Introduction à la Cryptologie

Chapitre 11 : Classification et construction des corps finis

Michael Eisermann (Institut Fourier, UJF Grenoble)

Année 2008-2009
IF / IMAG, Master 1, S1-S2

document mis à jour le 7 juillet 2009

www-fourier.ujf-grenoble.fr/~eiserm/cours#crypto

Objectifs de ce chapitre

Les corps finis sont une des plus belles structures algébriques.
Ils sont à la base de nombreuses applications algorithmiques,
notamment en cryptographie et en codage de l'information.

Nous connaissons déjà le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ où p est un nombre premier.
Ce chapitre établit d'abord la ***classification*** de tous les corps finis :

1. Tout corps fini est de cardinal p^n où p est premier et $n \geq 1$.
2. Pour tout tel couple (p, n) il existe un corps de cardinal p^n.
3. Deux corps finis de même cardinal sont isomorphes.

Ce superbe résultat, dû à Galois, est un bijou de l'algèbre du 19e siècle.
Pour le rendre effectif sur ordinateur, il faut néanmoins être plus explicite.
Le développement choisi ici explicitera comment ***construire*** concrètement
un corps de cardinal p^n donné puis comment ***l'implémenter*** sur ordinateur.

Littérature pour aller plus loin :

📖 Lidl & Niederreiter, *Finite Fields*, Cambridge 1997.
📖 Gathen & Gerhard, *Modern Computer Algebra*, Cambridge 1999.

Sommaire

Outils indispensables

Ce chapitre est le couronnement de notre bref développement algébrique. Il utilise d'une manière essentielle toutes les techniques (mathématiques et algorithmiques) mises en place par les chapitres précédents :

- Groupes (abéliens) finis, morphismes, quotients
- Sous-groupes, théorème de Lagrange, ordre d'un élément
- Anneaux, morphismes, idéaux, quotients, théorème d'isomorphisme
- Caractéristique d'un anneau, le morphisme de Frobenius
- L'arithmétique des polynômes, notamment la division euclidienne
- Divisibilité des polynômes, calcul du pgcd, factorialité de $\mathbb{K}[X]$
- Nombre et multiplicité des racines, critère de multiplicité
- Sous-groupes multiplicatifs finis de $\mathbb{K}^\times$

En outre, on aura besoin d'un concept basique omniprésent :

- La théorie des espaces vectoriels sur un corps $\mathbb{K}$ quelconque (ici $\mathbb{F}_p$)

Le groupe $F^\times$ est cyclique

Théorème (rappel)

Soit A un anneau intègre et soit $G \subset A^\times$ un sous-groupe fini du groupe $A^\times$.
Alors G est cyclique, c'est-à-dire qu'il existe $g \in G$ tel que $G = \langle g \rangle$. □

Corollaire (rappel)

Pour tout corps fini F le groupe multiplicatif $F^\times$ est cyclique.
*Tout générateur du groupe $F^\times$ est appelé **racine primitive** de F.* □

Exemple (rappel)

Comme $\mathbb{Z}/7$ est un corps, le groupe $\mathbb{Z}/7^\times$ est cyclique d'ordre 6. (Le théorème ne garantit que l'existence d'un générateur, sans en expliciter aucun.)
Par tâtonnement on trouve $\mathrm{ord}(\bar{2}) = 3$ puis $\mathrm{ord}(\bar{3}) = 6$, donc $\mathbb{Z}/7^\times = \langle \bar{3} \rangle$.

Remarque (rappel)

Pour tout corps $\mathbb{F}_q$ de cardinal q, le groupe $\mathbb{F}_q^\times$ est cyclique d'ordre $n = q - 1$.
Toute racine primitive ξ de $\mathbb{F}_q$ définit alors un isomorphisme de groupes $\exp_\xi : (\mathbb{Z}/n, +) \xrightarrow{\sim} (\mathbb{F}_q^\times, \cdot)$, $k \mapsto \xi^k$, et son inverse $\log_\xi : (\mathbb{F}_q^\times, \cdot) \xrightarrow{\sim} (\mathbb{Z}/n, +)$.
C'est une situation typique de la cryptographie (Diffie–Hellman, Elgamal).

Sous-corps premier et cardinal d'un corps fini

Proposition

Soit F un corps fini. Le morphisme canonique $\varphi\colon \mathbb{Z} \to F$, $k \mapsto k \cdot 1_F$ a pour image un sous-anneau $K := \operatorname{im}\varphi$. Celui-ci est intègre car $F \supset K$ est intègre.

Le noyau $\ker\varphi$ est un idéal de $\mathbb{Z}$, donc de la forme (p) pour un $p \in \mathbb{N}$. Comme F est fini, φ ne peut être injectif, donc $p > 0$. Par passage au quotient on obtient un isomorphisme $\bar{\varphi}\colon \mathbb{Z}/p \xrightarrow{\sim} K$. Mais $\mathbb{Z}/p$ est intègre si et seulement si p est premier. Ainsi $K \cong \mathbb{Z}/p$ est même un corps. □

On appelle K le ***sous-corps premier***, et p la ***caractéristique*** du corps F. Via $\bar{\varphi}$ on identifie $\mathbb{F}_p = \mathbb{Z}/p$ à K, et on écrit simplement $\mathbb{F}_p \subset F$.

Proposition (rappel)

Soit K un sous-corps d'un anneau F. Alors l'addition $+\colon F \times F \to F$ et la multiplication $\cdot\colon K \times F \to F$ font de F un K-espace vectoriel. □

Corollaire

Si F est un corps fini, alors son cardinal est p^d où p est premier et $d \geq 1$. □

Ici $p = \operatorname{car}(F)$ est le cardinal du sous-corps premier K, et $d = \dim_K(F)$. Toute base $(u_1, \ldots, u_d)$ de F définit un isomorphisme $K^d \xrightarrow{\sim} F$ d'espaces vectoriels sur K par $(k_1, \ldots, k_d) \mapsto k_1u_1 + \cdots + k_du_d$, d'où $|F| = |K^d| = p^d$.

