

Théorème: Soit p premier, et $n \geq 1$. Il existe un unique corps à $q = p^n$ éléments noté $\mathbb{F}_q$, unique à isomorphisme près.

Preuve: Posons $P = X^q - X \in \mathbb{Z}/p\mathbb{Z}[X]$. Soit K le corps de décomposition de P sur $\mathbb{Z}/p\mathbb{Z}$. On pose:

$$L = \{x \in K \mid P(x) = 0\} \subseteq K.$$

1) Il. L est un sous-corps de K .

- * $0, 1 \in L$.
- * Si $x, y \in L$, $y \neq 0$ alors $(xy^{-1})^q = x^q (y^q)^{-1} = xy^{-1}$, $xy^{-1} \in L$.
- * Si $x \in L$.
 - Si $p=2$, alors, $(-x)^{2^n} = x^{2^n} = x = -x$ car $\text{car}(K)=2$.
 - Sinon, $(-x)^q = -x^q = -x$, donc $-x \in L$.
- * Si $x, y \in L$, $(x+y)^q = ((x+y)^p)^{p^{n-1}} = (x^p + y^p)^{p^{n-1}} = (x+y)^{p^{n-1}} = \dots = x+y$, et $x+y \in L$.

2) Il. $|L| = q$, $L = K$ (et donc l'existence du thm)

On a que $P'(X) = qX^{q-1} - 1 = -1$ car $p \mid q$, donc, $P \wedge P' = 1$, donc les racines de P sont simples. Comme $\deg P = q$ et que K est un corps de décomposition pour P , $|L| = q$.
 De plus, car $K = p$ (car extension de $\mathbb{Z}/p\mathbb{Z}$ de car. p), donc le sous-corps premier de K est $\mathbb{Z}/p\mathbb{Z}$, et par minimalité du sous-corps premier, $\mathbb{Z}/p\mathbb{Z} \subseteq L$. Par définition du corps de décomposition, $L = K$.

3) Montrons l'unicité.

Soit L' un corps de card. q , on sait que $\text{car } L' = p$, donc $\mathbb{Z}/p\mathbb{Z} \subseteq L'$ (si $\text{car } L' \neq p$, alors, $\text{car } L' = \tilde{p}$ premier, donc, $\tilde{p}^m = p^n$, pas possible). Puis, $|L'|^q = q-1$ donc $\forall x \in L'$, $x^{q-1} = 1$ i.e. $x^q = x$. Donc, L' est un autre corps de décomposition de P , donc par unicité du corps de décomposition, $L' \cong K$.

Théorème: Soit p premier, et $n \geq 1$. On note $q = p^n$, alors $\mathbb{F}_q$ est isomorphe à $\mathbb{F}_p[X]/\langle \pi \rangle$ où π est un polynôme irréductible de degré n de $\mathbb{F}_p[X]$. De plus, il existe toujours un tel polynôme.

Preuve: On note $\mathcal{K} = \{P \in \mathbb{F}_p[X] \mid P \text{ est irréductible de degré } n\}$.

1) Montrons qu'il existe $\pi \in \mathcal{K}$. $\mathbb{F}_q \cong \mathbb{F}_p/\langle \pi \rangle$. $\mathbb{F}_q^*$ est cyclique, donc ξ est générateur, de sorte que $\mathbb{F}_q = \{0, 1, \xi, \dots, \xi^{q-2}\}$. Alors, $\mathbb{F}_q \subseteq \mathbb{F}_p[\xi]$ et pour tout $P \in \mathbb{F}_p[X]$, $P(\xi) \in \mathbb{F}_q$ (car $\mathbb{F}_p \subseteq \mathbb{F}_q$ et est un anneau). Donc, $\mathbb{F}_q = \mathbb{F}_p[\xi] = \mathbb{F}_p(\xi)$ car ξ est alg. sur $\mathbb{F}_p$ ($X^q - X$ est annulateur). Soit μ le polynôme minimal de ξ . Alors, $\mathbb{F}_p(\xi)$ est le corps de rupture de μ sur $\mathbb{F}_p$. Par unicité de ce dernier, $\mathbb{F}_q = \mathbb{F}_p(\xi) \cong \mathbb{F}_p[X]/\langle \mu \rangle$.

et on a que $\deg \mu = [\mathbb{F}_q : \mathbb{F}_p] = n$.

2) Il. $\forall \pi \in \mathcal{K}$, $\mathbb{F}_q \cong \mathbb{F}_p[X]/\langle \pi \rangle$. Soit $\pi \in \mathcal{K}$. $\mathbb{F}_p[X]/\langle \pi \rangle$ est le corps de rupture de π sur $\mathbb{F}_p$.

