

Cinquième fascicule : 10/03/2008

### 3 Corps finis

#### 3.1 Structure des corps finis

Soit  $K$  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  $K$  vérifie  $x^q = x$  et par conséquent  $K$  est l'ensemble des racines du polynôme  $X^q - X$  :

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

tandis que  $K^\times$  est l'ensemble des racines du polynôme  $X^{q-1} - 1$  :

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

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

$$F : K \rightarrow K \\ x \mapsto x^p$$

est un automorphisme du corps  $K$  ; on l'appelle le *Frobenius* de  $K$ . Si  $\ell$  est un entier  $\geq 0$ , on désigne par  $F^\ell$  l'automorphisme composé

$$F^0 = I, \quad F^\ell = F^{\ell-1} \circ F \quad (\ell \geq 1),$$

de sorte que  $F^\ell(x) = x^{p^\ell}$  pour  $x \in K$ . Si  $K$  est fini avec  $p^s$  éléments alors  $F^s = I$ .

Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique. En particulier si  $K$  est fini avec  $q = p^s$  éléments alors le groupe multiplicatif  $K^\times$  de  $K$  est cyclique d'ordre  $q-1$ . Si  $\alpha$  un générateur de  $K^\times$  on a  $F^\ell(\alpha) \neq 1$  pour  $1 \leq \ell < s$  donc  $F$  est d'ordre  $s$  dans le groupe des automorphismes de  $K$ . Il en résulte que l'extension  $K/\mathbf{F}_p$  est galoisienne, de groupe de Galois le groupe cyclique d'ordre  $s$  engendré par  $F$ . On en déduit aussi que si  $K$  est un corps fini, tout polynôme 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  $k$  est un corps fini et  $K$  une extension finie de  $k$ , alors l'extension  $K/k$  est monogène.*

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

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

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

### 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  $\Omega$  est un corps algébriquement clos de caractéristique  $p$ , alors  $\Omega$  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  $\Omega$  est un corps algébriquement clos de caractéristique  $p$ , alors le seul sous-corps de  $\Omega$  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  $F^n$ .

**Exercice.** Soient  $K$  un corps,  $m$  et  $n$  deux entiers  $\geq 1$ ,  $a$  et  $b$  deux entiers  $\geq 2$ . 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

$$f(X) = a_0 + a_1X + \cdots + a_nX^n,$$

on a

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

et par récurrence

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

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

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

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

*Démonstration.* L'extension  $E(\alpha)/E$  est finie, soit  $s$  son degré. Le corps  $E(\alpha)$  est donc fini avec  $q^s$  éléments. Soit  $m$  l'ordre de  $\alpha$  dans le groupe multiplicatif  $E(\alpha)^\times$ . Comme ce groupe est d'ordre  $q^s - 1$ , on a  $q^s \equiv 1 \pmod{m}$ . Donc  $\alpha^{q^s-1} = 1$  et  $\alpha^{q^s} = \alpha$ .

Soit  $f$  le polynôme irréductible de  $\alpha$  sur  $E$ . On a  $f(X^q) = f(X)^q$  car  $f \in E[X]$ , donc l'ensemble des racines de  $f$  est stable sous l'automorphisme  $F : x \mapsto x^q$  (qui est une puissance du Frobenius).

Il en résulte que  $f$  est multiple du polynôme  $g$  défini par (3.6). Mais ce polynôme  $g$  appartient à  $E[X]$  car  $g(X^q) = g(X)^q$ . Par conséquent  $g = f$ . Ainsi  $f$  est de degré  $r$ , donc  $[E(\alpha) : E] = r$ , par conséquent  $E(\alpha)$  a  $q^r$  éléments. On en déduit aussi  $r = s$ . □

**Proposition 3.7.** *Soient  $E$  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  $E[X]$  dont le degré divise  $r$ .*

*Démonstration.* Soit  $f \in E[X]$  un polynôme irréductible de degré  $d$ . Notons  $K = E[X]/(f)$  son corps de rupture sur  $E$  : c'est une extension de degré  $d$  de  $E$ , il a donc  $q^d$  éléments, la classe  $\alpha$  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  $\gamma$  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  $r$ . □

### 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  $n$ . Alors tous les facteurs irréductibles du polynôme  $\Phi_n$  dans  $\mathbf{F}_q[X]$  sont de degré  $d$ .*

*Démonstration.* Soient  $p$  la caractéristique de  $K$ ,  $\overline{\mathbf{F}}_p$  une clôture algébrique de  $\mathbf{F}_q$ ,  $P$  un facteur irréductible de  $\Phi_n$  dans  $\mathbf{F}_q[X]$ ,  $s$  son degré et  $\mathbf{F}_{q^s}$  le sous-corps de  $\overline{\mathbf{F}}_p$  ayant  $q^s$  éléments. Le corps  $\mathbf{F}_{q^s}$  est donc un corps de rupture de  $P$  sur  $\mathbf{F}_q$ . Soit  $\zeta$  une racine de  $P$  dans  $K$ . Comme  $\zeta$  est racine de  $P$  et que  $P$  est facteur de  $\Phi_n$  on a  $\Phi_n(\zeta) = 0$ , donc  $\zeta$  est une racine primitive  $n$ -ième de l'unité.

