Université P. et M. Curie (Paris VI) date de mise à jour: 05/03/2009
Deuxième semestre 2008/2009

Master de sciences et technologies 1ère année - Mention : Mathématiques et applications
Spécialité : Mathématiques Fondamentales

Cinquième fascicule : 02/03/2009

3 Corps finis

Références :
M. Mignotte, *Algèbre concrète*, Cours et exercices ; Chap. III : Les corps finis. Ellipses, 2003, 206p.
M. Demazure [4], Chap. 8.
S. Lang [9], Chap. 5 § 5.
D.S. Dummit & R.M. Foote [5], § 14.3.
R. Lidl & H. Niederreiter [10].
V. Shoup [15], Chap. 20.

3.1 Structure des corps finis

Soit K un corps. Rappelons (voir l'exercice au début du § 2.7) que *tout sous-groupe fini du groupe multiplicatif $K^\times$ est cyclique.* Une des démonstrations est la suivante. La suite $(\Phi_n)_{n\geq 0}$ des polynômes cyclotomiques peut être définie par récurrence sur n par les relations $\Phi_0 = 1$, $\Phi_1(X) = X - 1$ et

$$X^n - 1 = \prod_{d|n} \Phi_d(X).$$

(cf. (2.22)). Les racines du polynôme $X^n - 1$ dans K sont les racines n-ièmes de l'unité dans K, les racines du polynôme $\Phi_n(X)$ dans K sont les racines primitives n-ièmes de l'unité dans K, c'est–à–dire les éléments d'ordre n dans le groupe multiplicatif $K^\times$. Maintenant soit G un sous-groupe de $K^\times$ d'ordre n. Tout élément x de G vérifie $x^n = 1$, donc d'après (2.22) est racine d'un des Φ_d pour d divisant n. Notons a_d le nombre de racines de $\Phi_d(X)$ dans K. On vient de montrer $n \leq \sum_{d|n} a_d$. Mais Φ_d est un polynôme de degré $\varphi(d)$, et n'a donc pas plus de $\varphi(d)$ racines dans le corps K. Les degrés des deux membres de (2.22) donnent $\sum_{d|n} \varphi(d) = n$. Ainsi

$$n \leq \sum_{d|n} a_d \leq \sum_{d|n} \varphi(d) = n.$$

Il en résulte que $a_d = \varphi(d)$ pour tout $d|n$, en particulier pour $d = n$, donc $a_n \geq 1$ et il existe dans G au moins un élément d'ordre n. Ceci montre que G est cyclique, que G est l'unique sous-groupe de $K^\times$ d'ordre n (il est constitué des racines du polynôme $X^n - 1$) et que le polynôme $X^n - 1$ est

complètement décomposé dans K sans racine multiple. Les générateurs du groupe cyclique G sont les $\varphi(n)$ racines de Φ_n.

Supposons maintenant K de caractéristique finie p et soit m un entier positif. Écrivons $m = p^s n$ avec $s \geq 0$ et $\mathrm{pgcd}(p, n) = 1$. Dans $K[X]$ on a

$$X^m - 1 = (X^n - 1)^{p^s}.$$

On en déduit que l'ordre d'un sous-groupe fini du groupe multiplicatif $K^\times$ est premier avec p.

Soit maintenant K un corps fini ayant q éléments. La caractéristique de K est alors un nombre premier p, le sous-corps premier est (isomorphe à) $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ et K est une extension finie de $\mathbf{F}_p$. Si on pose $s = [K : \mathbf{F}_p]$, alors $q = p^s$.

