Algèbre II

Un ensemble compréhensible de notes de cours

Auteur
Yago Iglesias

4 novembre 2024

Table des matières

1 Introduction

Ce document est un recueil de notes de cours sur l'algèbre niveau L3. Il est basé sur les cours de M. Régis de la Bretèche à Université Paris Cité, cependant toute erreur ou inexactitude est de ma responsabilité. Si bien Yago IGLESIAS est l'auteur de ce document, il n'est pas le seul contributeur. En effet, de nombreux étudiants ont participé à la rédaction de ce document. Leurs noms sont disponibles dans la section contributeurs du répertoire GitHub. Un remerciement particulier à Erin Le Boulc'h, Gabin Dudillieu et Mathusan Selvakumar pour leur participation active à la rédaction de ce document.

Le document est structuré en 3 parties. La première partie est consacrée aux anneaux et aux polynômes. La deuxième partie est consacrée aux corps et aux extensions de corps. Et la dernière partie porte sur la réduction des endomorphismes.

Toute erreur signalée ou remarque est la bienvenue. Sentez-vous libres de contribuer à ce document par le biais de GitHub, où vous pouvez trouver le code source de ce document et une version pdf à jour. Si vous n'êtes pas familiers avec *Git* ou LaTeX, vous pouvez toujours me contacter par mail.

2 Anneaux de Polynômes

2.1 Construction formelle

Définition 2.1 (Anneau de polynômes)**.** Soit A un anneau commutatif. On note $A^{\mathbb{N}}$ l'ensemble des suites presque nulles d'éléments de A. On munit $A^{\mathbb{N}}$ d'une structure d'anneau en posant :

- $(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}}$
- $(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}}$ où $c_n = \sum_{k=0}^{n} a_k b_{n-k}$

On note $A[X]$ l'anneau commutatif (proposition à montrer si besoin) $A^{\mathbb{N}}$.

Définition 2.2 (Anneau intègre)**.** Un anneau $(A, +, \cdot)$ est intègre s'il est commutatif, non trivial et pour tout $x, y \in A$,

$$xy = 0 \implies x = 0 \quad \text{ou} \quad y = 0$$

Proposition 2.3. *Soit A un anneau commutatif. Soient $P, Q \in A[X]$. Alors $\deg(PQ) \leq \deg(P) + \deg(Q)$. De plus, si A est intègre, $\deg(PQ) = \deg(P) + \deg(Q)$.*

Démonstration. Soient $P = a_n x^n + \ldots + a_0$ et $Q = b_m x^m + \cdots + b_0$ avec $a_n \neq 0$ et $b_m \neq 0$. Ainsi, $\deg(P) = n$ et $\deg(Q) = m$. Le terme de plus haut degré dans PQ vient de $a_n X^n \cdot b_m X^m = a_n \cdot b_m X^{n+m}$. Par conséquent, $\deg(PQ) \leq n + m = \deg(P) + \deg(Q)$.
Si A est intègre, alors $a_n b_m \neq 0$ si $a_n \neq 0$ et $b_m \neq 0$. Ainsi :

$$\deg(PQ) = n + m = \deg(P) + \deg(Q).$$

□

Corollaire 2.4. *$A[X]$ intègre $\iff$ A intègre.*

Démonstration. — $\Rightarrow$ C'est immédiat, car un sous-anneau d'un anneau intègre est intègre.

— $\Leftarrow$ Soient $P, Q \in A[X]$ non nuls. On a donc $\deg(P) \geqslant 0$ et $\deg(Q) \geqslant 0$.
Mais alors, on a :

$$\deg(PQ) = \deg(P) + \deg(Q) \geqslant 0, \text{ par la proposition précédente}$$

Ce qui entraîne que PQ est non nul, d'où l'intégrité de $A[X]$.

□

Exemple 2.1.1. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, avec p premier, est intègre, donc $\mathbb{F}_p[X] = \mathbb{Z}/p\mathbb{Z}[X]$ est intègre.

