CORPS FINIS

$\varphi : \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{K}$ morphisme

On a une identification $\mathbb{Z}/p\mathbb{Z} \subset \mathbb{K}$ sous corps

$\ker(\varphi) = \{0\}$ ($\ker(\varphi)$ idéal de $\mathbb{Z}/p\mathbb{Z}$ corps donc $\ker(\varphi) = \{0\}$ ou $\ker(\varphi) = \mathbb{Z}/p\mathbb{Z}$ si $\ker(\varphi) = \mathbb{Z}/p\mathbb{Z}$ $\varphi(1_{\mathbb{Z}/p\mathbb{Z}}) = 0 = 1_{\mathbb{K}} \neq 0$)

(1) $\mathbb{K}$ corps fini ; alors $\mathrm{car}(\mathbb{K}) = p$ où p est un nombre premier et $\mathrm{card}(\mathbb{K}) = p^n$ où $n \in \mathbb{N}$ $n \geq 1$

(2) Soit p un nombre premier, $P \in \mathbb{F}_p[X]$ irréductible de degré n, $n \in \mathbb{N}$ $n \geq 1$

alors $\mathbb{F}_p[X]/\langle P \rangle$ est un corps fini de cardinal p^n et on sait calculer explicitement dans un tel corps.

(3) $\mathbb{K}$ corps fini ; alors $\mathbb{K}^\times$ est cyclique (non effectif)

($\exists x \in \mathbb{K}^\times$, $\mathbb{K}^\times = \{x^n\}_{n \in \mathbb{N}}$)

(4) Application de (3) Soit p un nombre premier $n \in \mathbb{N}$ $n \geq 1$ et $\mathbb{K}$ corps fini de cardinal p^n ; alors il existe un polynôme $P \in \mathbb{F}_p[X]$ irréductible de degré n tel que $\mathbb{K}$ est isomorphe à $\mathbb{F}_p[X]/\langle P \rangle$

Démonstration Soit $x \in \mathbb{K}^\times$ tel que $\mathbb{K}^\times = \{x^m\}_{m \in \mathbb{N}}$

On définit $\varphi : \mathbb{F}_p[X] \longrightarrow \mathbb{K}$

comme l'unique morphisme de $\mathbb{F}_p$-algèbres de $\mathbb{F}_p[X]$ vers $\mathbb{K}$ qui envoie X sur x.

c'est-à-dire $\sum_{i=0}^{d} a_i X^i \longmapsto \sum_{i=0}^{d} a_i . x^i$ où $a_i \in \mathbb{F}_p$ utilise $\mathbb{F}_p \subset \mathbb{K}$

Montrons que φ est surjectif $0_{\mathbb{K}} = \varphi(0_{\mathbb{F}_p[X]})$

Soit $y \in \mathbb{K} \setminus \{0_{\mathbb{K}}\} = \mathbb{K}^\times$ Soit $n \in \mathbb{N}$ tel que $y = x^n$

Donc $y = \varphi(X^n)$ Donc φ est surjectif

(en particulier $\mathbb{F}_p[X]/\ker(\varphi)$ est isomorphe à $\mathbb{K}$)

$\ker(\varphi)$ est un idéal maximal de $\mathbb{F}_p[X]$ (car $\mathbb{K}$ est un corps) donc il existe $P \in \mathbb{F}_p[X]$ irréductible tel que $\ker(\varphi) = \langle P \rangle = P \cdot \mathbb{F}_p[X]$

Donc $\mathbb{K}$ est isomorphe à $\mathbb{F}_p[X]/\langle P \rangle$

On $\mathrm{card}(\mathbb{F}_p[X]/\langle P \rangle) = \mathrm{card}(\mathbb{F}_p)^{\deg(P)} = p^{\deg(P)}$

$\| \mathrm{card}(\mathbb{K})$ donc $\deg(P) = n$

A anneau, $n \in \mathbb{N}$

$A \to A$, $a \mapsto a^n$: n'est pas en général un morphisme d'anneaux

$(a \times b)^n = a^n \times b^n$

~~$(a+b)^n = a^n + b^n$~~ est FAUSSE en général

(5) Frobenius

p un nombre premier

$\mathbb{K}$ corps de caractéristique p

Alors $\forall x, y \in \mathbb{K} \quad \forall n \in \mathbb{N} \quad (x+y)^{p^n} = x^{p^n} + y^{p^n}$

(ingrédient clef : si $1 \leq k \leq p-1$, alors $p \mid \binom{p}{k}$)

en particulier ($n \in \mathbb{N}$) : $\mathbb{K} \to \mathbb{K}$, $x \mapsto x^{p^n}$ est un morphisme d'anneaux

$n = 1$ « morphisme de Frobenius »

(6) Soit p premier, $n \in \mathbb{N}$, $n \geq 1$, $\mathbb{K}$ et $\mathbb{L}$ deux corps de cardinal p^n. Alors $\mathbb{K}$ et $\mathbb{L}$ sont isomorphes.

