Table des matières

[11pt,a4]amsbook [T1]fontenc [french]babel color
setspace amsmath amssymb graphpap graphicx
Théorème[section] [theo]Définition [theo]Proposition Démonstration [theo]Lemme [theo]Remarque [theo]Exemple [theo]Corollaire [section]Exercise [theo]Conjecture
Définition Théorème Propriété
lettrine
fancyheadings

Corps finis

Par $\mathbb{Z}_n$ on note l'anneau $\mathbb{Z}/n\mathbb{Z}$.
Un corps est un anneau où tous les éléments non nuls sont inversibles.
Un corps fini est aussi appelé corps de Galois qu'on note $GF(q)$ ou $\mathbb{F}_q$.

0.1. Propriétés des corps finis

THÉORÈME 0.1.1. *L'anneau $(\mathbb{Z}_n, +, .)$ est un corps si et seulement si n est un nombre premier.*

DÉMONSTRATION. $\Rightarrow$) $(\mathbb{Z}_n, +, .)$ est un corps. Si $n = ab$, avec $1 < a, b < n$, alors $b = a^{-1}ab = a^{-1}n = 0 \mod n$, contradiction.
$\Leftarrow$) n est un nombre premier. Tout nombre $1 \leq m \leq n-1$ est premier avec n. D'après le théorème de Bezout il existe des entiers u et v tels que $un + vm = 1$ d'où en passant à $\mathbb{Z}_n$ $\bar{v}\bar{m} \equiv \bar{1}$ et $\bar{m}$ est inversible, donc $(\mathbb{Z}_n, +, .)$ est un corps. □

DÉFINITION 0.1.2. *Tout corps K contenant le corps $\mathbb{F}$ s'appelle extension de $\mathbb{F}$. K est un espace vectoriel sur F et on sa dimension $[K : F]$.*

THÉORÈME 0.1.3. *Soit $\mathbb{F}$ un corps. Alors ou bien $\mathbb{F}$ est une extension du corps $\mathbb{Q}$ des nombres rationnels, ou bien $\mathbb{F}$ est une extension de $\mathbb{Z}_p$ pour un nombre premier p uniquement déterminé.*

Preuve : On considère le morphisme d'anneaux $f : \mathbb{Z} \longrightarrow \mathbb{F}$ défini par $f(1) = 1$. Si f est injective, alors $\mathbb{F}$ contient l'image $f(\mathbb{Z})$, qui est isomorphe à $\mathbb{Z}$, et le corps de fraction de $\mathbb{Z}$ qui est isomorphe à $\mathbb{Q}$. Si f n'est pas injective il existe un plus petit entier non nul p tel que $f(p) = 0$ et $ker(f) = p\mathbb{Z}$. L'image $f(\mathbb{Z})$ est isomorphe à $\mathbb{Z}_p$. Si p n'est pas premier alors $p = rs$ où $1 < r, s < p$ d'où $f(p) = f(rs) = f(r)f(s) = 0$ dans $\mathbb{F}$, ce qui n'est pas possible.

COROLLAIRE 0.1.4. *Soit $\mathbb{F}$ un corps, alors la caractéristique de $\mathbb{F}$ est soit nulle, soit un nombre premier.*

DÉFINITION 0.1.5. *Soit R un anneau. La caractéristique de R est le plus petit entier $m > 0$ lorsqu'il existe vérifiant $ma = 1 + \cdots + 1 = 0$. Si un tel m n'existe pas, càd pour tout $m \in \mathbb{N}^*$, $m.1 \neq 0$, on dit alors que R est de caractéristique nulle.*

LEMME 0.1.6. *Soit $\mathbb{F}$ un corps fini de caractéristique p, alors $(a+b)^{p^i} = a^{p^i} + b^{p^i}$ pour tout $a, b \in \mathbb{F}$ et $i \in \mathbb{N}^*$.*

DÉMONSTRATION. On utilise la formule du binôme, et le fait que p divise $\binom{p}{k}$ car $p(p-1)\cdots(p-k+1) = k!\binom{p}{k}$ et p est premier et donc premier avec $k!$ puisque $0 < k < p$. Donc p divise $\binom{p}{k}$. Puis on raisonne par récurrence sur i. □

DÉFINITION 0.1.7. *L'ordre d'un corps fini $\mathbb{F}$ est le nombre d'éléments de $\mathbb{F}$.*

THÉORÈME 0.1.8. *Soit $\mathbb{F}$ un corps fini, alors l'ordre de $\mathbb{F}$ est p^r où p est un nombre premier et r est un entier > 0. De plus $\mathbb{F}$ contient un sous-corps isomorphe à $\mathbb{Z}_p$.*

DÉMONSTRATION. Puisque $\mathbb{F}$ est fini, $\mathbb{F}$ contient un sous corps isomorphe à $\mathbb{Z}_p$ et la caractéristique de $\mathbb{F}$ est un nombre premier p. $\mathbb{F}$ est un espace vectoriel fini sur $\mathbb{Z}_p$. Soit r sa dimension et $\omega_1, \cdots, \omega_r$ une base de $\mathbb{F}$ sur $\mathbb{Z}_p$. Chaque élément de $\mathbb{F}$ s'écrit d'une façon unique sous la forme $a_1.\omega_1 + \cdots + a_r.\omega_r$ avec $a_i \in \mathbb{Z}_p$. Donc $q = p^r$. □

Le sous corps de $\mathbb{F}_q$ isomorphe à $\mathbb{Z}_p$ s'appelle sous corps premier de $\mathbb{F}_q$.

