Loi de réciprocité quadratique

Chen Thomas
t.chen.thomas1[at]gmail.com

16 mai 2024

Attention

1. Ce document contient certainement des coquilles. N'hésitez pas à me le signaler. De même si vous avez une question.
2. Pour les recasages, ce sont les miens mais ce développement se case peut-être ailleurs et je n'y ai pas réfléchi.
3. Il se peut que ce développement dure plus de 15 minutes. J'ai essayé de le découper pour faire des recollements personnalisés.

Leçons

- 120 : Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.
- 121 : Nombres premiers. Applications.
- 123 : Corps finis. Applications.

Références

[1] J.-P. Serre. *Cours d'arithmétique*. Puf, 1994.

Tout est dans [1].
Dans la suite sauf mention du contraire, p est premier et $q = p^n$.

Définition 1. On note $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q : \exists g \in \mathbb{F}_q, x = y^2\}$ et $\mathbb{F}_q^{*2} = \mathbb{F}_q^2 \cap \mathbb{F}_q^*$. Si p est premier différent de 2, on note $\left(\frac{x}{p}\right)$ l'entier $x^{\frac{p-1}{2}}$ pour tout $x \in \mathbb{F}_p^*$. Si $x = 0$, on étend en écrivant $\left(\frac{0}{p}\right) = 0$.

***Proposition* 2.** Pour $p = 2$, on a $\mathbb{F}_q^2 = \mathbb{F}_q$. Sinon, $|\mathbb{F}_q^2| = \frac{q+1}{2}$ et $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$.

Démonstration. Puisque $x \in \mathbb{F}_q \mapsto x^p \in \mathbb{F}_q$ est un automorphisme de corps, le cas $p = 2$ est automatique. Sinon, pour $p \neq 2$, l'application $x \in \mathbb{F}_q^* \mapsto x^2 \in \mathbb{F}_q^{*2}$ est un morphisme de groupes de noyau de $\{-1, 1\}$ – le polynôme $X^2 - 1$ admet au plus deux racines dans le corps $\mathbb{F}_q$ et $-1, 1$ sont racines distinctes, $-1 \neq 1$ –. Elle est par construction surjective donc

$$q - 1 = 2 \times |\mathbb{F}_q^{*2}|$$

donc $|\mathbb{F}_q^{*2}| = \frac{q-1}{2}$. Tout carré est inversible sauf 0 : ainsi, $\mathbb{F}_q^2 = \mathbb{F}_q^{*2} \cup \{0\}$ et son cardinal est $\frac{q+1}{2}$. □

***Proposition* 3.** Soit $p \in \mathcal{P}, p > 2$. Alors $x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$.

Démonstration. Le sens direct est clair. Réciproquement, soit $X = \{x \in \mathbb{F}_q^{*2} : x^{\frac{q-1}{2}} = 1\}$. Alors X contient tous les carrés inversibles et son cardinal est au plus $\frac{q-1}{2}$ – X forme les racines d'un polynôme de degré au plus $\frac{q-1}{2}$ – qui se trouve être le cardinal de $\mathbb{F}_q^{*2}$. Ainsi, $X = \mathbb{F}_q^{*2}$. □

Il est alors immédiat que $x \neq 0$ est un carré dans $\mathbb{F}_p$ si, et seulement si, $\left(\frac{x}{p}\right) = 1$. Traitons 2 cas particulier.

***Proposition* 4.** Soit $p \in \mathcal{P}, p > 2$. (-1) est un carré sur $\mathbb{F}_q$ si, et seulement si $q \equiv 1[4]$.

Démonstration. (-1) est un carré si, et seulement si, $(-1)^{\frac{q-1}{2}} = 1$ ce qui demande la parité de $\frac{q-1}{2}$ et c'est équivalent à $q - 1 \equiv 0[4]$. □

***Proposition* 5.** Soit $p \in \mathcal{P}, p > 2$. 2 est un carré sur $\mathbb{F}_p$ si, et seulement si, $p \equiv \pm 1[8]$.

Démonstration. Soit Ω une clôture algébrique de $\mathbb{F}_q$ et α une racine 8e primitive de l'unité. Alors $\alpha^4 = -1$ et en posant $y = \alpha + \alpha^{-1}$, on a $y^2 = 2$. Par Frobenius, $y^p = \alpha^p + \alpha^{-p}$. p étant impair, p est congru à $\pm 1[8]$ ou à $\pm 5[8]$.