Premier exemple : un corps de cardinal 4

Le polynôme $X^2 + X + 1$ de degré 2 est irréductible sur $\mathbb{F}_2$, car sans racine.
(Nous avons vu que c'est le seul polynôme irréductible de degré 2 sur $\mathbb{F}_2$.)
Le quotient $\mathbb{F}_4 := \mathbb{F}_2[X]/(X^2 + X + 1)$ est donc un corps de cardinal 4.

Comme $\mathbb{F}_2$-base on peut choisir $(1, x)$ où $x = \bar{X}$ est l'image de X dans $\mathbb{F}_4$.
Les tables d'addition et de multiplication sont (en abrégeant $1 + x$ par y) :

$+$	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

$\cdot$	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	1
y	0	y	1	x

On voit que $x^2 = x + 1$, et ainsi la multiplication peut être reformulée comme

$$(\alpha + \beta x)(\alpha' + \beta' x) = (\alpha\alpha' + \beta\beta') + (\alpha\beta' + \beta\alpha' + \beta\beta')x.$$

Ceci permet d'implémenter $\mathbb{F}_4$ comme $\mathbb{F}_2^2$ avec les opérations ci-dessus.

Par contre, il n'est pas évident de partir d'une telle formule « tombée du ciel » pour établir qu'il s'agit d'un corps. On préférera la construction $\mathbb{F}_p[X]/(P)$.

Exercice

De manière analogue, expliciter des corps de cardinal 8, 9, 25, 27.

Le polynôme minimal d'un élément algébrique

Exercice

Soit K un corps et $I \subsetneq K[X]$ un idéal. Si $P \in I$ est irréductible, alors $I = (P)$.

Solution. Nous savons que $I = (Q)$ pour un $Q \in K[X]$.
Ainsi $P \in (Q)$ veut dire que $Q \mid P$, d'où $Q \sim 1$ ou $Q \sim P$.
Le premier cas $I = (1)$ étant exclu, nous concluons que $I = (P)$. ☺

Exercice

Soit K un corps et soit a un élément d'un anneau A contenant K.

1. On a $\dim_K(K[a]) < \infty$ si et seulement s'il existe $P \in K[X]^*$ tel que $P(a) = 0$. Dans ce cas on dit que l'élément a est ***algébrique*** sur K. On peut alors choisir P de degré minimal et unitaire, appelé ***polynôme minimal*** de a. Si A est intègre, le polynôme minimal est irréductible.
2. Si a est annulé par un polynôme irréductible $P \in K[X]^*$, $P(a) = 0$, alors le morphisme d'anneaux $\phi\colon K[X] \to A$ défini par $\phi(X) = a$ induit un isomorphisme de corps $\bar{\phi}\colon K[X]/(P) \xrightarrow{\sim} K[a]$.

Solution. Les éléments $1, a, a^2, \ldots, a^n$ dans A sont linéairement liés sur K, c'est-à-dire $c_0 1 + c_1 a + c_2 a^2 + \cdots + c_n a^n = 0$, si et seulement si le polynôme $P(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_n X^n$ s'annule en a. Les conséquences énoncées découlent de l'arithmétique des polynômes sur K (à détailler). ☺

Illustration : corps de cardinal 125

Comme un exemple un peu plus complexe et plus intéressant, on se propose d'analyser puis de comparer deux quotients de $\mathbb{F}_5[X]$ de cardinal 125 :

$$P = X^3 + X + 1, \qquad E = \mathbb{F}_5[X]/(P),$$
$$Q = Y^3 + 2Y^2 - Y + 2, \qquad F = \mathbb{F}_5[Y]/(Q).$$

Exercice

1. Quel est le cardinal de E et de F ? Ces anneaux sont-ils des corps ?
2. Notons x l'image de X dans E. Expliciter les lois d'addition et de multiplication par rapport à la $\mathbb{F}_5$-base $(1, x, x^2)$:
   - Comment additionner $a = a_0 + a_1x + a_2x^2$ et $b = b_0 + b_1x + b_2x^2$ pour obtenir un résultat de la forme $c = c_0 + c_1x + c_2x^2$?
   - Comment multiplier $a = a_0 + a_1x + a_2x^2$ et $b = b_0 + b_1x + b_2x^2$ pour obtenir un résultat de la forme $c = c_0 + c_1x + c_2x^2$?
3. Pour $y = x^2 - x$ calculer $Q(y)$ dans E.
4. En déduire le noyau du morphisme $\phi\colon \mathbb{F}_5[Y] \to E$, $Y \mapsto y$.
5. Construire un isomorphisme $\mathbb{F}_5[Y]/(Q) \xrightarrow{\sim} \mathbb{F}_5[X]/(P)$.

