

Leçon 141 : Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Matei Lefebvre

2025/2026

1 Polynômes irréductibles.

1.1 Définitions et premières propriétés.

[Goz09], I.3

~ 6 items.

définition polynôme irréductible | exemples | factorialité de $\mathbb{K}[X]$ | premiers résultats sur les polynômes irréductibles | contre-exemple | $\mathbb{K}[X]/(P)$ est un corps, degré

1.2 Critères d'irréductibilité.

[Goz09], I.3

~ 9 items.

racines rationnelles de $P \in \mathbb{Z}[X]$ | exemple | définition contenu | lemme de Gauss | irréductibles de $A[X]$ pour A factoriel | critère d'Eisenstein | exemple | critère de réduction modulo un idéal premier | exemple

2 Extensions de corps.

2.1 Éléments algébriques.

[Goz09], II.1 et [Per96], III.1.a

~ 13 items.

définition extension, degré | exemple | base télescopique | définition algébrique, transcendant | définition polynôme minimal | exemples | polynôme minimal est irréductible, définition degré | caractérisation éléments algébriques | définition extension algébrique : exemple : extension finie | sous-corps des algébriques | exemple : algébriques sur $\mathbb{Q}$ | définition algébriquement clos | D'Alembert-Gauss

2.2 Corps de rupture/décomposition.

[Goz09], V.1-2

~ 8 items.

définition corps de rupture | exemples | existence, unicité | critères irréductibilité polynômes | exemples | définition corps de décomposition | exemples | existence, unicité

3 Applications.

3.1 Corps finis.

[Per96], III.2 et [Goz09], VII

~ 10 items.

caractéristique | existence, unicité corps finis | groupe multiplicatif est cyclique | élément primitif
| écriture d'un corps fini comme corps de rupture | exemple | facteurs irréductibles de $X^{p^n} - X$ |
nombre de polynômes irréductibles | DEV 1 | sous-corps d'un corps fini

D1

Théorème (Algorithme de Berlekamp). Soit $P = P_1 \dots P_r \in \mathbb{F}_q[X]$ avec $P_1, \dots, P_r$ irréductibles 2 à 2 premiers entre eux. On note $S_P : \mathbb{F}_q[X]/(P) \rightarrow \mathbb{F}_q[X]/(P)$, c'est une application $\mathbb{F}_q$ -linéaire.
$$\overline{Q} \mapsto \overline{Q^q} = \overline{Q(X^q)}$$

On a alors $r = \dim(\ker(S_P - id)) = \deg(P) - \text{rg}(S_P - id)$. Si de plus $r \geq 2$ et $\overline{V} \in \ker(S_P - id) \setminus \mathbb{F}_q$, alors $P = \prod_{\alpha \in \mathbb{F}_q} \text{pgcd}(P, V - \alpha)$ est une décomposition non triviale de P .

Lemme. Soit $P \in \mathbb{F}_q[X]$, alors :

1. $\text{pgcd}(P, P') = 1 \Leftrightarrow P$ n'a pas de facteur carré.
2. $\text{pgcd}(P, P') = P \Leftrightarrow \exists R \in \mathbb{F}_q[X], P = R^p$.
3. Si on est dans aucun des deux cas précédents, alors $P = \text{pgcd}(P, P') \cdot \frac{P}{\text{pgcd}(P, P')}$ est une décomposition non triviale de P .

(L'algo suivant est sûrement à mettre en annexe).

Algorithme (de factorisation d'un polynôme $P \in \mathbb{F}_q[X]$). Soit $P \in \mathbb{F}_q[X]$.

. Si P est constant :

. Fin de l'algorithme.

. Sinon :

. On calcule $D := \text{pgcd}(P, P')$.

. Si $D = 1$:

. On applique l'algorithme de Berlekamp à P .

. Si $D = P$:

. On trouve $R \in \mathbb{F}_q[X]$ tq $P = R^p$ (il suffit de mettre les coefficients de P à la puissance p^{n-1}).

. On applique l'algorithme à R .

. Sinon :

. On applique l'algorithme à D et $\frac{P}{D}$.

[BMP05], V.3.2 et [Dem09], IX.6

3.2 Cyclotomie.

[Goz09], VI.1

~ 10 items.

définition racines primitive (dans $\mathbb{C}$), cardinal | obtention des autres racines primitives | définition
corps cyclotomique | définition polynôme cyclotomique | $X^n - 1 = \prod_{d|n} \Phi_d$ | $\Phi_n \in \mathbb{Z}[X]$ | formule pour

Théorème. 1. Soit $n \geq 3$ et $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ sa décomposition en facteurs premiers. Alors, $e^{\frac{2i\pi}{n}}$ est constructible si et seulement si les $e^{\frac{2i\pi}{p_j^{\alpha_j}}}$ sont constructibles ;

2. $\forall \alpha \in \mathbb{N}$, $e^{\frac{2i\pi}{2^\alpha}}$ est constructible ;

3. Soient $p \geq 3$ un nombre premier et $\alpha \in \mathbb{N}^*$. Alors, $e^{\frac{2i\pi}{p^\alpha}}$ est constructible si et seulement si $\alpha = 1$ et p est un nombre premier de Fermat (i.e. de la forme $p = 2^m + 1$).

[Car01], IV.2 et X.4.1

3.3 Algèbre linéaire.

[Gou21], IV.5.problème 22

~ 3 items.

définition endomorphisme semi-simple | DEV 2 | réduction des endomorphismes semi-simples pour $\mathbb{K} = \mathbb{R}$

D2

Théorème. Soit f un endomorphisme d'un $\mathbb{K}$ -espace vectoriel de dimension finie et μ_f son polynôme minimal. Alors, f est semi-simple si et seulement si μ_f n'a pas de facteur carré.

[Gou21], IV.5.Problème 22

~ 3 items.

Références

- [Per96] D. PERRIN. *Cours d'algèbre (Agrégation)*. ELLIPSES, 1996. ISBN : 9782729855529.
- [Car01] J.C. CARREGA. *Théorie des corps : La règle et le compas*. HERMANN, 2001. ISBN : 9782705614492.
- [BMP05] V. BECK, J. MALICK et G. PEYRÉ. *Objectif Agrégation*. H&K, 2005. ISBN : 9782914010924.
- [Dem09] M. DEMAZURE. *Cours d'algèbre*. CASSINI, 2009. ISBN : 9782842251277.
- [Goz09] I. GOZARD. *Théorie de Galois : Niveau L3-M1*. ELLIPSES, 2009. ISBN : 9782729842772.
- [Gou21] X. GOURDON. *Les Maths en tête - Algèbre et probabilités - 3e édition*. ELLIPSES, 2021. ISBN : 9782340059597.