Université P. et M. Curie (Paris VI),
Deuxième semestre 2006/2007

Michel Waldschmidt
date de mise à jour: 27/02/2007

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

Mention : Mathématiques et applications
MO11 : Théorie des nombres (12 ECTS)

Deuxième partie : Corps finis

Fascicule 4 : Chapitre 2, sections 2.1 à 2.5 (8 pages) [1]

2 Corps finis

2.1 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 $s = [\mathbf{F}_p : \mathbf{F}]$, 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

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

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

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

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 α 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

[1] Ce texte est téléchargeable à partir de la page http ://www.math.jussieu.fr/∼miw/enseignement.html

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 1.21 :

Proposition 2.1. *Si k est un corps fini et K une extension finie de k, alors l'extension K/k est monogène.*

Démonstration de la proposition 2.1. Soit $q = p^s$ le nombre d'éléments de K ; le groupe multiplicatif $K^\times$ est cyclique : soit α 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 $K = k(\alpha)$.

□

2.2 Construction des corps finis et théorie de Galois

Théorème 2.2. *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

$$\mathbf{F}_{p^n} \subset \mathbf{F}_{p^m} \iff n \text{ divise } m; \tag{2.3}$$

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 ≥ 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 2.4. *Soient K un corps de caractéristique p et f un élément de $K[X]$. Alors $f \in \mathbf{F}_p[X]$ si et seulement si $f(X)^p = f(X^p)$.*

Démonstration. Nous avons vu au § 2.1 que, pour a dans K, on a $a^p = a$ si et seulement si $a \in \mathbf{F}_p$. Comme K est de caractéristique p, si on écrit

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

on a

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

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

□

Proposition 2.5. *Soient K un corps de caractéristique finie p, α un élément non nul de K algébrique sur $\mathbf{F}_p$. Il existe des entiers $s \geq 1$ tels que $\alpha^{p^s} = \alpha$. Notons r le plus petit. Alors le corps $\mathbf{F}_p(\alpha)$ a p^r éléments et le polynôme irréductible de α sur $\mathbf{F}_p$ est*

$$\prod_{i=0}^{r-1} (X - \alpha^{p^i}). \tag{2.6}$$

Démonstration. L'extension $\mathbf{F}_p(\alpha)/\mathbf{F}_p$ est finie, donc le corps $\mathbf{F}_p(\alpha)$ est fini : soit p^s son nombre d'éléments. Soit m l'ordre de α dans le groupe multiplicatif $\mathbf{F}_p(\alpha)^\times$. Comme ce groupe est d'ordre $p^s - 1$, on a $p^s \equiv 1 \pmod{m}$. Donc $\alpha^{p^s - 1} = 1$ et $\alpha^{p^s} = \alpha$.

Soit f le polynôme irréductible de α sur $\mathbf{F}_p$. On a $f(X^p) = f(X)^p$ car $f \in \mathbf{F}_p[X]$, donc l'ensemble des racines de f est stable sous le Frobenius $F : x \mapsto x^p$.

Il en résulte que f est multiple du polynôme g défini par (2.6). Mais ce polynôme g appartient à $\mathbf{F}_p[X]$ car $g(X^p) = g(X)^p$. Par conséquent $g = f$. Ainsi f est de degré r, donc $[\mathbf{F}_p(\alpha) : \mathbf{F}_p] = r$, par conséquent $\mathbf{F}_p(\alpha)$ a p^r éléments. On en déduit aussi $r = s$.

□

Proposition 2.7. *Soient p un nombre premier et r un entier positif. Le polynôme $X^{p^r} - X$ est le produit de tous les polynômes unitaires irréductibles de $\mathbf{F}_p[X]$ dont le degré divise r.*

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

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

□

2.3 Décomposition des polynômes cyclotomiques en facteurs irréductibles

Théorème 2.8. *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 Φ_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 Φ_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 ζ une racine de P dans K. Comme ζ est racine de P et que P est facteur de Φ_n on a $\Phi_n(\zeta) = 0$, donc ζ est une racine primitive n-ième de l'unité.

D'un côté le fait que ζ 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 ζ 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 (2.3) s divise d. □

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 2.9. *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 2.8 :

Corollaire 2.10. *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.*

2.4 Loi de réciprocité quadratique

Soit p un nombre premier. 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

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

Supposons 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

$$\sum_{\alpha \in \mathbf{F}_p} \left(\frac{\alpha}{p}\right) = 0. \tag{2.11}$$

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 moduio p sont les éléments ζ^k de $\mathbf{F}_p^\times$ avec $0 \leq k \leq p-3$ et k pair, tandis que les non résidus quadratiques sont les ζ^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

$$\left(\frac{\alpha}{p}\right) = \alpha^{(p-1)/2}. \tag{2.12}$$

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 2.13. *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

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

Démonstration. La relation (2.12) 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 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 $\mathbf{F}_p[X]$. 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

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

□

Voici l'énoncé de la loi de réciprocité quadratique :

Théorème 2.14. *Soient p et ℓ des nombres premiers impairs distincts. Alors*

$$\left(\frac{\ell}{p}\right)\left(\frac{p}{\ell}\right) = (-1)^{\frac{p-1}{2}\frac{\ell-1}{2}}. \tag{2.15}$$

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 ζ (c'est-à-dire un élément d'ordre p dans $K^\times$). On pose

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

Démonstration du théorème 2.14. Comme ζ^a ne dépend que de la classe de a modulo p et que le symbole de Legendre $\left(\frac{a}{p}\right)$ 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

$$S^2 = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \zeta^a \sum_{\beta \in \mathbf{F}_p^\times} \left(\frac{\alpha\beta}{p}\right) \zeta^{\alpha\beta} = \sum_{\beta \in \mathbf{F}_p^\times} \left(\frac{\beta}{p}\right) \sum_{\alpha \in \mathbf{F}_p^\times} \zeta^{\alpha(1+\beta)}.$$

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

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

En utilisant (2.11) on en déduit

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

Ainsi

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

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

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

Ceci démontre la relation (2.15).