L'automorphisme de Frobenius d'un corps fini

Proposition

Soit F un corps fini de caractéristique p. Alors l'application $\mathfrak{f}\colon F \to F$ définie par $x \mapsto x^p$ est un automorphisme du corps F.
On appelle $\mathfrak{f}$ ***l'automorphisme de Frobenius*** *de F.*

Démonstration. Tout d'abord, l'application $\mathfrak{f}\colon x \mapsto x^p$ est multiplicative : elle satisfait $\mathfrak{f}(1) = 1$ et $\mathfrak{f}(xy) = (xy)^p = x^p y^p = \mathfrak{f}(x) \cdot \mathfrak{f}(y)$.
Puis $\mathfrak{f}$ est aussi additive, d'après le développement binomial :

$$\mathfrak{f}(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k}$$

Dans $\mathbb{Z}$ nous avons vu que p divise $\binom{p}{k}$ si $0 < k < p$. Comme F est de caractéristique p, tous ces termes sont nuls dans F, et on obtient

$$\mathfrak{f}(x+y) = (x+y)^p = x^p + y^p = \mathfrak{f}(x) + \mathfrak{f}(y).$$

Ceci prouve que $\mathfrak{f}\colon F \to F$ est un morphisme d'anneaux.
Or, F est un corps et tout morphisme de corps est injectif.
Comme le cardinal de F est fini, $\mathfrak{f}$ est une bijection. □

Exemple

Dans $\mathbb{F}_4 = \{0, 1, x, y\}$ l'automorphisme $\mathfrak{f}$ fixe 0 et 1 mais échange x et y.

Le groupe d'automorphismes d'un corps fini

Proposition

Soit F un corps de cardinal p^n.

- *Le groupe $\mathrm{Aut}(F)$ des automorphismes de F est cyclique d'ordre n, engendré par l'automorphisme de Frobenius $\mathfrak{f}\colon F \to F$, $x \mapsto x^p$.*
- *Ainsi $\mathrm{Aut}(F) = \langle \mathfrak{f} \rangle \cong \mathbb{Z}/n$ et pour tout $d \mid n$ il existe un unique sous-groupe $H \subset \mathrm{Aut}(F)$ d'indice d, à savoir $H = \langle \mathfrak{f}^d \rangle$.*

Démonstration. On a $\mathfrak{f}^k(x) = ((x^p)^p)\cdots)^p = x^{p^k}$ pour tout $x \in F$.
Si $\mathfrak{f}^k = \mathrm{id}_F$ pour $0 < k < n$, alors $X^{p^k} - X$ aurait p^n racines dans F.
Finalement on a $\mathfrak{f}^n = \mathrm{id}_F$ car $x^{p^n} = x$ pour tout $x \in F$.

Choisissons $a \in \mathbb{F}$ tel que $F = \mathbb{F}_p[a]$, par exemple une racine primitive de F.
Soit $P \in \mathbb{F}_p[X]$ son polynôme minimal ; ainsi $\mathbb{F}_p[X]/(P) \cong F$ et $\deg(P) = n$.
Les automorphismes $\mathrm{id}_F = \mathfrak{f}^0, \mathfrak{f}^1, \ldots, \mathfrak{f}^{n-1}$ permutent les racines de P,
car $P(x) = 0$ entraîne $P(\mathfrak{f}^k(x)) = \mathfrak{f}^k(P(x)) = \mathfrak{f}^k(0) = 0$.
Si $\mathfrak{f}^k$ fixe a, alors $\mathfrak{f}^k$ fixe $\mathbb{F}_p[a] = F$, donc $\mathfrak{f}^k = \mathrm{id}_F$ et $k \in n\mathbb{Z}$.
Ceci fait que $a, \mathfrak{f}^1(a), \ldots, \mathfrak{f}^{n-1}(a)$ sont les n racines distinctes de P.

Tout automorphisme $g \in \mathrm{Aut}(F)$ permute les n racines de P.
Il existe donc un $k \in \{0, 1, \ldots, n-1\}$ tel que $g(a) = \mathfrak{f}^k(a)$.
Ainsi $\mathfrak{f}^k g^{-1}$ fixe a et donc $F = \mathbb{F}_p[a]$. Ceci veut dire que $g = \mathfrak{f}^k$. □

Sous-corps fixé par des automorphismes

Lemme

Soit F un corps et soit $h\colon F \to F$ un automorphisme.
Alors $K = \{x \in F \mid h(x) = x\}$ est un sous-corps de F.

Démonstration. On a $0 \in K$, et $a, b \in K$ implique $a + b \in K$, car

$$h(a + b) = h(a) + h(b) = a + b.$$

On a $h(-a) = -h(a) = -a$, donc l'opposé de $a \in K$ aussi est dans K.

On a $1 \in K$, et $a, b \in K$ implique $a \cdot b \in K$, car

$$h(a \cdot b) = h(a) \cdot h(b) = a \cdot b.$$

Pour $a \in K^*$ on a $h(a^{-1}) = h(a)^{-1} = a^{-1}$, donc a^{-1} aussi est dans K. □

Corollaire

Soit F un corps et soit $H \subset \mathrm{Aut}(F)$ un groupe d'automorphismes.
Alors $F^H = \{x \in F \mid h(x) = x$ pour tout $h \in H\}$ est un sous-corps de F. □

Exemple

Pour tout corps fini F nous avons $F^{\langle \mathrm{f} \rangle} = \{x \in F \mid x^p = x\} = \mathbb{F}_p$.

Polynômes remarquables sur un corps fini

Lemme

Soit F un corps fini de cardinal q. Alors $X^q - X = \prod_{a \in F}(X - a)$.

Démonstration. D'après le théorème de Lagrange, tout $a \in F^\times$ vérifie $a^{q-1} = 1$, donc $a^q = a$. Cette dernière égalité est aussi vérifiée pour $a = 0$. On trouve ainsi q racines distinctes du polynôme $X^q - X$, qui est de degré q, ce qui équivaut à la factorisation complète énoncée. □

Lemme

Dans l'anneau euclidien $\mathbb{F}_p[X]$ des polynômes sur $\mathbb{F}_p$ nous avons

$$\operatorname{pgcd}(\, X^{p^m} - X,\, X^{p^n} - X \,) = X^{p^d} - X \quad \textit{où} \quad d = \operatorname{pgcd}(m, n).$$

En particulier, $X^{p^m} - X$ divise $X^{p^n} - X$ si et seulement si m divise n.

