Option C

Exercices Corps finis

D. Kohel

10/11/2020

Exercices corps finis

Ex. 1. Combien d'anneaux comm. de cardinal 4 est-ce qu'il y a ?

Soit A un anneau (avec 1), $|A| = 4$.
Alors la caractéristique est un générateur du noyau

$$(n) \subseteq \mathbb{Z} \xrightarrow{\exists!} A$$
$$1 \longmapsto 1_A$$

Ici : $\mathrm{car}(A) = \begin{cases} 2, \text{ ou} \\ 4. \end{cases}$ — par Lagrange

$\Leftrightarrow \mathbb{Z}/n\mathbb{Z} \hookrightarrow A$ (*) groupe additif d'ordre 4

a) Si $\mathrm{car}(A) = 4$, alors $A \cong \mathbb{Z}/4\mathbb{Z}$: (*) est un isomorphisme (*0)

b) Si $\mathrm{car}(A) = 2$, alors A est un $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$-espace vectoriel, $\dim_{\mathbb{F}_2} A = 2$

$\mathbb{F}_2$-algèbre.

$\Rightarrow$ Soit $\alpha \in A \setminus \mathbb{F}_2$, $\{\alpha, \alpha+1\}$

$$\text{on a } A = \mathbb{F}_2[\alpha] \cong \mathbb{F}_2[x]/(f(x)) \quad \alpha \longleftrightarrow x$$

Base : $\{1, \alpha\}$

où $f(x) = x^2 + ax + b$. On peut énumérer :

(*3) $\mathbb{F}_2[\alpha]$ où $\alpha^2 = 0$ (nilpotent)

α ↓ $\beta+1$:
- x^2
- $x^2 + x = x(x+1)$
- $x^2 + 1 = (x+1)^2$
- $x^2 + x + 1$ irred.

$\mathbb{F}_2[\beta]$ où $\beta^2 = 1$

(*2) chinois $A \cong \mathbb{F}_2 \times \mathbb{F}_2$.

(*1) : $A \cong \mathbb{F}_2[x]/(x^2+x+1) \cong \mathbb{F}_4$

Ex. 3 : Trouver les premiers p et degrés r tel qu'il existe qu'un seul polynôme irred de degré r.

Exemple : $p=2$ et $r=2$

$$x^2+x+1 \in \mathbb{F}_2[x]$$

est le seul polynôme irred degré 2.
Alors

$$\mathbb{F}_4 \cong \mathbb{F}_2[x]/(x^2+x+1)$$

est une repr. unique comme quotient de $\mathbb{F}_2[x]$ (ou comme extension de $\mathbb{F}_2$).

Exemple : p premier, $r=p-1$

$$\frac{x^p-1}{x-1} = x^{p-1}+\dots+x+1 = \Phi_p(x)$$

est irred dans $\mathbb{Q}[x]$ (ou $\mathbb{Z}[x]$) mais pas dans $\mathbb{F}_p[x]$:

$$x^p-1 = (x-1)^p$$

Si $r=1$, on a $p>1$ polynômes irreds.

Si $p=2$ et $r=3$: $\mathbb{F}_8 \cong \mathbb{F}_2[x]/(f(x))$, où $f(x)$ est irred de degré 3 ? $\mathbb{F}_8[x]$

On a $\mathbb{F}_8^*$ un groupe d'ordre 7.

$$\Phi_7(x) = \frac{x^7-1}{x-1} = \prod (x-\alpha) = f_1(x) f_2(x) \in \mathbb{F}_2[x]$$

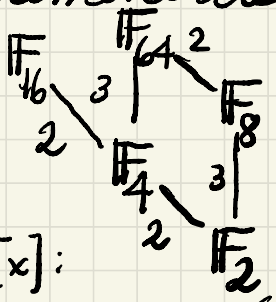
degré 6 → $\alpha \in \mathbb{F}_8^*$, $\alpha \neq 1$. (pourquoi)

Pourquoi deux polynômes irred de degré 3 ?

Réponse : $\Phi_7(x)$ est le produit des polynômes minimaux des $\alpha \in \mathbb{F}_8^* \setminus \mathbb{F}_2^* = \mathbb{F}_8 \setminus \mathbb{F}_2$.
Comme l'extension

$$\mathbb{F}_8/\mathbb{F}_2 = \mathbb{F}_{2^3}/\mathbb{F}_2$$

est degré 3, tout polynôme minimal d'un élément de $\mathbb{F}_8 \setminus \mathbb{F}_2$ est de dégré 3.