□

2.5 Factorisation dans $\mathbf{F}_p[X]$

Soit $f \in \mathbf{Z}[X]$ un polynôme unitaire. Une des méthodes efficaces pour factoriser f en produit de polynômes irréductibles consiste à étudier sa réduction modulo p pour différentes valeurs de p premier. Si, pour un nombre premier p, la réduction modulo p de f est irréductible dans $\mathbf{F}_p[X]$, alors f lui-même est irréductible.

Un critère d'irréductibilité pour un polynôme de $\mathbf{F}_p[X]$ est donné par la proposition suivante :

Proposition 2.16. *Soient p un nombre premier, $A \in \mathbf{F}_p[X]$ un polynôme unitaire non nul et $m \geq 1$ un entier positif. Les deux conditions suivantes sont équivalentes.*
(i) A est produit de polynômes unitaires irréductibles sur $\mathbf{F}_p$ deux-à-deux distincts de degré m.
(ii) $A(X)$ divise $X^{p^m} - X$ et pour tout diviseur premier ℓ de m,

$$\operatorname{pgcd}\big(X^{p^{m/\ell}} - X, A(X)\big) = 1.$$

Démonstration. La proposition 2.7 montre qu'un polynôme unitaire dans $\mathbf{F}_p[X]$ divise $X^{p^m} - X$ si et seulement s'il est produit de facteurs irréductibles unitaires deux-à-deux distincts de degrés divisant m. La condition *(ii)* revient à dire qu'aucun de ces facteurs n'a un degré divisant strictement m.

□

Le critère de Berlekamp permet non seulement de décider si un polynôme de $\mathbf{F}_p[X]$ est irréductible, mais aussi de disposer d'un algorithme pour le factoriser.

Proposition 2.17. *Soient p un nombre premier et $A \in \mathbf{F}_p[X]$ un polynôme unitaire sans facteurs carrés. On écrit sa décomposition en facteurs irréductibles dans $\mathbf{F}_p[X]$:*

$$A = A_1 \cdots A_r$$

où les polynômes A_i sont unitaires et irréductibles dans $\mathbf{F}_p[X]$, deux-à-deux distincts. Soit $Q \in \mathbf{F}_p[X]$. Alors les deux conditions suivantes sont équivalentes :
(i)

$$Q(X)^p \equiv Q(X) \pmod{A(X)}.$$

(ii) Pour tout $i = 1, \ldots, r$, il existe $\alpha_i \in \mathbf{F}_p$ tel que

$$Q(X) \equiv \alpha_i \pmod{A_i(X)}.$$

De plus il existe p^r polynômes satisfaisant ces conditions qui sont soit le polynôme nul, soit de degré $< \deg A$.

Démonstration. Pour $1 \leq i \leq r$ le quotient K_i de $\mathbf{F}_p[X]$ par l'idéal principal (A_i) est un corps et l'anneau quotient $\mathbf{F}_p[X]/(A)$ est isomorphe au produit $K_1 \times \cdots \times K_r$ (ces deux anneaux ont p^d éléments, d désignant le degré de A). Un tel isomorphisme Ψ est

$$P \pmod{A} \longmapsto \big(P \pmod{A_i}\big)_{1 \leq i \leq r}.$$

Dans chaque K_i le polynôme $X^p - X$ a p racines, à savoir les p éléments du sous-corps premier $\mathbf{F}_p$. Donc l'équation

$$(x_1^p, \ldots, x_r^p) = (x_1, \ldots, x_r)$$

a p^r solutions dans $K_1 \times \cdots \times K_r$. Ces solutions sont les images par Ψ des classes modulo A des polynômes $Q \in \mathbf{F}_p[X]$ satisfaisant $Q^p \equiv Q \pmod{A}$.

□

Exercice. Sous les hypothèses de la proposition 2.17, on désigne par R l'anneau quotient $\mathbf{F}_p[X]/A(X)\mathbf{F}_p[X]$, par $S : R \to R$ l'endomorphisme $Q \mapsto Q^p$ du $\mathbf{F}_p$-espace vectoriel R et on pose $N = \ker(S - I)$. Quelle est la dimension du $\mathbf{F}_p$-espace vectoriel N ?

On suppose $r \geq 2$. Soit $Q \in N$. Vérifier

$$A = \prod_{\alpha \in \mathbf{F}_p} \operatorname{pgcd}(A, Q - \alpha).$$

Montrer que si Q n'est pas dans $\mathbf{F}_p$, alors il existe $\alpha \in \mathbf{F}_p$ tel que $\operatorname{pgcd}(A, Q - \alpha)$ soit différent de 1 et de A.

Références

[1] M. Demazure – *Cours d'algèbre. Primalité. Divisibilité. Codes*, Nouvelle Bibliothèque Mathématique Cassini, Paris, 1997.