Démonstration. Supposons que $m = sn + r$ où $0 \leq r < n$. Alors

$$X^{p^m} = X^{p^{sn+r}} = (((X^{p^n})^{p^n} \cdots)^{p^n})^{p^r} \equiv X^{p^r} \quad \text{modulo} \quad X^{p^n} - X.$$

Ainsi le calcul revient à calculer $\operatorname{pgcd}(m, n)$ dans les exposants. □

Sous-corps d'un corps fini

Proposition

Soit F un corps fini de cardinal p^n.

- *Si K est un sous-corps de F, alors $|K| = p^d$ où $d \mid n$.*
- *Pour tout $d \mid n$ il existe un unique sous-corps $K \subset F$ de cardinal p^d.*

Démonstration. Le corps F contient le sous-corps premier est $\mathbb{F}_p$.
D'une part tout sous-corps K contient $\mathbb{F}_p$, donc $|K| = p^d$ avec $d = \dim_{\mathbb{F}_p} K$.
D'autre part F est un K-espace vectoriel, donc $|F| = |K|^m$ où $m = \dim_K F$.
On conclut que $p^n = p^{dm}$, donc $d \mid n$ comme souhaité.

Réciproquement, pour tout diviseur $d \mid n$, nous avons un sous-corps

$$K = \{a \in F \mid a^{p^d} = a\} = F^{\langle \mathfrak{f}^d \rangle}.$$

Comme le polynôme $X^{p^d} - X$ divise $X^{p^n} - X = \prod_{a \in F}(X - a)$,
on obtient $X^{p^d} - X = \prod_{a \in K}(X - a)$. Ceci prouve que $|K| = p^d$.

Finalement, si L est un sous-corps de cardinal p^d, alors tous ses éléments sont racines de $X^{p^d} - X$, ce qui implique $L = K$, d'où l'unicité énoncée. □

Correspondance de Galois pour un corps fini

Théorème

Pour tout corps fini F nous avons une correspondance naturelle entre les sous-corps de F et les sous-groupes de $\mathrm{Aut}(F)$:

À tout sous-corps $K \subset F$ on associe le sous-groupe

$$\mathrm{Gal}(F|K) := \{h \in \mathrm{Aut}(F) \mid h(x) = x \text{ pour tout } x \in K\}.$$

À tout sous-groupe $H \subset \mathrm{Aut}(F)$ on associe le sous-corps

$$F^H := \{x \in F \mid h(x) = x \text{ pour tout } h \in H\}.$$

Ce sont des bijections mutuellement inverses :
Pour tout sous-corps $K \subset F$ nous avons $F^{\mathrm{Gal}(F|K)} = K$.
Pour tout sous-groupe $H \subset \mathrm{Aut}(F)$ nous avons $\mathrm{Gal}(F|F^H) = H$.

Explicitement, si K est de cardinal p^d, alors $\mathrm{Gal}(F|K) = \langle \mathfrak{f}^d \rangle$.
Si $H \subset \mathrm{Aut}(F)$ est d'indice d, alors F^H est le sous-corps de cardinal p^d.

Soit $K \subset F$ un sous-corps. Tout automorphisme $h\colon F \to F$ se restreint à un automorphisme de K car $h(K) = K$. On obtient ainsi un épimorphisme de groupes $\mathrm{Aut}(F) \to \mathrm{Aut}(K)$, $h \mapsto h|_K$, qui a pour noyau le groupe $\mathrm{Gal}(F|K)$.

Démonstration de la correspondance de Galois

Soit F un corps fini. Il est de cardinal p^n où p est premier et $n \geq 1$.
Le groupe $\mathrm{Aut}(F)$ est cyclique d'ordre n engendré par $\mathfrak{f}\colon F \to F$, $x \mapsto x^p$.
Tout sous-corps $K \subset F$ est de cardinal $|K| = p^d$ où $d \mid n$ et ainsi

$$K = \{x \in F \mid x^{p^d} = x\} = F^{\langle \mathfrak{f}^d \rangle}.$$

Montrons que $\mathrm{Gal}(F|K) = \langle \mathfrak{f}^d \rangle$, l'inclusion $\mathrm{Gal}(F|K) \supset \langle \mathfrak{f}^d \rangle$ étant claire.
Nous savons que le sous-groupe $\mathrm{Gal}(F|K)$ est de la forme $\langle \mathfrak{f}^e \rangle$ où $e \mid n$.
Comme $\langle \mathfrak{f}^e \rangle \supset \langle \mathfrak{f}^d \rangle$ nous avons alors $e \mid d$. Observons ensuite que

$$K \subset F^{\mathrm{Gal}(F|K)} = \{x \in F \mid x^{p^e} = x\}.$$

Puisque $|K| = p^d$, ceci exclut $e < d$. On a donc $e = d$ et $\mathrm{Gal}(F|K) = \langle \mathfrak{f}^d \rangle$.
Ceci prouve que $F^{\mathrm{Gal}(F|K)} = K$ ainsi que $\mathrm{Gal}(F|F^H) = H$.

L'unicité du sous-corps K de cardinal p^d dans F assure que $h(K) = K$ pour tout automorphisme $h \in \mathrm{Aut}(F)$.
Ainsi nous obtenons une morphisme $\mathrm{Aut}(F) \to \mathrm{Aut}(K)$ par restriction.
Il est surjectif car $\mathrm{Aut}(K)$, comme $\mathrm{Aut}(F)$, est engendré par $\mathfrak{f}$.
Le noyau est le sous-groupe $\mathrm{Gal}(F|K)$ par définition.