Le groupe multiplicatif de K est d'ordre $q - 1$, tout élément de $K^\times$ vérifie $x^{q-1} = 1$, par conséquent $K^\times$ est l'ensemble des racines du polynôme $X^{q-1} - 1$:

$$X^{q-1} - 1 = \prod_{x \in K^\times} (X - x),$$

tandis que K est l'ensemble des racines du polynôme $X^q - X$:

$$X^q - X = \prod_{x \in K} (X - x).$$

Soit K un corps de caractéristique finie p. Pour x et y dans K on a $(x+y)^p = x^p + y^p$. Il en résulte que l'application

$$\begin{array}{rccc} \mathrm{Frob}_p : & K & \to & K \\ & x & \mapsto & x^p \end{array}$$

est un automorphisme du corps K ; on l'appelle le *Frobenius* de K sur $\mathbf{F}_p$. Si s est un entier ≥ 0, on désigne par Frob_p^s l'automorphisme composé que l'on note aussi Frob_{p^s} :

$$\mathrm{Frob}_p^0 = I, \quad \mathrm{Frob}_{p^s} = \mathrm{Frob}_{p^{s-1}} \circ \mathrm{Frob}_p \qquad (s \geq 1),$$

de sorte que $\mathrm{Frob}_{p^s}(x) = x^{p^s}$ pour $x \in K$. Si K est fini avec p^s éléments alors l'automorphisme $\mathrm{Frob}_p^s = \mathrm{Frob}_{p^s}$ de K est l'identité.

Si K est un corps fini avec $q = p^s$ éléments, alors le groupe multiplicatif $K^\times$ de K est cyclique d'ordre $q - 1$. Si α un générateur de $K^\times$, c'est–à–dire un élément d'ordre $q - 1$, pour $1 \leq \ell < s$ on a $1 \leq p^\ell - 1 < p^s - 1 = q - 1$, donc $\alpha^{p^\ell - 1} \neq 1$ et $\mathrm{Frob}_p^\ell(\alpha) \neq \alpha$. Il en résulte que Frob_p est d'ordre s dans le groupe des automorphismes de K. Par conséquent l'extension $K/\mathbf{F}_p$ est galoisienne, de groupe de Galois le groupe cyclique d'ordre s engendré par Frob_p. La théorie de Galois montre alors que si F est un corps fini à q éléments et K une extension de F, alors l'extension K/F est galoisienne de groupe de Galois cyclique engendré par l'automorphisme Frob_q de K qui envoie x sur x^q : c'est le *Frobenius de K sur F*.

On en déduit aussi que si K est un corps fini, tout polynôme irréductible de $K[X]$ est séparable : *tout corps fini est parfait.*

En passant nous pouvons compléter la démonstration du corollaire 2.21 :

Proposition 3.1. *Si F est un corps fini et K une extension finie de F, alors l'extension K/F est monogène.*

Démonstration de la proposition 3.1. Soit $q = p^s$ le nombre d'éléments de K où p est la caractéristique de K ; le groupe multiplicatif $K^\times$ est cyclique : soit α un générateur de ce groupe. Alors

$$K = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\} = \mathbf{F}_p(\alpha),$$

et à plus forte raison $K = F(\alpha)$.

□

3.2 Construction des corps finis et théorie de Galois

Théorème 3.2. *Soient p un nombre premier et s un entier positif. On pose $q = p^s$. Il existe un corps ayant q éléments. Deux corps ayant q éléments sont isomorphes. Si Ω est un corps algébriquement clos de caractéristique p, alors Ω contient un unique sous-corps fini ayant q éléments,*

Démonstration. Soit K un corps de décomposition sur $\mathbf{F}_p$ du polynôme $X^q - X$. Alors K est l'ensemble des racines de ce polynôme et donc a q éléments.

Inversement, si K est un corps avec q éléments, alors K est l'ensemble des racines du polynôme $X^q - X$.

Par conséquent si Ω est un corps algébriquement clos de caractéristique p, alors le seul sous-corps de Ω ayant q éléments est l'ensemble des racines du polynôme $X^q - X$.