COROLLAIRE 0.1.9. *Tout corps $\mathbb{F}$ d'ordre premier p est isomorphe à $\mathbb{Z}_p$.*

DÉMONSTRATION. D'après le Théorème 0.1.8, $\mathbb{F}$ contient un sous-corps isomorphe à $\mathbb{Z}_p$. Puisque $\mathbb{F}$ est d'ordre p il coïncide avec son sous-corps isomorphe à $\mathbb{Z}_p$. □

0.2. Construction de corps finis

On va montrer que pour tout nombre premier p et r un entier > 0 on peut construire un corps d'ordre p^r.

Soit $\mathbb{F}$ un corps alors $\mathbb{F}[x]$ est un anneau principal. càd pour tout idéal I dans $\mathbb{F}[x]$ on a $I = (p(x))$ où $p(x)$ est un polynôme non nul de plus petit degré dans I.

Soit $\mathbb{F}$ un corps, $p(x) \in \mathbb{F}[x]$, l'idéal engendré par $p(x)$ est

$$((p(x)) = (p(x))\mathbb{F}[x] = \{p(x)g(x) \mid g(x) \in \mathbb{F}[x]\}$$

L'anneau quotient

$$\mathbb{F}[x]/(p(x) = \{f(x) + I \mid f(x) \in \mathbb{F}[x]\}$$

on note $f(x) + I$ par $\overline{f(x)}$ ainsi $\overline{p(x)} = \overline{0}$.

Cet anneau est muni des opérations :
- addition : $\overline{f(x)} + \overline{g(x)} = \overline{f(x) + g(x)}$ et,
- multiplication : $\overline{f(x)}.\overline{g(x)} = \overline{f(x).g(x)}$

THÉORÈME 0.2.1. *K est un anneau. Soit $\mathbb{F}$ un corps et $p(x) \in \mathbb{F}[x]$ un polynôme irréductible sur $\mathbb{F}$. L'anneau quotient $K = \mathbb{F}[x]/(p(x))$ est un corps. De plus K contient un sous corps isomorphe à $\mathbb{F}$.*

DÉMONSTRATION. Soit $f(x) \in \mathbb{F}[x]$ tel que $\overline{f(x)} \neq 0$. Puisque $p(x)$ est irréductible et $p(x)$ n'est pas un facteur de $f(x)$ alors $pgcd(f(x), p(x)) = 1 \in \mathbb{F}^*$ d'où il existe $a(x)$ et $b(x)$ dans $\mathbb{F}[x]$ tels que $a(x)f(x)+b(x)p(x) = 1$ d'où $\bar{a}(x)\bar{f}(x) + \bar{b}(x)\bar{p}(x) = \bar{1}$ or $\overline{p}(x) = 0$. Donc tout élément non nul de K est inversible. Donc K est un corps.

On a $\mathbb{F} \subset \mathbb{F}[x]$ et on considère la restriction à $\mathbb{F}$ de la surjection canonique

$$\begin{aligned} \phi : \quad & \mathbb{F} \to K \\ & a \to \overline{a} \end{aligned}$$

c'est un morphisme injectif d'où $Im(\phi) = \overline{\mathbb{F}}$ est un sous corps de K. □

Nous avons montré que pour tout corps $\mathbb{F}$ nous pouvons construire un corps K contenant $\mathbb{F}$ comme sous corps. Nous disons que K est une extension de $\mathbb{F}$ et on identifie $\bar{a}$ avec $a \in \mathbb{F}$.

Soit $p(x) \in \mathbb{F}[x]$ un polynôme irréductible de degré $m \geq 1$: $p(x) = c_0 + c_1x + \cdots + c_mx^m$ et $f(x) \in \mathbb{F}[x]$, il existe deux polynômes $q(x)$ et $r(x)$ dans $\mathbb{F}(x)$ tel que $f(x) = q(x)p(x) + r(x)$ où $deg(r) < m$ et donc $r(x)$ est de la forme $r(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1}$ avec $a_i \in \mathbb{F}$.

En utilisant le fait que $\overline{p(x)} = \bar{0}$ on déduit que

$\overline{f(x)} = \overline{q}(x).\overline{p}(x) + \overline{r}(x) = \overline{a}_0 + \overline{a}_1\overline{x} + \cdots + \overline{a}_{m-1}.\overline{x}^{m-1}$

on pose $t = \overline{x}$ d'où $\overline{f(x)} = \overline{a}_0 + \overline{a}_1t + \cdots + \overline{a}_{m-1}.t^{m-1}$

THÉORÈME 0.2.2. *Soit $\mathbb{F}$ un corps et $p(x) = c_0+c_1x+\cdots+c_mx^m \in \mathbb{F}[x]$ un polynôme irréductible de degré $m \geq 1$. Alors le corps $K = \mathbb{F}[x]/(p(x))$ peut être représenté comme $K = \{a_0 + a_1t + \cdots + a_{m-1}t^{m-1}/a_0, \cdots, a_{m-1} \in \mathbb{F}; p(t) = 0\}$.*

Avec cette représentation d'addition est trivial. La multiplication :
si $a(t) = a_0 + \cdots + a_{m-1}t^{m-1}$ et $b(t) = b_0 + \cdots + b_{m-1}t^{-1}$

$$a(t)b(t) = a_0b_0 + (a_0b_1 + a_1b_0) + \cdots + a_{m-1}b_{m-1}t^{2m-2}$$

$$a(t)b(t) = q(t)(c_0 + c_1t + \cdots + c_mt_m) + d_0 + d_1t + \cdots + d_{m-1}t^{m-1}$$

d'où $a(t)b(t) = d_0 + d_1t + \cdots + d_{m-1}t^{m-1}$.

