Algèbre et Arithmétique Effectives — 02/12/25
Cours 12

Rappels de la dernière fois

Soit $P \in K[x]$.

$I = (P) := \{ PA : A \in K[x] \}$

Anneau quotient $\frac{K[x]}{(P)} = \{ [B] : B \in K[x] \}$, où

$[B] = \{ B + PA : A \in K[x] \}$

On a montré qu'il existe une bijection :

$$K[x]_{<\deg(P)} \longrightarrow \frac{K[x]}{(P)}$$
$$R \longmapsto [R]$$

Exemple

$\mathbb{Q}[x]$

$P(x) = x^3 - 1 \in \mathbb{Q}[x]$

$$\frac{\mathbb{Q}[x]}{(x^3-1)} = \{ [R] : R \in \mathbb{Q}[x] \text{ et } \deg(R) < 3 \}$$

$[x^4] = [x]$: en effet $x^4 - x = (x^3-1)x \in (x^3-1)$

idéal engendré

$$\begin{array}{r|l} x^4 & x^3 - 1 \\ \cline{2-2} x^4 - x & x \\ \hline // \quad x & \end{array}$$

$x^4 = (x^3-1)x + x$

Est-ce que $\frac{\mathbb{Q}[x]}{(x^3-1)}$ est un anneau intègre ?

On remarque que $x^3 - 1 = (x-1)(x^2+x+1)$ dans $\mathbb{Q}[x]$

Donc $[x-1][x^2+x+1] = [x^3-1] = [0]$

$\underset{[0]}{\neq}$ $\quad$ $\underset{[0]}{\neq}$ $\quad$ $x^3-1 \in (x^3-1)$

$[a],[b] \in \frac{A}{I}$, $[a]=[b] \Leftrightarrow a-b \in I$

$\Rightarrow$ $\frac{\mathbb{Q}[x]}{(x^3-1)}$ n'est pas intègre.

<u>Proposition</u> : Soit $P \in K[x]$. L'ensemble des éléments inversibles de l'anneau

$$\frac{K[x]}{(P)}$$

est formé des classes de polynômes qui sont premiers avec P.

($[A]$ est inversible dans $\frac{K[x]}{(P)} \Leftrightarrow$ $\text{pgcd}(A,P)=1$)

Cette proposition est l'analogue de ce qu'on a démontré dans $\frac{\mathbb{Z}}{n\mathbb{Z}}$:

$a \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ est inversible $\Leftrightarrow$ $\text{pgcd}(a,n)=1$.

et sa démonstrations est analogue à celle sur $\frac{\mathbb{Z}}{n\mathbb{Z}}$ (par exercice).

<u>Proposition</u> : Soit $P \in K[x] \setminus \{0\}$
Alors $\frac{K[x]}{(P)}$ est un corps si et seulement si P est irréductible dans $K[x]$

<u>Dém</u>

$\Rightarrow$) Supposons que $\frac{K[x]}{(P)}$ est un corps. En particulier $\frac{K[x]}{(P)}$ est un anneau intègre.

Tout d'abord P n'est pas inversible, car sinon $(P) = (1) = K[x]$ et donc $\frac{K[x]}{(P)} = \{0\}$ qui n'est pas un corps.

Soient $A, B \in K[x]$ tels que $P = AB \Rightarrow$

$$\Rightarrow \underset{[A][B]}{\underbrace{[AB]}} = [P] = [0] \underset{\text{intègre}}{\Longrightarrow} [A] = [0] \text{ ou } [B] = [0]$$

si $[A] = [0] \Rightarrow A \in (P) \underset{P=AB}{\Longrightarrow} \deg(B) = 0 \Rightarrow B$ est inversible

si $[B] = [0] \Rightarrow B \in (P) \Rightarrow \deg(A) = 0 \Rightarrow A$ est inversible

Donc P est irréductible.

$\Leftarrow$) Supposons que P est irréductible. Soit $A \in K[x]$ tel que $[A] \neq [0]$. Alors P ne divise pas A

$$\underset{P \text{ est irréductible}}{\Longrightarrow} \operatorname{pgcd}(P, A) = 1 \underset{\text{proposition précédente}}{\Longrightarrow} [A] \text{ est inversible.}$$

$\Rightarrow \frac{K[x]}{(P)}$ est un corps

<u>Exemple</u>

<u>Notation</u> : $\mathbb{F}_p := \frac{\mathbb{Z}}{p\mathbb{Z}}$, avec p un nombre premier

Donc $\mathbb{F}_p$ est un corps fini avec p éléments

$\mathbb{F}_7[x]$

Est-ce qu'il existe un polynôme de degré 2 irréductible dans $\mathbb{F}_7[x]$?

$(x^2 + 6) = (x-1)(x-6)$ n'est pas irréductible dans $\mathbb{F}_7[x]$

(x^2+1) est irréductible car n'a pas de racines dans $\mathbb{F}_7$

Un polynôme P de degré 2 (ou 3) est irréductible dans $K[x]$ $\Leftrightarrow$ P n'a pas de racines dans K

Donc $\dfrac{\mathbb{F}_7[x]}{(x^2+1)}$ est un corps qui est en bijection avec $\mathbb{F}_7[x]_{<2} = \{ax+b : a,b \in \mathbb{F}_7\}$ et ce dernier a 7^2 éléments.