□

Notons $\overline{\mathbf{F}}_p$ une clôture algébrique de $\mathbf{F}_p$. Pour chaque entier $s \geq 1$ il existe un unique sous-corps fini de $\overline{\mathbf{F}}_p$ ayant p^s éléments : c'est l'ensemble des racines du polynôme $X^{p^s} - X$. On le note $\mathbf{F}_{p^s}$. Pour n et m entiers positifs, on a l'équivalence

$$\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m} \iff n \text{ divise } m; \tag{3.3}$$

si ces conditions sont vérifiées, alors l'extension $\mathbf{F}_{p^m}/\mathbf{F}_{p^n}$ est cyclique, de groupe de Galois le groupe cyclique d'ordre m/n engendré par Frob_{p^n}.

Exercice. Soient K un corps, m et n deux entiers ≥ 1, a et b deux entiers ≥ 2. Vérifier que les conditions suivantes sont équivalentes.
(i) n divise m
(ii) Dans $K[X]$ le polynôme $X^n - 1$ divise $X^m - 1$
(iii) $a^n - 1$ divise $a^m - 1$
(ii') Dans $K[X]$ le polynôme $X^{a^n} - X$ divise $X^{a^m} - X$
(iii') $b^{a^n} - b$ divise $b^{a^m} - b$.

`Indication.` *Si r est le reste de la division de m par n, alors $a^r - 1$ est le reste de la division de $a^m - 1$ par $a^n - 1$.*

Lemme 3.4. *Soient E un corps fini à q éléments, K une extension de E et f un élément de $K[X]$. Alors $f \in E[X]$ si et seulement si $f(X)^q = f(X^q)$.*

Démonstration. Nous avons vu au § 3.1 que, pour a dans K, on a $a^q = a$ si et seulement si $a \in E$. Comme q est une puissance de la caractéristique p de K, si on écrit

$$f(X) = a_0 + a_1 X + \cdots + a_n X^n,$$

on a

$$f(X)^p = a_0^p + a_1^p X^p + \cdots + a_n^p X^{np}$$

et par récurrence

$$f(X)^q = a_0^q + a_1^q X^q + \cdots + a_n^q X^{nq}$$

Par conséquent $f(X)^q = f(X^q)$ si et seulement si $a_i^q = a_i$ pour tout $i = 0, 1, \ldots, n$.

□

Théorème 3.5. *Soient F un corps fini à q éléments, K une extension de F et α un élément non nul de K algébrique sur F. Il existe des entiers $s \geq 1$ tels que $\alpha^{q^s} = \alpha$. Notons r le plus petit. Alors le corps $F(\alpha)$ a q^r éléments et le polynôme irréductible de α sur F est*

$$\prod_{i=0}^{r-1} (X - \alpha^{q^i}). \tag{3.6}$$

Démonstration. Soit $s = [F(\alpha) : F]$. L'extension $F(\alpha)/F$ est galoisienne de groupe de Galois le groupe cyclique d'ordre s engendré par Frob_q. Les conjugués de α sont les images de α par ces automorphismes. Comme Frob_q^s est l'identité sur K on a $\mathrm{Frob}_q^s(\alpha) = \alpha$. Si $\mathrm{Frob}_q^h(\alpha) = \mathrm{Frob}_q^\ell(\alpha)$ alors $\mathrm{Frob}_q^{h-\ell}(\alpha) = \alpha$. Il en résulte que si r est le plus petit entier positif tel que $\mathrm{Frob}_q^r(\alpha) = \alpha$, alors pour $\ell \in \mathbf{Z}$ si j est le reste de la division Euclidienne de ℓ par r on a $\mathrm{Frob}_q^\ell(\alpha) = \mathrm{Frob}_q^j(\alpha)$. Ceci montre que l'ensemble des conjugués de α est $\{\alpha, \mathrm{Frob}_q(\alpha), \mathrm{Frob}_q^2(\alpha), \ldots, \mathrm{Frob}_q^{r-1}(\alpha)\}$. Le théorème 3.5 en résulte.