- Si $p \equiv \pm 1[8]$, alors $y^p = \alpha + \alpha^{-1} = y$: d'où $\left(\frac{2}{p}\right) = y^{p-1} = 1$ donc 2 est un carré dans $\mathbb{F}_p$.
- Si $p \equiv \pm 5[8]$, alors $y^p = -y$ – puisque $\alpha^4 = \alpha^{-4} = -1$ – : d'où $\left(\frac{2}{p}\right) = y^{p-1} = -1$ donc 2 n'est pas un carré dans $\mathbb{F}_p$.

□

Théorème 6 (Loi de réciprocité quadratique)**.** *Soit p, q deux nombres premiers distincts. Alors*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}.$$

Quelles sont les étapes de la preuve ? En notant formellement $y = \sum_{x \in \mathbb{F}_p} \left(\frac{x}{p}\right)\omega^x$ avec ω racine q-ème de l'unité dans une clôture algébrique, on montre que $y^2 = (-1)^{\frac{q-1}{2}} q$. On passe ensuite à la conclusion en regardant y^p.

Démonstration. Soit Ω une clôture algébrique de $\mathbb{F}_p$ et ω une racine q-ème de l'unité. On note

$$y = \sum_{x \in \mathbb{F}_q} \left(\frac{x}{q}\right)\omega^x.$$

Cette somme est bien définie puisque $\forall k \in \mathbb{Z}, \omega^{x+kq} = \omega^x$. Ainsi,

$$\begin{aligned}
y^2 &= \sum_{x \in \mathbb{F}_q} \sum_{t \in \mathbb{F}_q} \left(\frac{xt}{q}\right)\omega^{x+t} \\
&\underset{u=t+x}{=} \sum_{x \in \mathbb{F}_q} \sum_{u \in \mathbb{F}_q} \left(\frac{x(u-x)}{q}\right)\omega^u \\
&= \sum_{x \in \mathbb{F}_q^*} \sum_{u \in \mathbb{F}^q} \underbrace{\left(\frac{-x^2}{q}\right)}_{=(-1)^{\frac{q-1}{2}}} \left(\frac{1-ux^{-1}}{q}\right)\omega^u \\
&= (-1)^{\frac{q-1}{2}} \sum_{x \in \mathbb{F}_q^*} \sum_{u \in \mathbb{F}^q} \left(\frac{1-ux^{-1}}{q}\right)\omega^u \\
&= (-1)^{\frac{q-1}{2}} \sum_{u \in \mathbb{F}^q} \omega^u \sum_{x \in \mathbb{F}_q^*} \left(\frac{1-ux^{-1}}{q}\right)
\end{aligned}$$

Or, $x \in \mathbb{F}_q^* \mapsto 1 - ux^{-1} \in \mathbb{F}_q \backslash \{1\}$ est une bijection pour tout $u \in \mathbb{F}_q^*$: on en déduit que pour tout $u \in \mathbb{F}_q^*$

$$\sum_{x \in \mathbb{F}_q^*} \left(\frac{1-ux^{-1}}{q}\right) = \sum_{s \in \mathbb{F}_q} \left(\frac{s}{q}\right) - \left(\frac{1}{q}\right) = -1$$

car il y a $\dfrac{q-1}{2}$ carrés et non carrés non nuls sur $\mathbb{F}_q$. Cette même somme vaut $q-1$ si $u=0$. Ainsi,

$$y^2 = (-1)^{\frac{q-1}{2}} \left(u^0(q-1) - \sum_{u \in \mathbb{F}_q^*} \omega^u \right)$$

Or,

$$\sum_{u \in \mathbb{F}_q^*} \omega^u = \sum_{k=1}^{q-1} \omega^k = \sum_{k=1}^{q} \omega^k - \omega^q = 0 - 1$$

donc

$$y^2 = (-1)^{\frac{q-1}{2}} q.$$

On va aussi regarder y^p. On a par Frobenius,

$$y^p = \sum_{x \in \mathbb{F}_q} \underbrace{\left(\frac{x}{q}\right)^p}_{=(\frac{x}{q}) \text{ car } p \text{ est premier}} \omega^{xp}.$$

Or, p est premier avec q donc $x \in \mathbb{F}_q \mapsto xp \in \mathbb{F}_q$ est une bijection : on a

$$y^p = \sum_{x \in \mathbb{F}_q} \left(\frac{xp^{-1}}{q}\right) \omega^x = \left(\frac{p-1}{q}\right) y = \left(\frac{p}{q}\right) y.$$

Pour conclure, il suffit de voir

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

□