Donc $\dfrac{\mathbb{F}_7[x]}{(x^2+1)}$ est un corps (fini) avec 7^2 éléments.

<u>Déf</u> : Soit A un anneau et soient 0_A et 1_A les éléments neutres respectivement de l'addition et de la multiplication.

La <u>caractéristique</u> de A est le plus petit entier $n>0$ tel que

$$n \cdot 1_A = 0_A$$

si un tel entier existe et 0 sinon.

On la note $\mathrm{char}(A)$.

<u>Exemple</u> : $\mathrm{char}(\mathbb{Z}) = 0$

$\mathrm{char}(\mathbb{Q}) = 0$

$\mathrm{char}\left(\dfrac{\mathbb{Z}}{n\mathbb{Z}}\right) = n$

<u>Remarque</u> : A a caractéristique 0 si

$$n \cdot 1_A = 0_A \Leftrightarrow n = 0.$$

<u>Proposition</u> : Soit A un anneau intègre. Alors $\mathrm{char}(A) = 0$ ou $\mathrm{char}(A) = p$ est un nombre premier.

Dém : Supposons que $char(A) = n \neq 0$.

Si n n'est pas un nombre premier, alors $\exists\, 1 < a, b < n$ tels que $n = ab$. Mais alors :

$$0_A = n \cdot 1_A = (ab) 1_A = (a \cdot 1_A) \cdot (b \cdot 1_A) \Longrightarrow$$

$$\underset{A \text{ est intègre}}{\Longrightarrow} \quad a \cdot 1_A = 0_A \text{ ou } b \cdot 1_A = 0_A$$ ce qui contredit le fait que n est minimal.

Proposition : Soit K un corps.

1) Si $char(K) = 0$, alors K contient un sous-corps isomorphe à $\mathbb{Q}$.

2) Si $char(K) = p$, avec p premier, alors K contient un sous-corps isomorphe à $\mathbb{F}_p$.

Dem de 2

On considère le morphisme d'anneaux :

$$\varphi : \mathbb{Z} \longrightarrow K$$
$$m \longmapsto m \cdot 1_K$$

Puisque $char(K) = p$, alors $Ker(\varphi) = p\mathbb{Z}$

$$\underset{\text{I théorème d'isomorphisme}}{\Longrightarrow} \quad \frac{\mathbb{Z}}{p\mathbb{Z}} \simeq Im(\varphi) \subseteq K$$

Donc $Im(\varphi)$ est un sous-corps de K isomorphe à $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$.

Proposition : Soit K un corps fini. Alors $char(K) = p$, où p est un nombre premier.

De plus, il existe un entier $n \geq 1$ tel que $|K| = p^n$.

Remarque : la proposition dit que tout corps fini a un nombre d'éléments égal à une puissance d'un nombre premier.

Démo

Puisque K est un corps fini, alors K ne contient pas un sous-corps isomorphe à $\mathbb{Q}$ $\Rightarrow$ $\text{char}(K)=p$, avec p un nombre premier.

Donc K contient un sous-corps isomorphe à $\mathbb{F}_p$.

On peut facilement montrer que K est un $\mathbb{F}_p$-espace vectoriel avec l'addition (dans K) et la multiplication par scalaires dans $\mathbb{F}_p$.

Puisque K est fini, alors $\dim_{\mathbb{F}_p}(K) = n$, avec $1 \leq n < +\infty$ ($n>0$, car $K \neq \{0\}$).

Soit $(v_1, \ldots, v_n)$ une base de K, alors :

$$K = \{a_1 v_1 + \cdots + a_n v_n : a_i \in \mathbb{F}_p\}$$

En particulier on obtient $|K| = p^n$.

Proposition : Soit $P \in \mathbb{F}_p[x]$ un polynôme irréductible dans $\mathbb{F}_p[x]$ de degré $n>0$.

Alors $\frac{\mathbb{F}_p[x]}{(P)}$ est un corps fini avec p^n éléments.

Démo : Puisque P est irréductible, $\frac{\mathbb{F}_p[x]}{(P)}$ est un corps qui est en bijection avec :

$$\mathbb{F}_p[x]_{<\deg P} = \{a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} : a_i \in \mathbb{F}_p\}$$

$$\Longrightarrow \left|\frac{\mathbb{F}_p[x]}{(P)}\right| = p^n.$$

Par ailleurs on a que $\frac{\mathbb{F}_p[x]}{(P)}$ est un $\mathbb{F}_p$-espace vectoriel avec base $\{1, x, \ldots, x^{n-1}\}$.

On peut montrer que $\forall$ p premier, $\forall n > 0$, il existe un polynôme de degré n irréductible sur $\mathbb{F}_p[x]$, donc il existe un corps fini avec p^n éléments.

De plus les corps avec p^n éléments sont tous isomorphes entre eux.

Donc on note $\mathbb{F}_{p^n}$ l'unique corps, à isomorphisme près, avec p^n éléments.

<u>Exemple</u> : Une construction de $\mathbb{F}_{3^3}$.

Pour cela il faut un polynôme de degré 3 irréductible sur $\mathbb{F}_3$:

x^3+x^2+x+2 n'a pas de racines dans $\mathbb{F}_3$ est donc irréductible dans $\mathbb{F}_3[x]$

Donc on obtient $\mathbb{F}_{3^3} \simeq \dfrac{\mathbb{F}_3[x]}{(x^3+x^2+x+2)}$.