□

Proposition 3.7. *Soient F un corps fini à q éléments et r un entier positif. Le polynôme $X^{q^r} - X$ est le produit de tous les polynômes unitaires irréductibles de $F[X]$ dont le degré divise r.*

Démonstration. Soit $f \in F[X]$ un polynôme irréductible de degré d. Notons $K = F[X]/(f)$ son corps de rupture sur K : c'est une extension de degré d de K, il a donc q^d éléments, la classe α de X vérifie $\alpha^{q^d} = \alpha$, donc le polynôme $X^{q^d} - X$ est multiple de f.

Si d divise r, alors le polynôme $X^{q^r} - X$ est multiple de $X^{q^d} - X$, donc multiple de f. Ceci montre que $X^{q^r} - X$ est multiple de tous les polynômes irréductibles de degré divisant r. Comme sa dérivée est -1, il n'a pas de facteur multiple.

Réciproquement si le polynôme $X^{q^r} - X$ est multiple de f, on a $\alpha^{q^r} = \alpha$ dans K, l'ensemble des $\alpha \in K$ qui vérifient $\alpha^{q^r} = \alpha$ est K lui-même et tout générateur γ du groupe multiplicatif $K^\times$, qui est d'ordre $q^d - 1$, satisfait $\gamma^{q^r - 1} = 1$. Il en résulte que $q^d - 1$ divise $q^r - 1$, donc d divise r.

□

Exercice. Soit F un corps fini à q éléments. Pour chaque entier n positif on désigne par $\Psi_q(n)$ le nombre de polynômes unitaires irréductibles de degré n dans $F[X]$.

a) Vérifier

$$q^n = \sum_{d|n} d\Psi_q(d)$$

b) En déduire

$$\Psi_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d},$$

où μ désigne la fonction de Möbius.

c) Donner les valeurs de $\Psi_2(n)$ pour $1 \le n \le 6$.

d) Vérifier

$$\frac{q^n}{2n} \le \Psi_q(n) \le \frac{q^n}{n}.$$

e) Soient p la caractéristique de F et $\mathbf{F}_p$ le sous-corps premier de F. Montrer que plus de la moitié des éléments α de F vérifient $F = \mathbf{F}_p(\alpha)$.

Exercice. Soient F un corps fini, E une extension de F et α, β deux éléments de E algébriques sur F de degrés respectivement a et b. On suppose a et b premiers entre eux. Vérifier

$$F(\alpha, \beta) = F(\alpha + \beta).$$

Soit F un corps fini ayant q éléments et soit E est une extension finie de degré s de F.Pour $\alpha \in E$, la norme de α de E sur F est le produit des conjugués de α sur F, tandis que la trace de α de E sur F est la somme de ces conjugués

$$\mathrm{N}_{E/F}(\alpha) = \prod_{i=0}^{s-1} \mathrm{Frob}_q^i(\alpha) = \alpha^{(q^s-1)/(q-1)}, \quad \mathrm{Tr}_{E/F}(\alpha) = \sum_{i=0}^{s-1} \mathrm{Frob}_q^i(\alpha) = \sum_{i=0}^{s-1} \alpha^{q^i}$$

Pour $\alpha \in F$ on a $\mathrm{N}_{E/F}(\alpha) = \alpha^s$ et $\mathrm{Tr}_{E/F}(\alpha) = s\alpha$. La norme $\mathrm{N}_{E/F}$ induit un homomorphisme surjectif du groupe $E^\times$ sur $F^\times$. La trace $\mathrm{Tr}_{E/F}$ est une application F–linéaire surjective de E sur F, dont le noyau est formé des racines dans E du polynôme $X + X^q + \cdots + X^{q^{s-1}}$.

