) \alpha^{px} \\
 &\quad \begin{array}{c} \uparrow \\ p \text{ impair} \\ \text{et } \left(\frac{x}{\ell}\right) \in \{-1, 0, 1\} \end{array} \\
 &= \sum_{t \in \mathbb{F}_\ell} \left(\frac{t p^{-1}}{\ell}\right) \alpha^t = \left(\frac{p^{-1}}{\ell}\right) y \\
 &= \left(\frac{p}{\ell}\right) y, \\
 &\quad \nearrow 1 = \left(\frac{1}{\ell}\right) = \left(\frac{p^{-1}}{\ell}\right) \left(\frac{p}{\ell}\right)
 \end{aligned}$$

donc $y^{p-1} = \left(\frac{p}{\ell}\right)$

□