Polynômes irréductibles sur $\mathbb{F}_p$

Lemme

Si $P \in \mathbb{F}_p[X]$ est un polynôme irréductible de degré n,
alors P divise $X^{p^n} - X$ mais ne divise pas $X^{p^d} - X$ pour $d < n$

Démonstration. Si $P \in \mathbb{F}_p[X]$ est irréductible de degré n, alors le quotient $F = \mathbb{F}_p[X]/(P)$ est un corps de cardinal $q = p^n$. L'élément $x = \bar{X} \in F$ est une racine commune de P et de $X^q - X$, donc de $P_1 = \operatorname{pgcd}(P, X^q - X)$. Ceci implique en particulier que $\deg P_1 \geq 1$. Or, P est irréductible, donc $P_1 \mid P$ implique $P_1 \sim P$. Par conséquent $P \mid X^q - X$.

Supposons par l'absurde que P divise $X^{p^d} - X$ pour un $d < n$. Alors P divise aussi $\operatorname{pgcd}(X^{p^n} - X, X^{p^d} - X)$, nous pouvons donc supposer $d \mid n$. Dans ce cas $x = \bar{X}$ serait contenu dans le sous-corps strict $K = \{a \in F \mid a^{p^d} = a\}$ de cardinal $p^d < p^n$. Mais les puissances $1, x, \ldots, x^{n-1}$ forment une base de F, donc le plus petit sous-corps contenant x est F. □

Critère d'irréductibilité dans $\mathbb{F}_p[X]$

Proposition

Un polynôme $P \in \mathbb{F}_p[X]$ de degré n est irréductible si et seulement si P divise $X^{p^n} - X$ et $\operatorname{pgcd}(P, X^{p^{n/t}} - X) = 1$ pour tout diviseur premier t de n.

Démonstration. Si P est irréductible de degré n alors P divise $X^{p^n} - X$ mais aucun des polynômes $X^{p^{n/t}} - X$, donc $\operatorname{pgcd}(P, X^{p^{n/t}} - X) = 1$.
Réciproquement supposons que P divise $X^{p^n} - X$, et que $\operatorname{pgcd}(P, X^{p^{n/t}} - X) = 1$ pour tout diviseur premier t de n. Soit Q un diviseur irréductible de P, de degré m. On sait que Q divise $X^{p^m} - X$ où $m \mid n$. Si $m < n$ alors Q diviserait un $\operatorname{pgcd}(P, X^{p^{n/t}} - X)$, ce qui est exclus.
Par conséquent $m = n$, et ainsi $P \sim Q$. □

⚠ Souvent le degré $n = \deg(P)$ est raisonnablement petit, mais le degré p^n de $X^{p^n} - X$ est déraisonnablement grand !

🔷 L'algorithme suivant réduit tous les calculs au degré $< n$.

Algorithme pour tester l'irréductibilité dans $\mathbb{F}_p[X]$

Algorithme 11.1 Tester l'irréductibilité de $P \in \mathbb{F}_p[X]$

Entrée: un polynôme $P \in \mathbb{F}_p[X]$ de degré n ainsi que la décomposition $n = n_1^{e_1} \cdots n_k^{e_k}$ en facteurs premiers.

Sortie: « irréductible » si P est irréductible, « composé » sinon.

$Q \leftarrow X^{p^n} \operatorname{rem} P$ // puissance dichotomique modulaire
si $Q \neq X$ **alors retourner** « composé » // car $P \nmid X^{p^n} - X$
pour i **de** 1 **à** k **faire**
  $m \leftarrow n/n_i$
  $Q \leftarrow X^{p^m} \operatorname{rem} P$ // puissance dichotomique modulaire
  $R \leftarrow \operatorname{pgcd}(P, Q - X)$ // algorithme d'Euclide
  si $R \neq 1$ **alors retourner** « composé » // car $\operatorname{pgcd}(P, X^{p^m} - X) \neq 1$
fin pour
retourner « irréductible » // d'après la proposition précédente

Exercice

Prouver que l'algorithme ci-dessus est correct. Estimer sa complexité.

Corps finis et polynômes irréductibles

Proposition

Soit F un corps fini de cardinal p^n. Alors il existe un polynôme $P \in \mathbb{F}_p[X]$ unitaire irréductible de degré n tel que $F \cong \mathbb{F}_p[X]/(P)$.

Démonstration. Nous avons $\mathbb{F}_p \subset F$ comme sous-corps premier.
Il existe $x \in F$ tel que $\mathbb{F}_p[x] = F$, par exemple une racine primitive de F.
Le morphisme d'anneaux $\varphi\colon \mathbb{F}_p[X] \to F$, $X \mapsto x$, est donc surjectif.
Son noyau est de la forme $\ker \varphi = (P)$ où $P \in \mathbb{F}_p[X]^*$ est unitaire.
Ainsi φ induit un isomorphisme $\bar{\varphi}\colon \mathbb{F}_p[X]/(P) \xrightarrow{\sim} F$.
En particulier P doit être irréductible de degré n. □

Corollaire

Il existe un corps de cardinal p^d si et seulement s'il existe un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré d. □

On montrera plus bas qu'il existe des polynômes irréductibles $P \in \mathbb{F}_p[X]$ de tout degré d. On les comptera même assez explicitement.

Unicité du corps de cardinal p^n

A priori deux polynômes différents $P, Q \in \mathbb{F}_p[X]$, supposés irréductibles de degré n, mènent à deux corps différents $\mathbb{F}_p[X]/(P)$ et $\mathbb{F}_p[X]/(Q)$.
Or, le résultat est toujours le même à isomorphisme près :

Proposition

Soit F un corps de cardinal p^n. Alors pour tout polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré n l'anneau quotient $\mathbb{F}_p[X]/(P)$ est isomorphe à F.