Démonstration D'après le point (4), il existe $P \in \mathbb{F}_p[X]$ de degré n tel que $\mathbb{K}$ est isomorphe à $\mathbb{F}_p[X]/\langle P \rangle$

Il suffit de montrer que $\mathbb{F}_p[X]/\langle P \rangle$ et $\mathbb{L}$ sont isomorphes.

Il suffit de construire un morphisme $\varphi : \mathbb{F}_p[X]/\langle P \rangle \to \mathbb{L}$

(nécessairement $\ker(\varphi) = \{0\}$ — cf. raisonnement ci-dessus — donc φ est injectif et $\mathrm{card}(\mathbb{F}_p[X]/\langle P \rangle) = \mathrm{card}(\mathbb{L})$ donc φ est bijectif)

Il suffit de construire un morphisme $\tilde{\varphi} : \mathbb{F}_p[X] \to \mathbb{L}$ contenant de noyau $\langle P \rangle$, donc il suffit d'exhiber un élément y de $\mathbb{L}$ tel que $P(y) = 0$

(on définit alors $\tilde{\varphi} : \mathbb{F}_p[X] \to \mathbb{L}$, $Q \mapsto Q(\alpha)$)

P a-t-il une racine dans $\mathbb{L}$?

Il suffit de construire un morphisme $\tilde{\varphi} : \mathbb{F}_p[X] \longrightarrow \mathbb{L}$ contenant de noyau $\langle P \rangle$, $P \in \mathbb{F}_p[X]$, donc il suffit d'exhiber un élément y de $\mathbb{L}$ tel que $P(y) = 0$

(on définit alors $\tilde{\varphi} : \mathbb{F}_p[X] \longrightarrow \mathbb{L}$, $Q \longmapsto Q(\alpha)$)

(Q) P a-t-il une racine dans $\mathbb{L}$?

Lemme Soit p un nombre premier et $P \in \mathbb{F}_p[X]$ irréductible de degré n. Alors P divise $X^{p^n} - X$

Admettons le lemme et répondons à la question (Q)

D'après le lemme, on peut écrire $X^{p^n} - X = P \cdot R$

$\deg(P) = n$ donc $\deg(R) = p^n - n < p^n$ or $\text{card}(\mathbb{L}) = p^n > \deg(R)$

Donc il existe $y \in \mathbb{L}$ tel que $R(y) \neq 0$

On a $y^{p^n} - y = P(y) \times R(y)$ (*)

or $\forall z \in \mathbb{L}$, $z^{p^n} - z = 0$

(soit $z \in \mathbb{L}$; si $z = 0$ ok ; si $z \in \mathbb{L} \setminus \{0\} = \mathbb{L}^\times$, $z^{\text{card}(\mathbb{L})-1} = 1$ d'après le théorème de Lagrange ; donc $z^{p^n - 1} = 1$ donc $z^{p^n} = z$)

(*) $R(y) \neq 0$ $y^{p^n} - y = 0$ $\mathbb{L}$ est intègre

donc $P(y) = 0$ donc (Q) a une réponse positive.

Lemme Soit p un nombre premier et $P \in \mathbb{F}_p[X]$ irréductible de degré n. Alors P divise $X^{p^n} - X$

(on fait on a une version plus forte)

Démonstration Soit $\mathbb{K} = \mathbb{F}_p[X]/\langle P \rangle$ et x l'image de X dans $\mathbb{K}$.

$\text{card}(\mathbb{K}) = p^n$

$P(x) = 0$ et si $Q \in \mathbb{F}_p[X]$ tel que $0 \leq \deg(Q) < n$ on a $Q(x) \neq 0$ (cf théorème 6 du chapitre 3)

$\{ Q \in \mathbb{F}_p[X],\ Q(x) = 0 \}$ est un idéal de $\mathbb{F}_p[X]$ qui : - contient P

- ne contient aucun polynôme Q tel que $0 \leq \deg(Q) < n$
- est de la forme $P_0 \cdot \mathbb{F}_p[X]$ avec $P_0 \in \mathbb{F}_p[X]$

donc $\{ Q \in \mathbb{F}_p[X],\ Q(x) = 0 \} = P \cdot \mathbb{F}_p[X]$

or $x^{p^n} - x = 0$ donc $X^{p^n} - X$ ce qui conclut. (cf ci dessus)