EXEMPLE 0.2.3. *L'anneau quotient $K = \mathbb{R}[x]/(x^2 + 1)$ est un corps isomorphe à $\mathbb{C}$. En effet, Puisque le polynôme $p(x) = x^2 + 1$ est irréductible sur $\mathbb{R}$, l'anneau quotient K est un corps. K peut être représenté par $K = \{a_0 + a_1t/a_0, a_1 \in \mathbb{R}\}$ où t vérifie $t^2 + 1 = 0$. On vérifie facilement que l'application $f : K \to \mathbb{C}$ définit par $f(a + bt) = a + ib$ est un isomorphisme de corps.*

Pour construire un corps fini d'ordre p^r, on considère le corps $\mathbb{Z}_p$ et $p(x) \in \mathbb{Z}_p[x]$ un polynôme irréductible de degré r. Soit $p(x) = c_0 + c_1x + \cdots + x^r$ alors le corps $K = \mathbb{Z}_p[x]/p(x)$ peut être représenté comme $K = \{a_0 + a_1t + \cdots + a_{r-1}t^{r-1} \mid a_i \in \mathbb{Z}_p, p(t) = 0\}$. K est d'ordre p^r.

THÉORÈME 0.2.4. *Il existe un corps $\mathbb{F}$ d'ordre n si et seulement si n est une puissance d'un nombre premier.*

$0 = 0$	$\alpha^7 = \alpha^3 + \alpha + 1$
$1 = 1$	$\alpha^8 = \alpha^2 + 1$
$\alpha = \alpha$	$\alpha^9 = \alpha^3 + \alpha,$
$\alpha^2 = \alpha^2$	$\alpha^{10} = \alpha^2 + \alpha + 1$
$\alpha^3 = \alpha^3$	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
$\alpha^4 = \alpha + 1$	$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^5 = \alpha^2 + \alpha$	$\alpha^{13} = \alpha^3 + \alpha^2 + 1$
$\alpha^6 = \alpha^3 + \alpha$	$\alpha^{14} = \alpha^3 + 1$

TABLE 1. Table du corps $\mathbb{F}_{16}$

DÉMONSTRATION. $\Rightarrow$) C'est le Théorème 0.1.8.

$\Leftarrow$) Soit p un nombre premier et $r \in \mathbb{N}^*$ tel que $n = p^r$ et $g(x)$ un polynôme irréductible dans $\mathbb{Z}_p[x]$ de degré r. $\mathbb{Z}_p[x]/(g(x))$ est un corps d'ordre p^r. □

COROLLAIRE 0.2.5. *Si $n = p^r$ où p un nombre premier et r un entier > 0. Alors il existe un corps fini $\mathbb{F}_{p^r}$ d'ordre p^r donné par*

$$\mathbb{F}_{p^r} = \left\{ a_0 + a_1 t + \cdots + a_{r-1} t^{r-1} \mid a_i \in \mathbb{Z}_p, p(t) = 0 \right\}$$

où $p(x) \in \mathbb{Z}_p[x]$ est un polynôme irréductible unitaire de degré r.

EXEMPLE 0.2.6. *Le polynôme x^2+1 est réductible sur $\mathbb{Z}_2$ car $(1+1=0)$ et $x^2 + 1 = (x + 1)(x + 1)$ dans $\mathbb{Z}_2[x]$.*

Par contre le polynôme $x^2 + x + 1$ est irréductible dans $\mathbb{Z}_2[x]$, on peut construire le corps $\mathbb{F}_4$. $\mathbb{F}_4 = \{0, 1, t, 1+t\}$. La somme par exemple $1+(1+t) = t$. La multiplication $t.(1 + t) = t + t^2 = -1 = 1$, $\mathbb{F}_4$ peut être identifié à $\mathbb{F}_2[x]/(x^2 + x + 1) = \{0, 1, t, 1 + t, t^2 + t + 1 = 0\}$.

