

121
123
125
141

Existence et
unicité des
corps finis

- Théorie de Galois, Gorenstein, p 85
- Algèbre Tome 4, Serre, p 61

602 Théorème : Soit p un nombre premier et $n \in \mathbb{N}^*$.

85 Soit $q = p^n$. Alors il existe un corps fini à q éléments. Il est le corps de décomposition sur $\mathbb{F}_p$ du polynôme $x^q - x$, et est noté $\mathbb{F}_q$.
Il est unique à $\mathbb{F}_p$ -isomorphisme près.

Preuve :

Unicité

Soit K un corps à $q = p^n$ éléments. Comme K est fini, $\text{carac}(K)$ est un nombre premier qui divise q , $\text{carac}(K) = p$ et le sous-corps premier de K est $\mathbb{F}_p$.

On a même que $n = [K : \mathbb{F}_p] = \dim_{\mathbb{F}_p}(K)$

On $(K^*, \cdot)$ est un groupe à $q-1$ éléments donc d'après le théorème de Lagrange, l'ordre de tout élément de $(K^*, \cdot)$ divise l'ordre du groupe.

Ainsi $\forall x \in K^*$, $x^{q-1} = 1$ donc $\forall x \in K^*$, $x^q = x$. Cette égalité est aussi vraie pour 0, donc $x^q = x \quad \forall x \in K$.

Soit $P(x) = x^q - x \in \mathbb{F}_p[x]$. Alors ce polynôme est de degré q mais donc admet au plus q racines.

Comme tout élément de K est racine de P , alors les racines de P sont exactement les éléments de K .

Ainsi P est scindé sur K et K est le plus petit corps ayant cette propriété.

Ainsi K est le corps de décomposition de P sur $\mathbb{F}_p$.

Par unicité du corps de décomposition et $\mathbb{F}_p$ -isomorphisme près, on se déduit l'unicité de $\mathbb{F}_q$.

Existence :

Soit K le corps de décomposition de $P = X^q - X$ sur $\mathbb{F}_p$.

Soit h l'ensemble des racines dans K de $X^q - X$:

$$h = \{x \in K ; P(x) = 0\} = \{x \in K ; x^q = x\} \subseteq K$$

S.Z.P

On montre que h est un corps

81

• $1 \in h$ donc h est non vide

• Soit $x, y \in h$ alors $x^q = x$ et $y^q = y$

donc $(xy)^q = x^q y^q = xy$ par commutativité de $h \subseteq K$
~~de $h \subseteq K$ car K est un corps fini donc commutatif~~

~~(h est fini car corps de décomposition~~
 car tout corps est supposé commutatif

• Soit $x \in h$ avec $x \neq 0$, alors

$$(x^{-1})^q = (x^q)^{-1} = x^{-1}$$

• Soit $x \in h$, $(-x)^q = (-1)^q x^q = -x$

et même si $p=2$ car alors $-x = x$

• Soit $x, y \in h$ Alors d'après le morphisme de Frobenius sur K , utilisé n fois,

$$\begin{aligned} (x+y)^q &= ((x+y)^p)^{q/p} \\ &= (x^p + y^p)^{q/p} \\ &= (x+y)^{q/p} = \dots = x+y \end{aligned}$$

Donc h est un corps.

$$\text{Or } P'(x) = q x^{q-1} - 1 = -1 \quad (\text{car } p \mid q)$$

donc est premier avec P .

Donc toutes les racines de P sont simples.

Donc $|h| = q$.

Ainsi k est un corps à q éléments
 (et même $k = K$). Car k est un corps contenant $\mathbb{F}_p$
 et toutes les racines de p et on obtient la
 minimalité du corps de décomposition.

602 Théorème : Soit p premier et $n \in \mathbb{N}^+$. Soit $q = p^n$. Alors
 87 $\mathbb{F}_q \cong \mathbb{F}_p[x]/(\pi)$ où π est un polynôme irréductible
 de degré n sur $\mathbb{F}_p$.

Preuve : On voit que $\mathbb{F}_p[x]/(\pi)$ est un corps car
 $\mathbb{F}_p[x]$ est principal et π irréductible donc (π) est
 maximal. C'est une extension de $\mathbb{F}_p$ et est alors
 de ~~cardinal~~ cardinal p^n où $n = \deg(\pi)$
 car une base de $\mathbb{F}_p[x]/(\pi)$ est $(1, x, \dots, x^{n-1})$
 en tant que $\mathbb{F}_p$ -ev.

Par unicité, $\mathbb{F}_p \cong \mathbb{F}_p[x]/(\pi)$

On pourrait aussi utiliser que $\mathbb{F}_p[x]/(\pi)$ est le
 corps de rupture de π sur $\mathbb{F}_p$.

• Réciproquement, $\mathbb{F}_q$ peut toujours être obtenu de
 cette manière.