Dans $\mathbb{F}_2[x]$:

* irreds de degré 2 : 1
* irreds de degré 3 : $2 = \varphi(2^3-1)/3$
* polynômes primitifs de degré r :

$$\varphi(2^r-1)/r \quad \circledast$$

On veut savoir si (ou quand) cette valeur est 1 ou > 1.

<u>Remarque</u>. Ça donne la motivation pour Ex 2.5 : M.q. r divise $\varphi(p^r-1)$.

Rappel : $\varphi(p^r-1) = \left|\mathbb{Z}/(p^r-1)\mathbb{Z}^*\right|$

$$= \deg\left(\Phi_{p^r-1}(x)\right).$$

- $\varphi(p^r-1)/r = 1$ pour un nombre fini de p et r

Rappel: Une des propriétés de $\Phi_n(x) \in \mathbb{F}_p[x]$, $n \wedge p = 1$, est que $\Phi_n(x)$ est le produit de polynômes irreds de degré r = ordre de p dans $(\mathbb{Z}/n\mathbb{Z})^*$.

Idée: Soit α une racine de $\Phi_n(x)$ dans $\overline{\mathbb{F}_p}$. Alors $\alpha^n = 1$, par défn de $\Phi_n(x)$, qui est diviseur de $x^n - 1$.

Alors $\alpha^1, \alpha^p, \dots, \alpha^{p^r} = \alpha^1$ sont des racines du polynôme minimal $f(x)$ de α.

N.B. On a bien $\alpha^{p^r} = \alpha^1$ car $p^r \equiv 1 \bmod n$.

et en plus $\alpha^1, \alpha^p, \dots, \alpha^{p^{r-1}}$ sont distincts car l'ordre exact d'α est n.

Dernier, on utilise le fait que $\mathbb{F}_p[x]/(f(x)) \cong \mathbb{F}_{p^r}$ et

Sinon α est racine de $\Phi_m(x)$, $m \mid n$.

et $\phi : \mathbb{F}_{p^r} \longrightarrow \mathbb{F}_{p^r}$ est un automorphisme de $\mathbb{F}_{p^r}$ d'ordre r.
$\alpha \longmapsto \alpha^p$

Les orbites de ϕ sont

$$\{\alpha, \alpha^p = \phi(\alpha), \alpha^{p^2}, \dots\},$$

qui sont de cardinaux r si α est un élément primitif de $\mathbb{F}_{p^r}/\mathbb{F}_p$.

Rappel de la définition de $\Phi_n(x)$:

$$x^n - 1 = \prod_{m \mid n} \Phi_m(x) = \prod (x - \alpha)$$

$\uparrow \alpha \in \mathbb{F}_{p^r}^*$

$n = p^r - 1$

décomp en $\mathbb{F}_{p^r}[x]$

$\mathbb{F}_p[x]$: = produit des polynômes minimaux des éléments de $\mathbb{F}_{p^r}^*$: ils sont tous de degré divisant r.

<u>Exemple</u>

$\mathbb{F}_{16}^* = \mathbb{F}_{2^4}^* / \mathbb{F}_4^* = \mathbb{F}_{2^2}^* / \mathbb{F}_2^*$

groupe d'ordre 15 — 3 — 1

1, 3, 5, 15.

$\Phi_1(x) = x - 1 = x + 1 \in \mathbb{F}_2[x]$

$x^3 - 1 = \Phi_1(x)\Phi_2(x) = (x+1)(x^2+x+1)$

Dans $\mathbb{F}_{16}^*$ on a des éléments d'ordre

$x^{15}-1 = \Phi_1(x)\Phi_3(x)\Phi_5(x)\Phi_{15}(x)$

polynômes minimaux d'éléments de $\mathbb{F}_4^*$

Racines :
Éléments primitifs de $\mathbb{F}_{16}/\mathbb{F}_2$
— éléments d'ordre 5
— éléments d'ordre 15
= éléments primitifs du groupe $\mathbb{F}_{16}^*$ (cyclique)

$\Phi_5(x) = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1.$ (irred)

$\Phi_{15}(x)$ = polynôme de degré $\varphi(15) = 2\cdot 4$
= produit de deux polynômes irreds de degré 4.

Lequels ? Si $g(x) \mid \Phi_{15}(x)$, irred, alors $g(0) \neq 0$ et $g(1) \neq 0$, donc $\neq \Phi_5(x)$

$g(x) = x^4 + \cdots + 1$, $(\neq x^4+x^3+x^2+x+1)$

avec un nombre impair de coeffs non nuls. Alors

$g(x) = x^4+x+1$ ou x^4+x^3+1, (pas $x^4+x^2+1 = (x^2+x+1)^2$)

sont les deux diviseurs.