EXEMPLE 0.2.7. *Cherchons un corps à 9 éléments. On a $9 = 3^2$, on a besoin d'un polynôme irréductible de degré 2 dans $\mathbb{Z}_3[x]$, $x^2 + 1$ l'est.*

$$\mathbb{F}_9 = \left\{ a + bt | a, b \in \mathbb{Z}_3, t^2 + 1 = 0 \right\}$$

d'où

$$\mathbb{F}_9 = \{0, 1, 2, t, 1 + t, 2 + t, 2t, 1 + 2t, 2 + 2t\}$$

Dans $\mathbb{F}_9$ on a $(1 + t)(1 + 2t) = 1 + t + 2t + 2t^2 = 1 + 2t^2 = 2$

EXEMPLE 0.2.8. *un corps à 16 éléments. On a $16 = 2^4$, un polynôme irréductible de degré 4 dans $\mathbb{Z}_2[x]$, est $x^4 + x + 1$. On note la classe de x par α alors α vérifie $\alpha^4 + \alpha + 1 = 0$ les éléments de $\mathbb{F}_{16}$ sont : 0, 1, α, $\alpha + 1$, α^2, $\alpha^2 + 1$, $\alpha^2 + \alpha$, $\alpha^2 + \alpha + 1$, α^3, $\alpha^3 + 1$, $\alpha^3 + \alpha$, $\alpha^3 + \alpha + 1$, $\alpha^3 + \alpha^2$, $\alpha^3 + \alpha^2 + 1$, $\alpha^3 + \alpha^2 + \alpha$, $\alpha^3 + \alpha^2 + \alpha + 1$.*

On a $\alpha^4 = \alpha + 1 = 0$ et $\alpha^5 = \alpha(\alpha + 1) = \alpha^2 + \alpha$ et ainsi de suite on obtient la Table 1.

THÉORÈME 0.2.9. *Soit $f(x) \in \mathbb{F}_q[x]$ un polynôme irréductible de degré m. Alors $\mathbb{F}_q[x]/(f(x)) \equiv \mathbb{F}_{q^m}$. De plus $f(x)$ a m racines distinctes dans*

$\mathbb{F}_q[x]/(f(x))$, *qui sont* $\bar{x}, \bar{x}^q, \bar{x}^{q^2}, \cdots, \bar{x}^{q^{m-1}}$ *où* $\bar{x}$ *est l'image de* $x \in \mathbb{F}_q[x]$ *dans* $\mathbb{F}_q[x]/(f(x))$.

DÉMONSTRATION. $\mathbb{F}_q[x]/(f(x))$ est un corps puisque $f(x)$ est irréductible. Et c'est un $\mathbb{F}_q$-espace vectoriel de dimension $deg(f(x)) = m$. D'où $\mathbb{F}_q[x]/(f(x))$ est d'ordre q^m, donc il est isomprphe à $\mathbb{F}_{q^m}$. □

THÉORÈME 0.2.10. *On* $\mathbb{F}_{p^r} \subset \mathbb{F}_{p's}$ *si et seulement si* $p = p'$ *et* r *divise* s.

DÉMONSTRATION. $\Rightarrow$) Si $\mathbb{F}_{p^r} \subset \mathbb{F}_{p^s}$ on a $p.1 = p'.1 = 0$ d'où $(p-p')1 = 0$ d'où $p = p'$. De plus $[\mathbb{F}_{p^r} : \mathbb{F}_p] = [\mathbb{F}_{p^r} : \mathbb{F}_{p^s}][\mathbb{F}_{p^s} : \mathbb{F}_p]$ d'où s divise r.
$\Leftarrow$: D'après le théorème précédent. □

COROLLAIRE 0.2.11. *Deux corps finis de même ordre sont isomorphes.*

LEMME 0.2.12. *Soit* $(G, .)$ *un groupe abélien,* a *et* b *deux éléments de* G *d'ordre* m *et* n *respectivement. Il existe un élément de* G *d'ordre* $ppcm(m, n)$.

DÉMONSTRATION. Posons $d = pgcd(m, n)$, $q = mn/d = ppcm(m, n)$, $c = a^d b$ et $c^q = (a^m)^n (b^n)^{m/d} = e$ d'où l'ordre de c divise q, on pose $r = ord(c)$. on a $c^r = e$ d'où $a^{dr} = b^{-r}$ et $ord(a^{dr}) = ord(b^{-r}) = ord(b^r) = t$ et $ord(a^{d)} = m/d$, $ord(b) = n$ donc t divise m/d et n mais m/d et n sont premier entre eux d'où q divise r. Donc $ord(c) = q = ppcm(m, n)$. □

THÉORÈME 0.2.13. *Soit* $\mathbb{F}$ *un corps fini et* $\mathbb{F}^* = \mathbb{F}\backslash\{0\}$ *alors,*
i) $(\mathbb{F}^*, .)$ *est un groupe cyclique d'ordre* q *où* $q = |\mathbb{F}^*|$.
ii) si α *est un générateur de* $\mathbb{F}^*$ *alors* $\mathbb{F} = \{0, 1 = \alpha^0, \cdots, \alpha^{q-2}\}$.
iii) $\alpha^k = 1$ *si seulement si* $q - 1$ *divise* k.

DÉMONSTRATION. Posons $|\mathbb{F}| = n$. $(\mathbb{F}^*, .)$ est un groupe abélien d'ordre $n-1$. Soit q le ppcm des ordres des éléments de $\mathbb{F}^*$. Alors $a^q = 1$ pour tout $a \in \mathbb{F}^*$, donc tout élément de $\mathbb{F}^*$, est une racine de $x^q - 1$, or un polynôme de degré q a au plus q racines. D'où $n - 1 \leq q$. En utilisant le lemme précédent, il existe un $\alpha \in \mathbb{F}^*$ d'ordre q. D'où q divise $n - 1$. Donc $q = n - 1$. Donc $\mathbb{F}^*$ est cyclique engendré par α. D'où i) et ii). iii) est trivial. □

Les éléments de $\mathbb{F}_q$ sont précisément les racines de $x^q - x$.