Démonstration. Nous avons la décomposition $X^{p^n} - X = \prod_{a \in F}(X - a)$.
Le polynôme P divise $X^{p^n} - X$, donc il existe $x \in F$ tel que $P(x) = 0$.
Le morphisme $\varphi\colon \mathbb{F}_p[X] \to F$, $X \mapsto x$, a pour noyau l'idéal (P), puisque P est irréductible. Par passage au quotient on obtient un morphisme injectif $\bar{\varphi}\colon \mathbb{F}_p[X]/(P) \hookrightarrow F$. Comme $\mathbb{F}_p[X]/(P)$ et F ont même cardinal, il s'agit bien d'une bijection. On obtient ainsi l'isomorphisme $\bar{\varphi}\colon \mathbb{F}_p[X]/(P) \xrightarrow{\sim} F$. □

Unicité du corps de cardinal p^n

Corollaire

Deux corps finis de même cardinal sont isomorphes.

Démonstration. Si E et F sont deux corps finis de cardinal p^n,
alors il existe un polynôme unitaire irréductible $P \in \mathbb{F}_p[X]$ de degré n.
Ainsi $\bar{\varphi}\colon \mathbb{F}_p[X]/(P) \xrightarrow{\sim} F$ et $\bar{\psi}\colon \mathbb{F}_p[X]/(P) \xrightarrow{\sim} E$, puis $\bar{\varphi}\bar{\psi}^{-1}\colon E \xrightarrow{\sim} F$. □

Remarque

Il n'y a pas d'identification canonique entre les éléments de E et F !

Étant deux corps E et F de cardinal p^n il existe un isomorphisme $E \xrightarrow{\sim} F$.
Ceci entraîne qu'il existe exactement n isomorphismes entre E et F,
car le groupe d'automorphismes est de cardinal $|\operatorname{Aut}(E)| = n$.

Le seul cas où tout est canonique est $n = 1$, c'est-à-dire que $E = F = \mathbb{Z}/p$.

Notation

Il est souvent commode de noter par $\mathbb{F}_q$ ***un*** corps de cardinal q.
Par un léger abus de langage on appelle $\mathbb{F}_q$ ***le*** corps de cardinal q.

Décomposition de $X^{p^n} - X$ dans $\mathbb{F}_p[X]$

Lemme

Le polynôme $Q = X^{p^n} - X$ dans $\mathbb{F}_p[X]$ n'a pas de facteurs multiples.
Autrement dit : si $Q = U^2V$ où $U, V \in \mathbb{F}_p[X]$, alors $\deg U = 0$.

Démonstration. D'un coté la dérivée de Q dans $\mathbb{F}_p[X]$ est

$$Q' = p^n X^{p^n - 1} - 1 = -1.$$

De l'autre coté, la dérivé de U^2V est

$$2UU'V + U^2V' = U(2U'V + UV').$$

Donc U est inversible, c'est-à-dire $\deg U = 0$. □

Remarque

Si nous savions déjà qu'il existait un corps F de cardinal p^n, alors la décomposition $Q = \prod_{a \in F}(X - a)$ montrerait l'absence de facteurs multiples.
Or, nous sommes en train de prouver justement cette existence.
La démonstration ci-dessus évite tout raisonnement circulaire.

Décomposition de $X^{p^n} - X$ dans $\mathbb{F}_p[X]$

Théorème

Soit $I_p^d \subset \mathbb{F}_p[X]$ l'ensemble des polynômes unitaires irréductibles de degré d. Alors dans $\mathbb{F}_p[X]$ on a la décomposition $X^{p^n} - X = \prod_{d|n} \prod_{P \in I_p^d} P$.

Démonstration. Pour $d \mid n$ tout $P \in I_p^d$ divise $X^{p^d} - X$ et donc $X^{p^n} - X$.
Ainsi leur ppcm $M := \mathrm{ppcm}\{P \mid P \in I_p^d, d \mid n\}$ divise Q.
Comme ces polynômes sont deux-à-deux premiers entre eux,
on trouve que $M = \prod_{d|n} \prod_{P \in I_p^d} P$ divise Q, donc $Q = MQ_1$.

Si $\deg Q_1 \geq 1$, il existerait un facteur unitaire irréductible P_1 de degré $m \geq 1$.
Puisque P_1 divise $X^{p^m} - X$ et $Q = X^{p^n} - X$, il divise aussi leur pgcd
$X^{p^d} - X$ où $d = \mathrm{pgcd}(m, n)$. Or, $d < m$ n'est pas possible, d'où $d = m$.
Donc $d = \deg P_1$ divise n, et P_1 est un des polynômes qui apparaissent déjà dans le produit M. Ainsi Q aurait un facteur multiple, ce qui est impossible.

Ainsi $\deg Q_1 = 0$ puis $\mathrm{dom}(Q) = \mathrm{dom}(M)Q_1$ montre que $Q_1 = 1$. □

Comptage des polynômes irréductibles

Proposition

La décomposition $X^{p^n} - X = \prod_{d|n} \prod_{P \in I_p^d} P$ *entraîne l'égalité*
$p^n = \sum_{d|n} d \cdot |I_p^d|$ *puis l'encadrement* $\frac{1}{n}\left(p^n - 2p^{n/2}\right) \leq |I_p^n| \leq \frac{1}{n} p^n$.