2.2 Division euclidienne

Proposition 2.5 (Division euclidienne). *Soit A un anneau commutatif. Soient $P, Q \in A[X]$ avec $Q \neq 0$ et Q a un coefficient dominant inversible. Alors il existe un unique couple $(U, R) \in A[X] \times A[X]$ tel que :*

— $P = UQ + R$

— $\deg(R) < \deg(Q)$

Proposition 2.6. *Soit K un corps. $K[X]$ est un anneau euclidien et donc principal.*

Démonstration. On commence par noter que K est intègre et donc $K[X]$ aussi. Soit I un idéal non nul de $K[X]$. On note $\mathcal{P}$ l'ensemble des degrés des polynômes de I :

$$\mathcal{P} = \{\deg(P) \mid P \in I\}$$

$\mathcal{P}$ est non vide et minoré par 0. Donc il existe $d \in \mathcal{P}$ tel que d est minimal. On note Q un polynôme de I de degré d. Soit $P \in I$. On réalise la division euclidienne de P par Q :

$$\exists (U, R) \in K[X] \times K[X] \mid P = UQ + R \quad \text{et} \quad \deg(R) < \deg(Q)$$

On a que $R = P - UQ \in I$ car I est un idéal. Comme $\deg(R) < d$ et par définition d est minimal pour tous les éléments non nuls, on a que $R = 0$. Donc $P = UQ$ et donc $I =< Q >$. □

Exemple 2.2.1 (Exemple pathologique). $\mathbb{Z}[X]$ n'est pas principal. En effet, on peut prendre $I =< 2, X >$.

Théorème 2.7 (Propriété universelle de l'anneau de polynômes). *Soient A et B des anneaux commutatifs. On considère $f : A \to B$ un morphisme d'anneaux. Soit $b \in B$. Alors il existe un unique morphisme d'anneaux $\tilde{f} : A[X] \to B$ tel que $\tilde{f}(X) = b$ et $\tilde{f}_{|A} = f$.*

Définition 2.8 (Evaluation). Soit A un anneau commutatif et $a \in A$. On note $\phi_x : A[X] \to A$ le morphisme d'anneaux induit par l'automorphisme trivial de A en utilisant la propriété universelle de l'anneau de polynômes 2.7.

Ce morphisme correspond à l'évaluation en x : $\phi_x(P) = P(x)$.

Définition 2.9 (Polynôme à plusieurs variables / à n indéterminés). Soit A un anneau commutatif. On définit par récurrence sur $n \in \mathbb{N}^*$ l'anneau $A[X_1, \ldots, X_n]$:

- $A[X_1] = A[X]$
- $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$

Définition 2.10 (Anneau factoriel). Soit A un anneau commutatif. On dit que A est factoriel si :

- A est intègre
- Tout élément non nul de A est inversible ou est produit d'un nombre fini d'éléments irréductibles ($a = up_1 \ldots p_n$ avec u inversible et p_i irréductible)
- La décomposition est unique à l'ordre près et à l'association près.

Proposition 2.11 (Admis). *Soit A un anneau factoriel. Alors $A[X]$ est factoriel.*

Proposition 2.12. *Soit A un anneau intègre tel que tout élément de $A \setminus \{A^\times\}$ est produit d'un nombre fini d'éléments irréductibles, alors les assertions suivantes sont équivalentes :*

1. *A est factoriel*

2. *Si $p \in A$ est irréductible, alors l'idéal $< p >$ est premier*
3. *Soient $a, b, c \in A \setminus \{0\}$ tels que $a \mid bc$ et a et b sont premiers entre eux. Alors $a \mid c$ (lemme de Gauss).*

Démonstration. 3) $\Longrightarrow$ 2) :
Soit $p \in A$ irréductible. On a que $< p > \neq A$ car p est irréductible, donc pas inversible. Si p divise ab et ne divise pas a, alors p et a sont premiers entre eux car p est irréductible. Donc tout diviseur commun de p et de c est soit inversible soit associé à p. Donc p divise c. Donc d'après 3), $< p >$ est premier.