DÉFINITION 0.2.14. *Un générateur du groupe multiplicatif* $\mathbb{F}^*$ *est appelé élément primitif de* $\mathbb{F}$.

Un élément primitif du corps fini $\mathbb{F}_q$ est un élément d'ordre $q - 1$.

DÉFINITION 0.2.15. *Soit* $\mathbb{F}$ *un corps fini et* $\alpha \in \mathbb{F}$. *L'ordre de* α *est le plus petit entier* n *tel que* $\alpha^n = 1$.

D'après le Théorème 0.1.8 on a :

COROLLAIRE 0.2.16. *Dans tout corps fini* $\mathbb{F}_q$ *il existe un élément primitif* α *et on a*

$$\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{q-2}\}$$

et $\mathbb{F}_q$ est l'ensemble des racines du polynôme $x^q - x$. On a aussi $ord(\alpha^i) = \frac{q-1}{pgcd(i,q-1)}$.

THÉORÈME 0.2.17. *Soit α un élément primitif du corps $\mathbb{F}_q$. Les éléments primitifs de $\mathbb{F}_q$ sont les α^i tels que $pgcd(i, q-1) = 1$.*

COROLLAIRE 0.2.18. *Soit α un élément primitif du corps $\mathbb{F}_q$ et $\mathbb{F}_s$ un sous corps de $\mathbb{F}_q$, alors les éléments de $\mathbb{F}_s$ sont $\{0, 1, \beta, \cdots, \beta^{s-2}\}$ où $\beta = \alpha^{(q-1)/(s-1)}$.*

DÉFINITION 0.2.19. *Soit $\alpha \in \mathbb{F}_{q^m}$. Les nombres α, α^q, α^{q^2}, $\cdots$, $\alpha^{q^{m-1}}$ sont appelés les conjugués de α par rapport à $\mathbb{F}_q$.*

EXERCISE 0.3. *Trouver tous les éléments primitifs de $\mathbb{F}_8$ et $\mathbb{F}_9$.*

0.4. Automorphismes de corps finis

Le groupe des automorphismes du corps $\mathbb{F}_q$ est noté $Aut(\mathbb{F}_q)$ et s'appelle groupe de Galois du corps $\mathbb{F}_q$.

Soit le corps $\mathbb{F}_q$ de caractéristique p. L'application $\sigma_p : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ définie par $\sigma_p(x) = x^p$ s'appelle automorphisme de Frobenius.

THÉORÈME 0.4.1. *i) $Aut(\mathbb{F}_q)$ est un groupe cyclique d'ordre m et engendré par l'automorphisme de Frobenius σ_p.*
ii) Le sous corps premier de $\mathbb{F}_q$ est l'ensemble des éléments de $\mathbb{F}_q$ tels que $\sigma_p(x) = x$.

0.5. Polynôme minimal

DÉFINITION 0.5.1. *Le polynôme unitaire dans $\mathbb{F}_q$ de plus petit degré annulé par $\beta \in \mathbb{F}_{q^t}$ s'appelle polynôme minimal de β sur $\mathbb{F}_q$.*

THÉORÈME 0.5.2. *Soit $\mathbb{F}_{q^t}$ une extension du corps $\mathbb{F}_q$ et $\alpha \in \mathbb{F}_{q^t}$ de polynôme minimal $m_\alpha(x)$ dans $\mathbb{F}_q[x]$. Alors :*
i) $m_\alpha(x)$ est irréductible sur $\mathbb{F}_q$;
ii) si $g(x) \in \mathbb{F}_q[x]$ tel que $g(\alpha) = 0$ alors $m_\alpha(x)$ divise $g(x)$;
iii) $m_\alpha(x)$ est unique.

DÉMONSTRATION. i) $m_\alpha(x)$ est irréductible. Sinon, on aurait $m_\alpha(x) = P(x)Q(x)$ dans $\mathbb{F}_p[x]$, où $p(x)$ et $q(x)$ sont de degré > 1 et $< d$. dans $\mathbb{F}_q$, on a $p(\alpha)q(\alpha) = 0$ et donc $p(\alpha) = 0$ ou $q(\alpha) = 0$, ce qui contredit que $m_\alpha(x)$ est le polynôme minimal.
ii) On fait la division euclidienne de $g(x)$ par $m_\alpha(x)$, le reste est nécessairement nul, sinon contradiction avec le fait que $m_\alpha(x)$ est le polynôme minimal.
ii) Si il existe 2 polynômes minimaux de $\alpha(x)$, ils seront nécessairement de même degré, et leur différence est nulle, sinon ils ne seront pas polynômes minimaux. □

THÉORÈME 0.5.3. *Soit $f(x)$ un polynôme irréductible unitaire sur $\mathbb{F}_q$ de degré r. Alors :*
i) toutes les racines de $f(x)$ sont dans $\mathbb{F}_{q^t}$; et dans tout corps contenant $\mathbb{F}_q$ et une racine quelconque de $f(x)$;
ii) $f(x) = \prod_{i=1}^{t}(x - \alpha_i)$, où $\alpha_i \in \mathbb{F}_{q^t}$ pour $1 \leq i \leq t$;
iii) $f(x)$ divise $x^{q^t} - x$.