En effet, comme $\mathbb{F}_q^*$ est un groupe cyclique, soit
 ξ un de ses générateurs. Alors d'après le théorème
 de Lagrange, $\xi^{q-1} = 1$ donc ξ est algébrique sur $\mathbb{F}_p$.
 Soit π son polynôme minimal.

Alors comme $\mathbb{F}_q = \{0, 1, \xi, \dots, \xi^{q-2}\} = \mathbb{F}_p[\xi] = \mathbb{F}_p(\xi)$
 et que $\mathbb{F}_p(\xi)$ est un corps de rupture de ξ sur $\mathbb{F}_p$,
 par unicité du corps de rupture, on a

$$\mathbb{F}_q \cong \mathbb{F}_p[x]/(\pi)$$

Ainsi $\deg(\pi) = [\mathbb{F}_q : \mathbb{F}_p] = n$.

On a en plus montré qu'il existe des polynômes irréductibles de tous degrés sur $\mathbb{F}_p$.

Remarque:

- 1) Avant de faire le 2^e théorème, il faut avoir mis dans le plan que $\mathbb{F}_q^*$ est cyclique.

- 602 2) Corollaire. Si π est un polynôme irréductible de
87 degré n sur $\mathbb{F}_p$, alors $\pi(x)$ divise $x^q - x$ dans $\mathbb{F}_p[x]$ donc est scindé sur $\mathbb{F}_q$ donc son corps de rupture est aussi son corps de décomposition.

Preuve: Soit π irréductible de degré n sur $\mathbb{F}_p$.
Si $\pi(x) \neq x$, soit D un corps de décomposition de $\pi(x)$ sur $\mathbb{F}_p$ et soit θ une racine de $\pi(x)$ dans D .

Alors $\theta \neq 0$ car θ n'était pas racine de π dans $\mathbb{F}_p$.

On a $\theta \in \mathbb{F}_p(\theta) \cong \mathbb{F}_p[x]/(\pi) \cong \mathbb{F}_q$ d'après le théorème précédent.

D'après le théorème de Zagrange, $\theta^{q-1} = 1$
donc $\pi(x)$ divise $x^{q-1} - 1$ dans $\mathbb{F}_p[x]$.

Ainsi $\pi(x)$ divise $x^q - x$ dans $\mathbb{F}_p[x]$ (même aussi pour $\pi(x) = x$)

Or ce dernier est scindé sur $\mathbb{F}_q$ d'après le 1^{er} théorème donc π l'est aussi.

Ainsi $\mathbb{F}_p(\theta) \cong \mathbb{F}_q$ qui était un corps de rupture de π sur $\mathbb{F}_p$ est en fait un corps de décomposition.

3) Dans un corps fini, le corps de rupture = corps de décomposition.

Ce n'est pas vrai en général.

Prendre $P(x) = x^3 - 2$ dans $\mathbb{Q}(x)$.

Alors P est irréductible par Eisenstein.

Un corps de rupture est $\mathbb{Q}(\sqrt[3]{2})$ mais il n'est pas un corps de décomposition car ne contient pas les racines complexes $j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$.

602 4) Corollaire: Le produit des éléments de $\mathbb{F}_q^*$ est
86 égal à -1 .

Preuve: On a $\mathbb{F}_q = \{a_0, a_1, \dots, a_{q-1}\}$ avec $a_0 = 0$

Alors $x^q - x = \prod_{i=0}^{q-1} (x - a_i)$ car $\mathbb{F}_q$ est le corps de décomposition de $x^q - x$ sur $\mathbb{F}_p$.

Ainsi: $x^{q-1} - 1 = \prod_{i=1}^{q-1} (x - a_i)$

donc le terme constant est:

$$-1 = a_1 a_2 \dots a_{q-1}$$

602 5) On peut dénombrer les polynômes irréductibles
88 sur $\mathbb{F}_p$.

Soit $j \in \mathbb{N}^+$, on note $I(p, j)$ le nombre de polynômes irréductibles de degré j sur $\mathbb{F}_p$.

Alors: $\forall n \in \mathbb{N}^+$,

$$p^n = \sum_{d|n} d \cdot I(p, d)$$

On a que $I(p, 1) = p$ car les irred de degré 1 sont les $(x - d)$ avec $d \in \mathbb{F}_p$.

Alors: $p^2 = I(p, 1) + 2 I(p, 2)$

$$\text{donc } I(p, 2) = \frac{p(p-1)}{2}$$

De même, $p^2 = I(p, 1) + \cancel{I(p, 2)} + 3 I(p, 3)$

d'où $p^3 = p + \cancel{I(p, 2)} + 3 I(p, 3)$

d'où : $I(p, 3) = \frac{p^3 - p}{3} = \frac{p(p+1)(p-1)}{3}$