$$ab \in < p > \quad et \quad a \notin < b > \Longrightarrow b \in < p > \Longrightarrow < p > \text{ premier}$$

□

Démonstration. 2) $\Longrightarrow$ 1) :
Soit $\mathcal{P}$ un système de représentants des irréductibles.

$$u \cdot \prod_{p \in \mathcal{P}} p^{n_q}(\text{divisible par } q^{n_q} \in < q >) = v \cdot \prod_{p \in \mathcal{P}} p^{m_q}(\text{divisible par } q^{m_q} \in < q >)$$

S'il existe $q \in \mathcal{P}$ tel que $m_q > n_q$, alors q divise $u \cdot \prod_{p \neq q} p^{n_q}$ $(\in < q >)$, ce qui n'est pas possible par 2).

□

Démonstration. 1) $\Longrightarrow$ 3) :
A est factoriel. Si a divise x, on écrit a, b, c sous la forme $u \cdot \prod_{p \in \mathcal{P}} p^{v_{p(x)}}$. On a alors $\forall p \in \mathcal{P}$, $v_p(a) \leqslant v_p(b) \leqslant v_p(c)$ car a divise bc. Si $v_p(a) \geqslant b$, alors $v_p(b) = 0$. Pour $H_p \in \mathcal{P}$, $v_p(a) \leqslant v_p(c)$, donc a divise c, qui vérifie 3).

□

Définition 2.13 (pgcd). Le plus grand commun diviseur est défini ainsi :

$$d = pgcd(a, b), \quad \text{tout diviseur de } a \text{ et de } b \text{ divise } d$$

et d divise a et b

Remarque 2.2.1. *Si K est un corps, il y a un seul idéal non nul, qui est K et donc tous les $pgcd$ valent 1.*

Proposition 2.14. *Si A est un anneau factoriel, alors deux éléments non nuls de A admettent un $pgcd$ défini à un facteur inversible près.*

Démonstration. Soit $\mathcal{P}$ un système de représentants des irréductibles de A. On écrit

$$a = u \prod_{p \in \mathcal{P}} p^{n_p} \quad \text{où} \quad u \in A^\times$$

$$b = v \prod_{p \in \mathcal{P}} p^{m_p} \quad \text{où} \quad v \in A^\times$$

$$pgcd(a,b) = \prod_{p \in \mathcal{P}} p^{\min(m_p, m_p)} \quad \text{où} \quad u \in A^\times$$

à facteur $\omega \in A^\times$ près □

Exemple 2.2.2.

$$A = \mathbb{Z}, \quad pgcd(-6,2) = 2 \quad \text{ou} \quad -2$$

Théorème 2.15 (admis). *A principal $\implies$ A factoriel*

Exemple 2.2.3 (Anneau factoriel non principal). $\mathbb{Z}[X]$ est un anneau factoriel, mais non principal.

Proposition 2.16. *Dans un anneau principal on écrit*

$$< a, b > \; = \; < d >, \quad \textit{où} \quad d = pgcd(a,b)$$

Définition 2.17. Soit A un anneau factoriel, et $P \in A[X]$, le contenu (notée $c(P)$) d'un polynôme P est le $pgcd$ de ses coefficients non nuls. P est dit primitif si $c(P) = 1$ (ou $c(P) \in A^\times$)

Exemple 2.2.4.

$$A = \mathbb{Z}, \quad c(3X+2) = 1$$

$$A = \mathbb{Z}, \quad c(14X^2 + 24X + 2) = 2$$

Lemme 2.18 (Lemme de Gauss). *Pour tout $P, Q \in A[X]$ on a*

$$c(PQ) = c(P)c(Q)$$

à facteur inversible près.