DÉMONSTRATION. i) Soit α et β deux racines de $f(x)$. le corps $\mathbb{F}_q[x]/(f(x))$ contient ces deux racines. iii) D'après ii) et le fait que $x^{q^t} - x = \prod_{\alpha \in \mathbb{F}_{q^t}}(x - \alpha)$. □

Ce théorème est en particulier valable pour le polynôme minimal $m_\alpha(x)$ dans $\mathbb{F}_q$.

THÉORÈME 0.5.4. *Soit $\mathbb{F}_{q^t}$ une extension du corps $\mathbb{F}_q$ et $\alpha \in \mathbb{F}_{q^t}$ de polynôme minimal $m_\alpha(x)$ dans $\mathbb{F}_q[x]$. Alors :*
i) le degré de $m_\alpha(x)$ divise t ;
ii) $x^{q^t} - x = \prod_\alpha m_\alpha(x)$, où $\alpha \in \mathbb{F}_{q^t}$ dont les $m_\alpha(x)$ sont tous distincts ;
iii) $x^{q^t} - x = \prod_{f(x)} f(x)$, où $f(x)$ sont tous les polynômes irréductibles unitaires sur $\mathbb{F}_q$ dont les degrés divisent t.

DÉMONSTRATION. i) $\mathbb{F}_q[x]/(m_\alpha(x))$ est une extension de $\mathbb{F}_q$ qui contient toutes les racines de $m_\alpha(x)$ et $\mathbb{F}_q[x]/(m_\alpha(x)) = \mathbb{F}_{q^{deg(m_\alpha(x))}}$ qui est un sous corps de $\mathbb{F}_{q^t}$. D'après le Théorème 0.2.10 $deg(m_\alpha(x))$ divise t. □

Deux éléments dans $\mathbb{F}_{q^t}$ ayant même polynôme minimal sont dits conjugués. Les conjugués de α sont donc toutes les racines de son polynôme minimal $m_\alpha(x)$. Le théorème suivant permet de trouver les conjugués de α.

THÉORÈME 0.5.5. *Soit $f(x)$ un polynôme dans $\mathbb{F}_q[x]$ et α une racine de $f(x)$ dans une extension $\mathbb{F}_{q^t}$ de $\mathbb{F}_q$. Alors :*
i) $f(x^q) = f(x)^q$;
ii) α^q est aussi une racine de $f(x)$ dans $\mathbb{F}_q$.

DÉMONSTRATION. Si $f(x) = \sum_{i=1}^{k} a_i x^i$ on utilise le fait que $a_i^q = a_i$ (les éléments de $\mathbb{F}_q$ sont les racines du polynôme $x^q - x$.) et le Lemme 0.1.6. □

Si on prend dans ce théorème $f(x)$ comme étant le polynôme minimal de $\alpha \in \mathbb{F}_q^t$ sur $\mathbb{F}_q$ alors les conjugués de α sont $\{\alpha, \alpha^q, \alpha^{q^2}, \cdots \alpha^{q^{t-1}}\}$.

Le polynôme minimal $m_{\alpha^i}(x)$ de $\alpha^i \in \mathbb{F}_{p^t}$?

$$f(x) = \prod_{k=0}^{t-1}(x - \alpha^{iq^k})$$

est un facteur de $m(x)$ à coefficients dans $\mathbb{F}_q$ (après développement). Donc $f(x) \in \mathbb{F}_q[x]$ et $f(\alpha^i) = 0$. D'où $m(x) = f(x)$.

DÉFINITION 0.5.6. *Le polynôme minimal $m_\alpha(x)$ d'un élément primitif α, s'appelle polynôme primitif.*

Le cardinal r d'une classe q-cyclotomique modulo $q^t - 1$ divise t.

THÉORÈME 0.5.7. *Si γ est un élément primitif $\mathbb{F}_{q^t}$ alors le polynôme minimal γ^s sur $\mathbb{F}_q$ est*

$$m_{\gamma^s(x)} = \prod_{i \in C_s} (x - \gamma^i)$$

xxx

Le polynôme $x^n - 1$ dans $\mathbb{F}_q[x]$ se décompose complètement dans une extension $\mathbb{F}_{q^m}[x]$ de $\mathbb{F}_q[x]$ où n divise $q^m - 1$. Soit ω un élément primitif de $\mathbb{F}_{q^m}$ alors $\alpha = \omega^{(q^m-1)/n}$ est une racine primitive n^{eme} de l'unité dans $\mathbb{F}_q$ et

$$x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i)$$

Il s'en suit que le polynôme générateur $g(x)$ d'un code cyclique C de longueur n se décompose comme $g(x) = \prod_{i \in I}(x - \alpha^i)$ dans $\mathbb{F}_{q^m}[x]$ où I est un sous ensemble de $\{0, 1, 2, \cdots, n-1\}$, appelé ensemble de définition de C relativement à α.

Soit $f(x)$ un polynôme irréductible qui divise $x^n - 1$ et α^i une racine de $f(x)$ dans $\mathbb{F}_{q^m}$. Les conjugués de α : $\alpha^{iq}, \alpha^{iq^2}, \cdots$ sont aussi des racines de $f(x)$ (les exposants sont modulo n puisque $\alpha^n = 1$). $\{iq^j \ mod \ n \mid j = 0, 1, \cdots\}$ est l'orbite C_i q-cyclotomique modulo n.

$$f(x) = \prod_{s \in C_i} (x - \alpha^s)$$

Ce polynôme $f(x)$ s'appelle polynôme minimal de α^i. On le note $m_i(x)$.