Démonstration. La majoration $n|I_p^n| \leq p^n$ est évidente. Ensuite on trouve

$$\sum_{d|n, d<n} d \cdot |I_p^d| \leq \sum_{1 \leq d \leq n/2} d \cdot |I_p^d| \leq \sum_{1 \leq d \leq n/2} p^d < \frac{p^{n/2+1} - 1}{p - 1} \leq 2p^{n/2}.$$

Ceci prouve la minoration $n|I_p^n| = p^n - \sum_{d|n, d<n} d \cdot |I_p^d| \geq p^n - 2p^{n/2}$. □

Corollaire

Pour tout nombre premier p *et tout* $n \geq 1$ *l'ensemble* I_p^n *est non vide.*
Il existe donc un polynôme irréductible $P \in \mathbb{F}_p[X]$ *de degré* n*,*
et par conséquent un corps $F := \mathbb{F}_p[X]/(P)$ *de cardinal* p^n*.*

Démonstration. L'affirmation est évidente pour $n = 1$.
Pour $n \geq 2$ il suffit de constater que $p^n > 2p^{n/2}$, donc $|I_p^n| > 0$.
Il y a une exception pour $p = 2$ et $n = 2$, où $p^n = 2p^{n/2}$,
mais dans ce cas nous avons déjà vu que $I_2^2 = \{X^2 + X + 1\}$. □

Comparaison avec le théorème des nombres premiers

Le comptage des polynômes irréductibles dans $\mathbb{F}_p[X]$
nous rappelle du comptage des nombres premiers dans $\mathbb{N}$.
Pour $N \in \mathbb{N}$ on note $\pi(N)$ le nombre des entiers premiers dans $\{1, \ldots, N\}$.

Théorème (Hadamard et de la Vallée Poussin 1896)

On a l'équivalence asymptotique $\pi(N) \sim N/\ln N$. □

Ceci veut dire que le quotient $\frac{\pi(N)}{N/\ln N}$ converge vers 1 pour $N \to \infty$.
Nous disposons des encadrements assez précis. On en déduit que dans l'intervalle $\{a \in \mathbb{N} \mid p^{n-1} \leq a < p^n\}$ une fraction $\sim \frac{1}{n \ln p}$ sont premiers.

Observation

Dans $\mathbb{F}_p[X]$ il existe exactement p^n polynômes unitaires de degré n.
Une fraction $\sim \frac{1}{n}$ parmi ces polynômes sont irréductibles.

Ceci veut dire que le comportement asymptotique est très similaire.
Dans les deux cas nous disposons des encadrements assez précis pour assurer une bonne probabilité de réussite des algorithmes probabilistes.

Trouver un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré n

Algorithme 11.2 Trouver un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré n

Entrée: un nombre premier $p \geq 2$ et un nombre naturel $n \geq 1$.
Sortie: un polynôme irréductible unitaire $P \in \mathbb{F}_p[X]$ de degré n

$P \leftarrow$ polynôme unitaire aléatoire de degré n dans $\mathbb{F}_p[X]$
pour m **de** 1 **à** $\lfloor \frac{n}{2} \rfloor$ **faire**
  $Q \leftarrow X^{p^m} \operatorname{rem} P$ // puissance dichotomique modulaire
  $R \leftarrow \operatorname{pgcd}(P, Q - X)$ // algorithme d'Euclide
  si $R \neq 1$ **alors** recommencer avec un nouveau choix de P
fin pour
retourner P

Exercice

Montrer que l'algorithme 11.2 est correct. Estimer sa complexité.
(Attention, il ne s'agit pas d'une simple reformulation de l'algorithme 11.1.)

Solution. Si P est composé, alors $P = P_1 P_2$ où $\deg P_1, \deg P_2 \geq 1$.
Puisque $n = \deg P_1 + \deg P_2$ on a $\deg P_1 \leq \lfloor n/2 \rfloor$ ou $\deg P_2 \leq \lfloor n/2 \rfloor$.
On peut supposer $\deg P_1 \leq \lfloor n/2 \rfloor$, et en itérant que P_1 est irréductible.
Ainsi le polynôme P_1 divise $X^{p^d} - X$ pour $d = \deg P_1 \leq \lfloor n/2 \rfloor$.
Par conséquent P_1 divise $R = \operatorname{pgcd}(P, X^{p^d} - X)$, d'où $\deg R \geq 1$. ☺

Clôture algébrique de $\mathbb{F}_p$

On fixe on nombre premier p. Pour tout n soit C_n un corps de cardinal $p^{n!}$.

Exercice

Pour tout n montrer que C_{n+1} contient un sous-corps isomorphe à C_n
Combien y a-t-il donc des homomorphismes de corps $C_n \hookrightarrow C_{n+1}$?

Exercice

Pour tout n on choisit un homomorphisme de corps $\phi_n : C_n \hookrightarrow C_{n+1}$.
Via ϕ_n on identifie C_n avec le sous-corps de C_{n+1} de même cardinal.
Montrer que leur réunion $C = \bigcup_{n\geq 1} C_n$ est un corps (de cardinal infini)
de sorte que les C_n sont des sous-corps (finis). On le notera $\bar{\mathbb{F}}_p$.

Ayant fixé nos choix ci-dessus, on peut finalement justifier notre notation :

Exercice

Montrer que $\bar{\mathbb{F}}_p$ contient un unique sous-corps $\mathbb{F}_{p^d}$ de cardinal p^d pour tout d.
Pour tout $d, e \in \mathbb{N}_{\geq 1}$ montrer que $\mathbb{F}_{p^d} \subset \mathbb{F}_{p^e}$ si et seulement si $d \mid e$.

Exercice

Montrer que $\bar{\mathbb{F}}_p$ est algébriquement clos, c'est-à-dire que tout $P \in \bar{\mathbb{F}}_p[X]$ se décompose comme $P = c_0(X - c_1)\cdots(X - c_n)$ où $c_0, c_1, \ldots, c_n \in \bar{\mathbb{F}}_p$.