Soit p un nombre premier. Désignons par $\overline{\mathbf{F}}_p$ une clôture algébrique algébrique de $\mathbf{F}_p$. L'extension $\overline{\mathbf{F}}_p/\mathbf{F}_p$ est algébrique infinie, normale et séparable : c'est une extension *galoisienne infinie*. Son *groupe de Galois* $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ est le groupe des automorphismes de $\mathbf{F}_p$. On le décrit comme la limite projective des groupes de Galois des extensions finies de $\mathbf{F}_p$ contenues dans $\overline{\mathbf{F}}_p/\mathbf{F}_p$:

$$\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p) = \varprojlim_{[L:\mathbf{F}_p]<\infty} \mathrm{Gal}(L/\mathbf{F}_p).$$

Ainsi $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ est le groupe

$$\hat{\mathbf{Z}} := \varprojlim_{n\to\infty} \mathbf{Z}/n\mathbf{Z}.$$

Cette limite projective est l'ensemble des $(a_n)_{n\ge1}$ dans le produit Cartésien $\prod_{n\ge1} \mathbf{Z}/n\mathbf{Z}$ qui vérifient $s_{nm}(a_n) = a_m$ pour tout couple d'entiers positifs (n, m) où m divise n, en désignant par

$$s_{n,m} : \mathbf{Z}/n\mathbf{Z} \longrightarrow \mathbf{Z}/m\mathbf{Z}$$

la surjection canonique.

On a aussi

$$\hat{\mathbf{Z}} := \prod_p \mathbf{Z}_p \quad \text{avec} \quad \mathbf{Z}_p = \varprojlim_{r\to\infty} \mathbf{Z}/p^r\mathbf{Z}.$$

Voir par exemple [5] exercice 19 p. 635 et [8] Appendice p. 288.

3.3 Décomposition des polynômes cyclotomiques en facteurs irréductibles

Théorème 3.8. *Soient $\mathbf{F}_q$ un corps fini à q éléments et n un entier premier avec q. On désigne par d l'ordre de q modulo n, c'est–à–dire l'ordre de l'image de q dans le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$. Alors tous les facteurs irréductibles du polynôme Φ_n dans $\mathbf{F}_q[X]$ sont de degré d.*

Démonstration. Dans un corps de décomposition K du polynôme Φ_n sur $\mathbf{F}_q$, soit α une racine de Φ_n. Nous avons vu que α était d'ordre n dans $K^\times$. Le degré de α sur $\mathbf{F}_q$ est donné par le théorème 3.5 : c'est le plus petit des entiers $s \geq 1$ tels que $\alpha^{q^s-1} = 1$. C'est donc le plus petit des entiers $s \geq 1$ tels que n divise $q^s - 1$, qui n'est autre que l'ordre de l'image de q dans le groupe multiplicatif $(\mathbf{Z}/n\mathbf{Z})^\times$.

□

Pour $d = 1$ cela signifie que si $\mathbf{F}_q$ un corps fini à q éléments et n un entier premier avec q, le polynôme cyclotomique Φ_n est complètement décomposé dans $\mathbf{F}_q$ si et seulement si $q \equiv 1 \pmod{n}$. On le voit directement puisque $\mathbf{F}_q^\times$ est cyclique d'ordre $q-1$.

L'autre cas extrême est $d = \varphi(n)$:

Corollaire 3.9. *Soient $\mathbf{F}_q$ un corps fini et n un entier premier avec q. Le polynôme Φ_n est irréductible sur $\mathbf{F}_q$ si et seulement si la classe de q modulo n est un générateur de $(\mathbf{Z}/n\mathbf{Z})^\times$.*

Bien entendu cela ne peut arriver que si le groupe $(\mathbf{Z}/n\mathbf{Z})^\times$ est cyclique.