Démonstration. Commençons par montrer que P et Q primitifs implique PQ primitif.
Sinon, il existe un irréductible $p \in A$ tel que p divise tous les coefficients de PQ.
Supposons que P et Q sont primitifs. On pose $P = \sum a_i X^i$ et $Q = \sum b_j X^j$ On a que

$$D = \{i \mid p \text{ ne divise pas } a_i\}$$

n'est pas vide, car si D est vide alors $\forall\ i, p \mid a_i \implies p|c(P)$. On note i_0 (resp. j_0) l'indice minimal tel que a_{i_0} (resp. b_{j_0}) ne soit pas divisible par p et :

$$\begin{aligned} \forall i,\, 0 \leq i \leq i_0\,, \quad p \mid a_i \\ \forall j,\, 0 \leq j \leq j_0\,, \quad p \mid b_j \end{aligned}$$

On a donc que le coefficient de degré $i_0 + j_0$ de PQ est :

$$\begin{aligned} PQ_{i_0+j_0} &= \sum_{k=0}^{i_0+j_0} a_k b_{i_0+j_0-k} \\ &= a_{i_0} b_{j_0} + \text{un multiple de } p \end{aligned}$$

Si $k \neq i_0$, soit $k \leq i_0 - 1$ soit $i_0 + j_0 - \leq j_0 - 1$ et donc $p \mid a_k b_{i_0+j_0-k}$
Donc le coefficient de degré $i_0 + j_0$ de PQ n'est pas divisible par p ce qui contredit les hypothèses. Donc on a P et Q primitif $\implies$ PQ primitif.
Dans le cas général

$$\begin{aligned} c(PQ) &= c\left(\frac{P}{c(P)}\frac{Q}{c(Q)}c(P)c(Q)\right) \\ &= c\left(\frac{P}{c(P))}\frac{Q}{c(Q)}\right)c(P)c(Q) \\ &= c(P)c(Q) \end{aligned}$$

car $\frac{P}{c(P)}$ est un polynôme primitif de $A[X]$ et $pgcd(ka, kb) = kpgcd(a, b)$ et donc $c(kP) = kc(P)$. □

Définition 2.19 (Corps de fraction). Soit A un anneau commutatif intègre. On introduit

$$E = \{(a, b) \in A \times A \mid b \neq 0\}$$

On munit E de 2 lois internes :

- $\times : (a, b) \times (a', b') = (aa', bb')$.
- $+ : (a, b) + (a', b') = (ab' + ba', bb')$.

On définit une relation d'équivalence :

$$(a, b) \backsim (a', b') \iff ab' = a'b$$

Alors $K/\backsim$ (les classes d'équivalence de E sur $\backsim$) est un corps et A se plonge dans K avec :

$$\phi : a \in A \mapsto \overline{(a, 1)}$$

Remarque 2.2.2. *$A, K = Frac(A)$. Le plongement $\phi : A \to K$ nous permet d'identifier A avec $\phi(A)$ de sorte que $A \subset K$. Ainsi un polynôme $P \in A[X]$ peut être vu comme un polynôme dans $K[X]$.*

Exemple 2.2.5. — $Frac((Z)) = \mathbb{Q}$

— $Frac((K[X])) = K(X)$

Exemple 2.2.6. $2X^2 + 2X + 2$ n'est pas irréductible dans $\mathbb{Z}[X]$ mais il est irréductible dans $\mathbb{Q}[X]$ car $2 \in \mathbb{Q}^\times$.

Théorème 2.20 (Clasification des irréductibles). *Lemme de Gauss*
Soit A un anneau factoriel de corps de fraction K. Alors les irréductibles de $A[X]$ sont de deux types :

- *Les polynômes constants $P = p$, p irréductibles dans A.*
- *Les polynômes primitifs de deg ≥ 1 qui sont irréductibles dans $K[X]$.*

Démonstration. On va traiter en premier les polynômes constants et après le reste.