D'un côté le fait que  $\zeta$  soit dans  $\mathbf{F}_{q^s}^\times$  implique  $\zeta^{q^s-1} = 1$ . Il en résulte que  $n$  divise  $q^s - 1$ , donc  $q^s \equiv 1 \pmod{n}$  et par conséquent  $d$  divise  $s$ .

D'un autre côté comme  $q^d \equiv 1 \pmod{n}$  et que  $\zeta^n = 1$  on a  $\zeta^{q^d} = \zeta$ , donc  $\zeta$  appartient au sous-corps  $\mathbf{F}_{q^d}$  à  $q^d$  éléments de  $\overline{\mathbf{F}}_p$ . Comme  $\mathbf{F}_{q^s} = \mathbf{F}_q(\zeta)$  on a  $\mathbf{F}_{q^s} \subset \mathbf{F}_{q^d}$ , donc (3.3)  $s$  divise  $d$ .  $\square$

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  $\Phi_n$  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  $\Phi_n$  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  $\Phi_{q^m-1}$  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  $p$  impair : comme 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  $\alpha$  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  $\alpha$  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 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

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

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  $\zeta^k$  de  $\mathbf{F}_p^\times$  avec  $0 \leq k \leq p-3$  et  $k$  pair, tandis que les non résidus quadratiques sont les  $\zeta^k$  avec  $1 \leq k \leq p-2$  et  $k$  impair. En particulier

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

et (*théorème de Wilson*)

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

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

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

Par exemple

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

**Lemme 3.13.** *Pour  $\alpha$  et  $\beta$  dans  $\mathbf{F}_p$  on a*

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

*De plus*

$$\left( \frac{2}{p} \right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{si } p \equiv \pm 1 \pmod{8} \\ -1 & \text{si } p \equiv \pm 3 \pmod{8}. \end{cases}$$

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

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

est un homomorphisme du groupe multiplicatif  $\mathbf{F}_p^\times$  sur le groupe à deux éléments  $\{-1, +1\}$ . Le noyau est d'ailleurs 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

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

Elle vérifie  $\alpha^2 = i$ . Le nombre  $\beta = \alpha + \alpha^{-1}$  est une racine du polynôme  $X^2 - 2$ . On vérifie aussi

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

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  $\beta$  est ou non dans  $\mathbf{F}_p^\times$ , c'est-à-dire si  $\beta^p$  est égal à  $\beta$  ou à  $-\beta$ .

Si  $p \equiv \pm 1 \pmod{8}$ , 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  $p \equiv \pm 3 \pmod{8}$ , 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 3.14.** *Soient  $p$  et  $\ell$  des nombres premiers impairs distincts. Alors*

$$\left(\frac{\ell}{p}\right) \left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2} \frac{\ell-1}{2}}. \quad (3.15)$$

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  $\zeta$ , c'est-à-dire un élément d'ordre  $p$  dans le groupe multiplicatif  $K^\times$ <sup>4</sup>. On pose

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

On met donc ensemble un caractère multiplicatif  $\mathbf{F}_p^\times \rightarrow K^\times$  et un caractère additif  $\mathbf{F}_p \rightarrow K$  du groupe  $\mathbf{F}_p^\times$  :

$$a \mapsto \left(\frac{a}{p}\right) \quad \text{et} \quad a \mapsto \zeta^a.$$

<sup>4</sup>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 !

*Démonstration du théorème 3.14.* Comme  $\zeta^a$  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

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

La somme des racines du polynôme  $X^p - 1$  est nulle, donc

$$\sum_{\gamma \in \mathbf{F}_p} \zeta^\gamma = 0 \quad \text{et} \quad \sum_{\gamma \in \mathbf{F}_p^\times} \zeta^\gamma = -1.$$

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) 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  $\zeta$ . Choisissons maintenant pour  $K$  une clôture algébrique  $\overline{\mathbf{F}}_\ell$  de  $\mathbf{F}_\ell$ . On a dans  $\overline{\mathbf{F}}_\ell$

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

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 (3.15). □

## Références

- [1] M. DEMAZURE – *Cours d'algèbre. Primalité. Divisibilité. Codes*, Nouvelle Bibliothèque Mathématique Cassini, Paris, 1997.
- [2] D.S. DUMMIT & R.M. FOOTE – *Abstract Algebra*, Prentice Hall 1991, 1999.
- [3] M. HINDRY – *Arithmétique*, Calvage et Mounet, Tableau Noir, Paris, 2008.