Voici un troisième exemple d'application du théorème 3.8 :

Corollaire 3.10. *Soient $\mathbf{F}_q$ un corps fini et m un entier positif. Le polynôme Φ_{q^m-1} se décompose en produit de polynômes irréductibles sur $\mathbf{F}_q$ qui sont tous de degré m.*

3.4 Loi de réciprocité quadratique

Soit p un nombre premier. Étudions les extensions quadratiques du corps $\mathbf{F}_p$ à p éléments. Dans une extension algébriquement close de $\mathbf{F}_p$ il y en a une et une seule. Pour l'expliciter on est amené à étudier les polynômes unitaires irréductibles de degré 2 sur $\mathbf{F}_p$. Pour $p = 2$ il y en a un et un seul, $X^2 + X + 1$.

Supposons dorénavant p impair. Dans K on peut diviser par 2 : on écrit $X^2 + aX + b = (X + a/2)^2 + b - a^2/4$. Il reste à déterminer quels sont les carrés dans $\mathbf{F}_p$.

Un élément α du corps $\mathbf{F}_p$ est appelé *résidu quadratique* si l'équation $X^2 - \alpha$ a une racine dans $\mathbf{F}_p$, on dit qu'il est *non–résidu quadratique* sinon, c'est-à-dire si ce polynôme $X^2 - \alpha$ est irréductible sur $\mathbf{F}_p$. On dit qu'un entier $a \in \mathbf{Z}$ est *résidu quadratique modulo p* si sa classe $\alpha \in \mathbf{Z}/p\mathbf{Z}$ modulo p l'est, *non–résidu modulo p* dans le cas contraire. En notant α la classe de a modulo p on définit le *symbole de Legendre* par

$$\left(\frac{\alpha}{p}\right) = \left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } \alpha = 0 \\ 1 & \text{si } \alpha \text{ est résidu quadratique} \\ -1 & \text{si } \alpha \text{ est non–résidu quadratique.} \end{cases}$$

On a supposé p impair. L'application $x \mapsto x^2$ est un endomorphisme du groupe $\mathbf{F}_p^\times$, de noyau $\{-1, +1\}$. L'image de cette application a donc $(p-1)/2$ éléments, ce qui veut dire qu'il y a $(p-1)/2$

éléments dans $\mathbf{F}_p^\times$ qui sont des résidus quadratiques non nuls dans $\mathbf{F}_p$ et il y en a autant qui ne sont pas résidus quadratiques. On en déduit

$$\sum_{\alpha\in\mathbf{F}_p}\left(\frac{\alpha}{p}\right)=0. \tag{3.11}$$

Les résidus quadratiques dans $\mathbf{F}_p^\times$ sont les racines du polynôme $X^{(p-1)/2}-1$, les non–résidus sont les racines du polynôme $X^{(p-1)/2}+1$. Par conséquent pour $\alpha\in\mathbf{F}_p$ on a

$$\left(\frac{\alpha}{p}\right)=\alpha^{(p-1)/2}. \tag{3.12}$$

Par exemple

$$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}=\begin{cases}1 & \text{si } p\equiv\ \ 1 \pmod 4\\ -1 & \text{si } p\equiv -1 \pmod 4.\end{cases} \tag{3.13}$$

Si $\zeta\in\mathbf{F}_p$ est une *racine primitive modulo p* (c'est-à-dire un générateur de $\mathbf{F}_p^\times$, ou encore une racine primitive $p-1$-ième de l'unité), alors les résidus quadratiques modulo p sont les éléments ζ^k de $\mathbf{F}_p^\times$ avec $0\le k\le p-3$ et k pair, tandis que les non–résidus quadratiques sont les ζ^k avec $1\le k\le p-2$ et k impair. En particulier

$$\left(\frac{\zeta}{p}\right)=-1$$

et (*théorème de Wilson*)

$$(p-1)!\equiv\prod_{k=1}^{p-1}\zeta^k\equiv\zeta^{p(p-1)/2}\equiv\zeta^{(p-1)/2}\equiv\left(\frac{\zeta}{p}\right)\equiv-1 \pmod p.$$

Lemme 3.14. *Pour α et β dans $\mathbf{F}_p$ on a*

$$\left(\frac{\alpha\beta}{p}\right)=\left(\frac{\alpha}{p}\right)\left(\frac{\beta}{p}\right).$$