Donc le polynôme générateur $g(x)$ d'un code cyclique C est le produit de certains polynômes minimaux.

0.6. Classes cyclotomiques

Les classes cyclotomiques permettent de déterminer le nombre de facteurs irréductibles de $x^{p^m-1} - 1$ sur $\mathbb{F}$. Connaissant le polynôme minimal d'une racine $x^{p^m-1} - 1$ elles permettent de trouver tous les polynômes minimaux des racines de $x^{p^m-1} - 1$, c'est à dire tous les facteurs $x^{p^m-1} - 1$

Rappelons que tous les conjugués de β ont donc le même polynôme minimal.

On considère le corps $\mathbb{F}_{16}$ avec $p = 2$, $m = 4$ et β admettant pour polynôme minimal $\beta^4 + \beta + 1$. Alors

Alors β est un zéro de $x^4 + x + 1$, il en est de même pour β^2, β^4, β^8 et β^{16}, on peut vérifier par le calcul que

$$x^4 + x + 1 = (x - \beta)(x - \beta^2)(x - \beta^4)(x - \beta^8).$$

Trouver l'ensemble des conjugués de toutes les racines revient à partitioner l'ensemble des puissances de β. Le corps F s'écrit $F = \{0\} \cup \{1, \beta, \beta^2, \cdots, \beta^{p^m-2}\}$ et l'ensemble des puissances de β est tout simplement $\mathbb{Z}_{p^m-1}$.

DÉFINITION 0.6.1. *Soit $a, b \in \mathbb{Z}_{p^m-1}$ a et b sont dits équivalents si $b = p^i a \ mod(p^m - 1)$.*

La relation d'équivalence est réflexive, symétrique et transitive. C_s représente une classe cyclotomique où s est le plus petit entier de la classe :

$$\{s, sp, sp^2, \cdots, sp^{m_s-1}\},$$

où m_s est le plus petit entier tel que $p^{m_s} = s(mod\ p^m - 1)$. L'entier s est appelé le représentant de la classe (en anglais coset leader).

Quelles sont les classes cyclotomiques *modulo* 15 pour $p = 2$?

$C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$, $C_3 = \{3, 6, 12, 9\}$, $C_5 = \{5, 10\}$, $C_7 = \{7, 14, 13, 11\}$.

EXERCISE 0.7. *Soit α une racine primitive de $x4 + x + 1$ sur $\mathbb{F}_{16}$. Déterminer les polynômes minimaux de 1, 3, 5, 7.*

0.8. Polynômes Cyclotomiques

Soit s un entier tel que $0 \leq s \leq n$. Par définition l'orbite q-cyclotomique de $s \mod n$ est

$$C_s = \{s, sq, \cdots, sq^{r-1}\} \ (mod n)$$

où r est le plus petit entier positif tel que $sq^r \equiv s \ (\mod n)$. Les ensembles C_s forment une partition de l'ensemble $\{0, 1, 2, \cdots, n-1\}$ Par définition $ord_n(q)$ est le cardinal de l'orbite q-cyclotomique $C_1 \ (\mod n)$.

Le polynôme minimal de α^s sur $\mathbb{F}_q$ est $m_{\alpha^s}(x) = \prod_{i \in C_s}(x - \alpha^i)$.

EXEMPLE 0.8.1. *Dans* $\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3 + x + 1)$. *Conjugacy Class : Associated Minimal Polynomial* $\{0\}$ *:* $p(x) = (x - 0) = x$
$\{\alpha^0 = 1\}$ *:* $p_0(x) = (x - 1) = x + 1$
$\{\alpha, \alpha^2, \alpha^4\}$ *:* $p_1(x) = p_2(x) = p_4(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4) = x^3 + x + 1$
$\{\alpha^3, \alpha^6, \alpha^5\}$ *:* $p_3(x) = p_6(x) = p_5(x) = (x-\alpha^3)(x-\alpha^6)(x-\alpha^5) = x^3+x^2+1$.

Soit α une racine primitive n^e de l'unité dans une clôture algébrique de $\mathbb{F}_q$. La plus petite extension de $\mathbb{F}_q$ qui contienne α est $\mathbb{F}_{q^r}$ où r est le plus petit entier tel que n divise $q^r - 1$.

On définit l'orbite q-cyclotomique de $s \mod (q^t - 1)$ comme

$$C_s = \{s, sq, \cdots, sq^{r-1}\} \mod (q^t - 1)$$

où r est le plus petit entier positif tel que $sq^r \equiv s \mod (q^t-1)$. Les ensembles C_s forment une partition de l'ensemble $\{0, 1, 2, \cdots, q^t - 2\}$

EXEMPLE 0.8.2. *Les orbites 2-cyclotomiques* $\mod 15$ *sont* $C_0 = \{0\}$, $C_1 = \{1, 2, 4, 8\}$, $C_3 = \{3, 6, 12, 9\}$, $C_5 = \{5, 10\}$ *et* $C_7 = \{7, 14, 13, 11\}$.