Donc c'est un corps et:

$$|\mathbb{F}_p[X]/\langle \pi \rangle| = |\mathbb{F}_p|^{\dim_{\mathbb{F}_p}(\mathbb{F}_p[X]/\langle \pi \rangle)} = p^{\deg \pi} = p^n = q$$

on conclut par unicité du théorème précédent.

1) **Sous corps premier.** On appelle sous corps premier de K le sous corps de K engendré par 1_K . C'est le plus petit sous corps engendré par contenu dans K . On a de plus que le sous corps premier de tout corps est $\mathbb{Q}$ ou $\mathbb{F}_p$ (on peut alors définir la caractéristique du corps 0 si c'est $\mathbb{Q}$, p si c'est $\mathbb{F}_p$).

Preuve: Soit $\varphi: m \in \mathbb{Z} \mapsto m \cdot 1_K \in K$ un morphisme d'anneaux. $\ker \varphi$ est un idéal de $\mathbb{Z}$, et $\mathbb{Z}/\ker \varphi \cong$ sous anneau de K , donc intègre.

(1) si $\ker \varphi = \{0\}$, alors, $\mathbb{Z} \cong \mathbb{Z} \cdot 1_K$. Or, tout élément de $\varphi(\mathbb{Z} \setminus \{0\})$ est inversible dans K , donc φ se prolonge en un morphisme de corps $\psi: \mathbb{Q} \rightarrow K$ donc injectif, et tout sous corps de K contient $1_K, n \cdot 1_K$ et leurs inverses. Donc le sous corps premier de K est $\psi(\mathbb{Q}) \cong \mathbb{Q}$.

(2) si $\ker \varphi = \langle p \rangle$, alors, $\mathbb{Z}/\ker \varphi$ est intègre, donc $\langle p \rangle$ (donc p) est premier. Alors, φ induit un isomorphisme de $\mathbb{F}_p$ sur son image formée des $m \cdot 1_K$ $\forall m \in \{0, p-1\}$. Dans ce cas, le sous corps premier de K est formé des éléments, que l'on identifie à $\mathbb{Z}/p\mathbb{Z}$.

Corollaire. Soit $k \subseteq K$ deux corps, alors k et K ont même caractéristique, car leur sous corps premier est le même.

2) **Corps de rupture de $P \in K[X]$.** Il existe une extension L de K unique à isomorphisme près tq. P ait au moins une racine α dans L et que L soit le plus petit corps contenant K et α : c'est le corps de rupture de $P \in K[X]$.

Preuve:

* **existence:** On pose $L = K[X]/\langle P \rangle$. K s'injecte dans L et pour $\alpha = \pi(X)$ (projection canonique) on a $P(\alpha) = P(\pi(X)) = \pi(P(X)) = 0$. Comme X engendre $K[X]$ et π est surj, α engendre L , car π est un morphisme d'anneaux.

et $L = K(\alpha) = K[\alpha]$.

* **unicité:** Si L et L' sont deux corps de rupture de P engendrés par α et α' deux racines. Soit u le morphisme $u: \mathbb{Q} \in K[X] \mapsto \mathbb{Q}(\alpha) \in L$. Alors, $\text{Im } u = K[\alpha] = L$ et $\ker u = \langle P \rangle$. Donc (thm d'isomorphisme), $K[X]/\langle P \rangle \cong L$ et de même, $K[X]/\langle P \rangle \cong L'$. D'où le résultat.

3) **Corps de décomposition de $P \in K[X]$:** Un corps de décomposition d'un polynôme P est une extension L de K tq. P soit scindé sur L et si $\alpha_1, \dots, \alpha_n$ sont les racines de P , alors, $L = K(\alpha_1, \dots, \alpha_n)$.

* **existence:** Par récurrence sur $n = \deg P$.

Si $n = 1$, K convient.

Soit $n \geq 2$, et le résultat suppose acquis jusqu'à $n-1$ (par tout corp K). Soit $P \in K[X]$ de deg. n et L un corps de rupture de P . $L = K(\alpha)$, et $P(X) = (X - \alpha)Q(X)$ dans $L[X]$. $\deg Q \leq n-1$, donc par HR, il existe un corps de décomp. de Q sur L donné par $L(\beta_1, \dots, \beta_{n-1})$. Donc,

$L(\beta_1, \dots, \beta_{n-1}) = K(\beta_1, \dots, \beta_{n-1}, \alpha)$ convient pour P .

* **unicité:** Hautement non trivial.

Remarques:

▷ Un développement difficile, car beaucoup de choses sont à connaître. Pourtant, le rapport du jury insiste sur le fait que la construction des corps finis doit être maîtrisée...

▷ La partie motée (*) est une partie que l'on trouve dans certaines versions, c'est peu précis... Le Gogart donne une justification longue du fait que $\mathbb{F}_p[\xi] = \mathbb{F}_p(\xi)$. Si c'est clair pour vous tant mieux, sinon demandez à quelqu'un de compétent! Perso, je m'ai jamais compris...