De plus

$$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}=\begin{cases}1 & \textit{si } p\equiv\pm1 \pmod 8\\ -1 & \textit{si } p\equiv\pm3 \pmod 8.\end{cases}$$

Démonstration. La relation (3.12) montre que l'application

$$\alpha\longmapsto\left(\frac{\alpha}{p}\right)$$

est un homomorphisme du groupe multiplicatif $\mathbf{F}_p^\times$ sur le groupe à deux éléments $\{-1,+1\}$. Le noyau est constitué des résidus quadratiques dans $\mathbf{F}_p^\times$.

Pour savoir si 2 est résidu quadratique modulo p, on doit déterminer si le polynôme X^2-2 est réductible ou non dans $\mathbf{F}_p[X]$.

Dans le corps des nombres complexes, une des racines primitives 8èmes de l'unité est

$$\zeta_8 = e^{2i\pi/8} = \frac{(1+i)\sqrt{2}}{2}.$$

Elle vérifie $\zeta_8^2 = i$ et $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$. On vérifie aussi

$$\zeta_8^n + \zeta_8^{-n} = \begin{cases} \sqrt{2} & \text{si } n \equiv 1 \text{ ou } 7 \pmod 8, \\ -\sqrt{2} & \text{si } n \equiv 3 \text{ ou } 5 \pmod 8. \end{cases}$$

Ces calculs complexes (et faciles) vont motiver ceux que nous allons faire en caractéristique finie p.

Soit $\overline{\mathbf{F}}_p$ une clôture algébrique de $\mathbf{F}_p$ et soit $\mathbf{F}_{p^2}$ le sous-corps de $\mathbf{F}_p$ ayant p^2 éléments. Comme p^2-1 est multiple de 8 il existe une racine primitive 8-ième de l'unité $\alpha \in \mathbf{F}_{p^2}$. Posons $\beta = \alpha + \alpha^{-1}$. On a $\alpha^4 = -1$ et $\alpha^2 = -\alpha^{-2}$, donc

$$\beta^2 = (\alpha + \alpha^{-1})^2 = \alpha^2 + \alpha^{-2} + 2 = 2.$$

Il s'agit maintenant de savoir si β est ou non dans $\mathbf{F}_p^\times$, c'est-à dire si β^p est égal à β ou à $-\beta$.

Si $p \equiv \pm 1 \mod 8$, alors $\{\alpha^p, \alpha^{-p}\} = \{\alpha, \alpha^{-1}\}$, donc $\beta^p = \beta$ et $\beta \in \mathbf{F}_p$, ce qui donne

$$\left(\frac{2}{p}\right) = 1.$$

Si $p \equiv \pm 3 \mod 8$, alors $\{\alpha^p, \alpha^{-p}\} = \{-\alpha, -\alpha^{-1}\}$, donc $\beta^p = -\beta$ et $\beta \notin \mathbf{F}_p$, d'où on conclut

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

□

Exercice. Vérifier que le polynôme $X^4 + 1$ est irréductible sur $\mathbf{Q}$ mais est réductible sur $\mathbf{F}_p$ pour tout nombre premier p.

Voici l'énoncé de la loi de réciprocité quadratique :

Théorème 3.15. *Soient p et ℓ des nombres premiers impairs distincts. Alors*

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}. \tag{3.16}$$

Il existe un grand nombre de démonstrations de cet énoncé, les premières ayant été données par C.F. Gauss. En voici une qui repose sur l'utilisation des *sommes de Gauss* qui sont définies de la façon suivante : soit K un corps contenant une racine primitive p-ième de l'unité ζ, c'est-à-dire un élément d'ordre p dans le groupe multiplicatif $K^\times$ [5]. On pose

$$S = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \zeta^a.$$

[5] Par exemple on peut prendre $K = \mathbf{C}$ et $\zeta = e^{2i\pi/p}$. Mais on ne peut pas prendre un corps de caractéristique p bien sûr !