EXERCISE 0.9. *Trouver les 2-cyclotomiques orbites* $\mod 16$, $\mod 31$

THÉORÈME 0.9.1. *Si* γ *est un élément primitif de* $\mathbb{F}_{q^t}$, *alors le polynôme minimal de* γ^s *sur* $\mathbb{F}_q$ *est*

$$m_{\gamma^s}(x) = \prod_{i \in C_s}(x - \gamma^i)$$

EXEMPLE 0.9.2. *Polynôme minimal de chaque élément de* $\mathbb{F}_8$ *sur* $\mathbb{F}_2$ *ainsi que les 2-cyclotomiques orbites*

racine	*polynôme minimal*	*2-cyclotomiques orbites*
0	x	
1	$x + 1$	$\{0\}$
$\alpha, \alpha^2, \alpha^4$	$x^3 + x + 1$	$\{1, 2, 4\}$
$\alpha^3, \alpha^5, \alpha^6$	$x^3 + x^2 + 1$	$\{3, 5, 6\}$

EXERCISE 0.10. *Trouver le polynôme minimal de chaque élément de* $\mathbb{F}_{16}$ *sur* $\mathbb{F}_2$ *ainsi que les 2-cyclotomiques orbites*

EXERCISE 0.11. *Sans factoriser le polynôme* $x^{63}-1$, *déterminer le nombre de ses facteurs irréductibles ainsi que leurs degrés sur* $\mathbb{F}_2$ *puis sur* $\mathbb{F}_4$

0.12. Polynômes Cyclotomiques

On appelle racine primitive n-ième de l'unité une racine n-ième de l'unité d'ordre exactement n. On notera $\pi_n(\mathbb{F})$ leur ensemble.

Le n-ième polynôme cyclotomique, est le polynôme

$$\varphi_n(X) = \prod_{\alpha \in \pi_n(\mathbb{F})} (X - \alpha) \in C[X].$$

PROPOSITION 0.12.1. *Les polynômes cyclotomiques vérifient les conditions suivantes :*
i) $\varphi_n(X)$ *est un polynôme unitaire de degré* $\phi(n)$,
ii) $X^n - 1 = \prod_{d|n} \varphi_d(X)$,
iii) le polynôme $\varphi_n(X)$ *est à coefficients entiers.*

DÉMONSTRATION. i) On sait que $\pi_n(\mathbb{F})$ est de cardinal $\phi(n)$.
ii) On a $X^n - 1 = \prod_{\alpha \in \pi_n(\mathbb{F})}(X - \alpha)$ or $ord(\alpha)$ divise n $\pi_n(\mathbb{F})$ est la réunion disjointe des $\pi_d(\mathbb{F})$ pour $d|n$.
iii) par récurrence sur n et division euclidienne. □

On peut montrer que $\varphi_n(X)$ est un polynôme irréductible de $\mathbb{Z}[X]$.

DÉFINITION 0.12.2. *Si* A *est un anneau commutatif, l'image de* $\varphi_n(X)$ *par le morphisme d'anneaux naturel* $\mathbb{Z}[X] \longrightarrow A[X]$ *est également appelé* n*-ième polynôme cyclotomique.*

Les premiers polynômes cyclotomiques sont donnés par :

$$\begin{aligned}
\varphi_1(X) &= X - 1, \\
\varphi_2(X) &= X + 1, \\
\varphi_3(X) &= X^2 + X + 1, \\
\varphi_4(X) &= X^2 + 1, \\
\varphi_5(X) &= X^4 + X^3 + X^2 + X + 1, \\
\varphi_6(X) &= X^2 - X + 1 \\
\varphi_8(X) &= X^4 + 1
\end{aligned}$$

et si p est un nombre premier

$$\varphi_p(X) = X^{p-1} + \cdots + X + 1.$$

0.13. Exercices

Le polynôme $t + 1$ est-il primitif dans $\mathbb{F}_9$? Trouvez les autres éléments primitifs.

Construire le corps $\mathbb{F}_8$.

exo : Trouver tous les éléments primitifs des corps $\mathbb{F}_2$, $\mathbb{F}_3$ et $\mathbb{F}_4$.

exo : Prener un élément primitif α de $\mathbb{F}_4$ et écrire la table de multiplication de $\mathbb{F}_4$ en utilisant $\{0, 1 = \alpha^0, \alpha, \alpha^2\}$. Vérifier que tous les éléments de $\mathbb{F}_4$ sont des racines du polynôme $x^q - x$.

exo : Soit C_1 et C_2 deux codes cycliques sur $\mathbb{F}_q$ de polynômes générateurs $g_1(x)$ et $g_2(x)$, respectivement. Montrer que $C_1 \subset C_2$ si seulement si $g_2(x)$ divise $g_1(x)$.

THÉORÈME 0.13.1 (de Wedderburn). *Tout corps fini est commutatif.*

Un corps fini à q éléments de caractéristique p peut toujours s'écrire sous la forme :

$$\mathbb{F}_q = F_p[\alpha] = \mathbb{F}_p[x] mod m_\alpha(x).$$

$p[x]$ polynôme minimal de α

Le polynôme minimal $m_\alpha(x)$ d'un élément $\alpha \in \mathbb{F}_q$ divise $x^q - x$, puisque $\alpha^q = \alpha$. Comme les éléments de C sont exactement les racines de $x^q - x$, $m_\alpha(x)$ se décompose complètement dans $\mathbb{F}_q$.

suite voir 200609crps fini