(7) Soit p un nombre premier et $n \in \mathbb{N}$ $n \geq 1$

Alors il existe un corps fini de cardinal p^n

(8) p nombre premier $n \in \mathbb{N}$ $n \geq 1$

$$X^{p^n} - X = \prod_{r \mid n} \ \prod_{P \in \{\text{ensemble des polynômes irréductibles de degré } r \text{ sur } \mathbb{F}_p[X]\}} P$$

(p premier, $n \geq 1$) $p = 2$ $n = 3$

Construire et calculer dans un corps de cardinal p^n

(1) on détermine un polynôme P de $\mathbb{F}_p[X]$ irréductible de degré n unitaire

Si $n = 2$ ou $n = 3$, on peut énumérer tous les polynômes unitaires de $\mathbb{F}_p[X]$ de degré n et en chercher un qui n'a pas de racines dans $\mathbb{F}_p$

~~X^3~~, $X^3 + [1]_2$, ~~$X^3 + X$~~, $X^3 + X + [1]_2$

~~$X^3 + X^2$~~, $X^3 + X^2 + [1]_2$, ~~$X^3 + X^2 + X$~~, $X^3 + X^2 + X + [1]_2$

$P = X^3 + [1]_2$ $\quad P([0]_2) = [1]_2$ $\quad P([1]_2) = [2]_2 = [0]_2$

$P = X^3 + X + [1]_2$ $\quad P([0]_2) = [1]_2$ $\quad P([1]_2) = [3]_2 = [1]_2$ ok

(p premier, $n \geq 1$) $\quad p=2 \quad n=3$

Construire et calculer dans un corps de cardinal p^n

(1) On détermine un polynôme P de $\mathbb{F}_p[X]$ irréductible de degré n unitaire

Si $n=2$ ou $n=3$, on peut énumérer tous les polynômes unitaires de $\mathbb{F}_p[X]$ de degré n et en chercher un qui n'a pas de racines dans $\mathbb{F}_p$

X^3, $X^3 + [1]_2$, $X^3 + X$, $X^3 + X + [1]_2$

$X^3 + X^2$, $X^3 + X^2 + [1]_2$, $X^3 + X^2 + X$, $X^3 + X^2 + X + [1]_2$

$P = X^3 + [1]_2 \quad P([0]_2) = [1]_2 \quad P([1]_2) = [2]_2 = [0]_2$

$P = X^3 + X + [1]_2 \quad P([0]_2) = [1]_2 \quad P([1]_2) = [3]_2 = [1]_2$ ok

(2) On considère $\mathbb{K} := \mathbb{F}_p[X]/\langle P \rangle \quad \text{card}(\mathbb{K}) = p^n$

On note α l'image de X dans $\mathbb{K}$ par le morphisme $\mathbb{F}_p[X] \longrightarrow \mathbb{F}_p[X]/\langle P \rangle$

(Théorème 6 du chapitre 3) $\quad \mathbb{F}_p^n \longrightarrow \mathbb{K}$

$\{1, \alpha, \dots, \alpha^{\deg(P)-1}\}$ est une base de $\mathbb{F}_p$-ev $\mathbb{K}$ $\quad (a_0, a_1, \dots, a_{n-1}) \longmapsto \sum_{i=0}^{n-1} a_i \cdot \alpha^i$

est une bijection (et même un isomorphisme de $\mathbb{F}_p$-espaces vectoriels)

$$\mathbb{K} = \{[0]_2, [1]_2, \alpha, \alpha + [1]_2, \alpha^2, \alpha^2 + [1]_2, \alpha^2 + \alpha, \alpha^2 + \alpha + [1]_2\}$$

Addition c'est l'addition dans $\mathbb{F}_p^n$ modulo l'isomorphisme de $\mathbb{F}_p$-ev ci dessus

$$\left(\sum_{i=0}^{n-1} a_i \cdot \alpha^i\right) + \left(\sum_{i=0}^{n-1} b_i \cdot \alpha^i\right) = \sum_{i=0}^{n-1} (a_i + b_i) \cdot \alpha^i$$

$a_0, \dots, a_{n-1} \in \mathbb{F}_p$

$b_0, \dots, b_{n-1}$

$$(\alpha + [1]_2) + (\alpha^2 + \alpha + [1]_2)$$
$$= \alpha^2 + [2]_2 \cdot \alpha + [2]_2$$
$$= \alpha^2$$