Cette formule associe l'application

$$a \longmapsto \left(\frac{a}{p}\right)$$

qui est un homomorphisme de groupes multiplicatifs de $\mathbf{F}_p^\times$ dans $\{-1,\ +1\}$ (ce qu'on appelle un *caractère multiplicatif* – cf. Lemme 3.14) avec l'application

$$a \longmapsto \zeta^a$$

qui est un homomorphisme du groupe additif $\mathbf{F}_p$ dans le groupe multiplicatif $K^\times$ (*caractère additif*).

Démonstration du théorème 3.15. Comme ζ^a ne dépend que de la classe de a modulo p, qu'il en est de même du symbole de Legendre $\left(\frac{a}{p}\right)$ et que ce dernier est nul pour $a = 0$, on peut écrire

$$S = \sum_{\alpha\in\mathbf{F}_p^\times} \left(\frac{\alpha}{p}\right)\zeta^\alpha.$$

Soit $\alpha \in \mathbf{F}_p^\times$. L'application $\beta \mapsto \alpha\beta$ est une bijection du groupe $\mathbf{F}_p^\times$ sur lui même, donc

$$S = \sum_{\beta\in\mathbf{F}_p^\times} \left(\frac{\alpha\beta}{p}\right)\zeta^{\alpha\beta}.$$

Comme

$$\left(\frac{\alpha}{p}\right)\left(\frac{\alpha\beta}{p}\right) = \left(\frac{\alpha^2\beta}{p}\right) = \left(\frac{\beta}{p}\right)$$

on obtient

$$S^2 = \sum_{\alpha\in\mathbf{F}_p^\times} \left(\frac{\alpha}{p}\right)\zeta^\alpha \sum_{\beta\in\mathbf{F}_p^\times} \left(\frac{\alpha\beta}{p}\right)\zeta^{\alpha\beta} = \sum_{\beta\in\mathbf{F}_p^\times} \left(\frac{\beta}{p}\right) \sum_{\alpha\in\mathbf{F}_p^\times} \zeta^{\alpha(1+\beta)}.$$

Comme la somme des racines du polynôme $X^p - 1$ est nulle, on a

$$\sum_{\gamma\in\mathbf{F}_p} \zeta^\gamma = 0, \qquad \text{donc} \qquad \sum_{\gamma\in\mathbf{F}_p^\times} \zeta^\gamma = -1.$$

Ainsi

$$\sum_{\alpha\in\mathbf{F}_p^\times} \zeta^{\alpha(1+\beta)} = \begin{cases} p-1 & \text{si } \beta = -1 \\ -1 & \text{si } \beta \neq -1. \end{cases}$$

En utilisant (3.11) et (3.13) on en déduit

$$S^2 = (p-1)\left(\frac{-1}{p}\right) - \sum_{\substack{\beta\in\mathbf{F}_p^\times \\ \beta\neq -1}} \left(\frac{\beta}{p}\right) = p\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}p.$$

Ces calculs sont valables dans tout corps K contenant une racine primitive p-ième de l'unité ζ. Choisissons maintenant pour K une clôture algébrique $\overline{\mathbf{F}}_\ell$ de $\mathbf{F}_\ell$. On a dans $\overline{\mathbf{F}}_\ell$

$$S^\ell = \sum_{\alpha\in\mathbf{F}_p^\times} \left(\frac{\alpha}{p}\right)\zeta^{\ell\alpha} = \left(\frac{\ell}{p}\right) \sum_{\alpha\in\mathbf{F}_p^\times} \left(\frac{\ell\alpha}{p}\right)\zeta^{\ell\alpha} = \left(\frac{\ell}{p}\right) S,$$

donc

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

Alors, toujours dans $\overline{\mathbf{F}}_\ell$, on a

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

Ceci démontre la relation (3.16).

□