Exercices

Exercice

Soit $p \geq 2$ un nombre premier. Notons $a_p^n = |I_p^n|$ le nombre des polynômes irréductibles de degré n sur $\mathbb{F}_p$. Calculer $a_2^1, a_2^2, a_2^3, a_2^4, a_2^5, a_2^6, \ldots$.
Même exercice pour $p = 3$, puis un nombre premier p quelconque.
(Si vous voulez vous pouvez écrire un programme qui effectue ce calcul.)

Exercice

Le polynôme $X^2 + X + 1$ admet-il une racine dans $\mathbb{F}_2$? dans $\mathbb{F}_4$? dans $\mathbb{F}_8$? dans $\mathbb{F}_{16}$? dans $\mathbb{F}_{32}$? dans un corps $\mathbb{F}_{2^n}$ pour n quelconque ?

Expliciter les sous-corps de $\mathbb{F}_{4096}$ et leurs inclusions mutuelles.

Exercice

Soit p un nombre premier et soit $a \in \mathbb{F}_p^\times$. Montrer que $X^p - X - a$ est irréductible sur $\mathbb{F}_p$. (On reconnaîtra le cas particulier $p = 2$.)

Exercice

Étant donnés un nombre premier $p \in \mathbb{N}$ et un nombre $n \in \mathbb{N}_{\geq 1}$, existe-t-il un polynôme irréductible $P \in \mathbb{F}_p[X]$ de degré n tel que le groupe multiplicatif $F^\times$ du corps $F = \mathbb{F}_p[X]/(P)$ de cardinal p^n soit engendré par l'image de X ?

Exercices

Exercice

Montrer le théorème de Wilson : pour tout corps fini F on a $\prod_{a \in F^\times} a = -1$.

Exercice

Soit $\mathbb{F}_q$ un corps de cardinal q. Pour $a \in \mathbb{F}_q$ expliciter les valeurs prises par la fonction polynomiale $\delta_a : \mathbb{F}_q \to \mathbb{F}_q$, $\delta_a(x) = 1 - (x-a)^{q-1}$. En déduire que toute application $g : \mathbb{F}_q \to \mathbb{F}_q$ est polynomiale (de degré $\leq q-1$).

Exercice

Dans $\mathbb{F}_{61}^\times$ combien y a-t-il des carrés ? des cubes ? des puissances 5 ? 6 ? 7 ?

Exercice

Dans $\mathbb{F}_q$ combien y a-t-il des racines primitives ? Dans $\mathbb{F}_3$ et $\mathbb{F}_4$ tous les éléments différents de 0 et 1 sont des racines primitives. Dans l'ordre de leurs cardinaux, quels sont les prochains corps ayant cette propriété remarquable ? Essayer de les caractériser les plus explicitement possible.

Un code détecteur d'erreurs

On souhaite transmettre un message à n bits, $P = (p_1, \ldots, p_n) \in \mathbb{F}_2^n$. Malheureusement la transmission subit des perturbations aléatoires, et le message reçu $P^* = (p_1^*, \ldots, p_n^*)$ peut être erroné.

Dans le cas d'une erreur simple un seul bit est changé. Comment transmettre le message de sorte que le récepteur puisse détecter une erreur simple ?

Exercice

La méthode naïve consiste à envoyer P deux fois. Est-ce efficace ? Expliquer comment rajouter un bit supplémentaire p_0, dit bit de parité, qui permet de détecter une erreur simple. Justifier l'intérêt de cette méthode.

On peut encoder les n bits par le polynôme $P = \sum_{i=1}^{n} p_i X^{i-1}$ dans $\mathbb{F}_2[X]$. Transmettre un polynôme équivaut à transmettre la suite de ses coefficients.

Exercice

On pose $T = XP + R$ où R est le reste de la division de XP par $X + 1$. Vérifier que $R = P(1)$ et que le reste de la division de T par $X + 1$ vaut 0, ce qui est un critère de parité simple pour tester l'intégrité du message T.

Supposons que la transmission de T résulte en réception de T^*, qui peut être erroné. Expliquer comment détecter une erreur simple (c'est-à-dire, on suppose $T^* = T + X^i$). Est-il possible de reconstituer T à partir de T^* ?

Un code correcteur d'erreurs

On veut transmettre un message à 120 bits (soit 15 octets) de sorte qu'une éventuelle erreur simple soit corrigible par le récepteur. Comment faire ?

Exercice

La méthode naïve consiste à envoyer trois fois le même message. Une méthode légèrement optimisée consiste à envoyer deux fois le message avec son bit de parité. Expliquer comment détecter puis corriger une erreur simple.

Voici une méthode plus raffinée : soit $A \in \mathbb{F}_2[X]$ irréductible de degré 7.
On pose $T = X^7 P + R$ où $R = X^7 P \operatorname{rem} A$. Ainsi on assure que $T \operatorname{rem} A = 0$.
Si le message reçu est $T^* = T + X^i$, alors $T^* \operatorname{rem} A = X^i \operatorname{rem} A$.

Exercice

Soit $F = \mathbb{F}_2[X]/(A)$ et notons x l'image de X dans F. Montrer que x engendre $F^\times$, et en déduire que l'application $X^i \mapsto x^i$ est injective pour $0 \leq i < 127$. Expliquer comment reconstituer T à partir d'un message simplement erroné T^*. Quel est l'intérêt de cette méthode ?

Exercice

Pour implémenter cette méthode il faut exhiber un polynôme irréductible de degré 7 dans $\mathbb{F}_2[X]$: Rappeler que les polynômes irréductibles de degré ≤ 3 dans $\mathbb{F}_2[X]$ sont X, $X+1$, X^2+X+1, X^3+X^2+1, X^3+X+1.
En déduire que $A = X^7 + X^3 + 1$ est irréductible dans $\mathbb{F}_2[X]$.