Multiplication

$$(\alpha^2+\alpha)\times(\alpha^2+[1]_2)$$
$$= \alpha^4 + \alpha^2 + \alpha^3 + \alpha \quad \in \mathbb{K}$$

pas de la forme $a_0 + a_1\alpha + a_2\alpha^2$ avec $a_0, a_1, a_2 \in \mathbb{F}_2$

$$(\alpha^2+\alpha)^2 = \alpha^4 + \alpha^2 \overset{?}{=} [1]_2 \quad (\mathrm{car}(\mathbb{K})=2)$$

on ne peut pas répondre sans cette forme

$$= a_0 + a_1\alpha + a_2\alpha^2 \overset{?}{=} [1]_2$$

$a_0, a_1, a_2 \in \mathbb{F}_2$

$$\Leftrightarrow \begin{cases} a_0 = [1]_2 \\ a_1 = [0]_2 \\ a_2 = [0]_2 \end{cases}$$

$$\pi(P) = 0 = \sum_{i=0}^{n-1} b_i \alpha^i + \alpha^n \quad \text{donc} \quad \alpha^n = -\sum_{i=0}^{n-1} b_i \alpha^i$$

$\pi(X) = \alpha$

$$P = \sum_{i=0}^{n-1} b_i \cdot X^i + X^n$$

$b_0, \dots, b_{n-1} \in \mathbb{F}_p$

$$P = X^3 + X + [1]_2 \qquad \alpha^3 + \alpha + [1]_2 = 0$$

donc $\alpha^3 = \alpha + [1]_2$ $(\mathrm{car}\ \mathbb{K}=2)$

donc $\alpha \times \alpha^3 = \alpha^2 + \alpha$

donc $\alpha^4 = \alpha^2 + \alpha$

$$(\alpha^2+\alpha)^2 = \alpha^4 + \alpha^2$$
$$= (\alpha^2+\alpha) + \alpha^2$$
$$= \alpha$$

Méthode algorithmique

$y_1, y_2 \in \mathbb{K}$ $\quad y_1 = \sum_{i=0}^{n-1} a_{i,1} \cdot \alpha^i$ $\quad a_{i,1} \in \mathbb{F}_p$

$y_2 = \sum_{i=0}^{n-1} a_{i,2} \cdot \alpha^i$ $\quad a_{i,2} \in \mathbb{F}_p$

$y_1 \times y_2 = ?$

$Q_1 = \sum_{i=0}^{n-1} a_{i,1} \cdot X^i \in \mathbb{F}_p[X]$ $\quad \pi(Q_1) = y_1$

$Q_2 = \sum_{i=0}^{n-1} a_{i,2} \cdot X^i \in \mathbb{F}_p[X]$ $\quad \pi(Q_2) = y_2$

$Q_1 Q_2 = P Q_3 + R$ division euclidienne de $Q_1 Q_2$ par P

$Q_3 \in \mathbb{F}_p[X]$ $\quad R \in \mathbb{F}_p[X]$ $\quad \deg(R) < n$

$$R = \sum_{i=0}^{n-1} r_i X^i \qquad r_i \in \mathbb{F}_p$$

Méthode algorithmique $y_1, y_2 \in \mathbb{K}$ $\quad y_1 = \sum_{i=0}^{m-1} a_{i,1} \cdot \alpha^i \quad a_{i,1} \in \mathbb{F}_p$

$y_2 = \sum_{i=0}^{m-1} a_{i,2} \cdot \alpha^i \quad a_{i,2} \in \mathbb{F}_p$

$y_1 \times y_2 = ?$

$Q_1 = \sum_{i=0}^{m-1} a_{i,1} \cdot X^i \in \mathbb{F}_p[X] \qquad \pi(Q_1) = y_1$

$Q_2 = \sum_{i=0}^{m-1} a_{i,2} \cdot X^i \in \mathbb{F}_p[X] \qquad \pi(Q_2) = y_2$

$Q_1 Q_2 = P Q_3 + R$ division euclidienne de $Q_1 Q_2$ par P

$Q_3 \in \mathbb{F}_p[X] \quad R \in \mathbb{F}_p[X] \quad \deg(R) < m$

$R = \sum_{i=0}^{m-1} r_i X^i \quad r_i \in \mathbb{F}_p$

$\pi(Q_1 Q_2) = \pi(P)\pi(Q_3) + \pi(R) = \sum_{i=0}^{m-1} r_i \cdot \alpha^i$

$\pi(Q_1 Q_2) = \pi(Q_1)\pi(Q_2) = y_1 y_2$; $\pi(P) = 0$