- Comme $A[X]^\times = A^\times$ si P est constant, i.e. $P = p \in A$, alors

$$P \text{ inversible } \iff p \text{ inversible dans } A$$

- Montrons les deux implications pour les polynômes non constants.
  - Si P primitif avec deg ≥ 1 dans $A[X]$ et irréductible dans $K[X]$, on écrit $P = QR$, avec $Q, R \in A[X]$.
    On a que $c(P) = c(Q)c(R) \in A^\times$ donc $c(Q) \in A^\times$ et $c(R) \in A^\times$.
    La relation $P = QR \in K[X]$ implique que Q ou R sont de degré 0 (car P primitif).
    Comme ils sont primitifs, Q ou $R \in A^\times \implies Q$ ou $R \in A[X]^\times$ donc P est irréductible dans $A[X]$.
  - Soit P irréductible de $A[X]$ avec deg ≥ 1.
    Alors $c(P)$ divise P donc $c(P) \in A^\times \implies P$ primitif.
    Montrons maintenant que P est irréductible dans $K[X]$.
    On écrit $P = QR$ avec $Q, R \in K[X]$. On choisit $a, b \in A$ tel que $aQ \in A[X]$ et $bR \in A[X]$. On a donc que

$$\begin{aligned} abP &= aQbR \\ c(aQ)c(bR) &= c(abP) \\ &= ab \end{aligned}$$

$$P = \frac{aQ}{c(aQ)} \frac{bR}{c(bR)}$$

    donc P produit de deux éléments de $A[X]$, donc, comme P irréductible dans $A[X]$, on a :

$$\deg(Q) = 0 \text{ ou } \deg(R) = 0$$

□

2.3 Critères d'irréductibilité dans $K[X]$

Proposition 2.21. *Un polynôme de degré 1 dans $K[X]$ est irréductible dans $K[X]$.*

Démonstration. Si $P = QR$, on a $1 = \deg(P) = \deg(Q) + \deg(R)$, donc Q ou R est de degré 0, donc c'est un inversible. □

Théorème 2.22 (d'Alambert-Gauss). *Les irréductibles de $\mathbb{C}[X]$ sont les polynômes de degré 1.*

Démonstration. Tout polynôme $P \in \mathbb{C}[X]$ de degré ≥ 1 admet $\alpha \in \mathbb{C}$ racine et donc $X - \alpha$ divise P. □

Proposition 2.23. *Soit $P \in \mathbb{R}[X]$ irréductible alors :*

- *Soit* $\deg P = 1$.
- *Soit* $\deg P = 2$ *et P n'admet pas de racines dans $\mathbb{R}$.*

Démonstration. $P(\alpha) = 0 \implies P(\bar{\alpha}) = 0$ sur $\mathbb{C}\backslash\mathbb{R}$, $(X-\alpha)(X-\bar{\alpha}) = X^2-(\alpha+\bar{\alpha})X+\alpha\bar{\alpha} \in \mathbb{R}[X]$ et divise P. □

Proposition 2.24. *Soit $P \in K[X]$ de degré 2 ou 3, P est irréductible dans $K[X] \iff P$ n'admet pas de racines dans K.*

Exemple 2.3.1 (contre-exemple). $K = \mathbb{R}, P = (X^2+1)^2$ n'a pas de racines dans $\mathbb{R}$, mais il n'est pas irréductible ($\deg P = 4 > 3$).

Exemple 2.3.2. $K = \mathbb{Q}, P = (x^2 - 2)$ n'a pas de racines, donc irréductible dans $\mathbb{Q}[X]$, mais il a des racines sur $\mathbb{R}[X]$, donc pas irréductible sur $\mathbb{R}[X]$.

Théorème 2.25 (Critère d'Eisenstein). *Soit A un anneau factoriel, P un polynôme de $A[X]$ de degré ≥ 1, p un irréductible de A. On écrit $P = \sum_{i=0}^{n} a_i X^i$ avec $a_n \neq 0$. Si on a les trois propriétés suivantes :*

- *p ne divise pas a_n*
- *p divise a_k $\forall$ $k < n$*
- *p^2 ne divise pas a_0*

Alors P est irréductible dans $K[X]$(avec K corps des fractions).

Exemple 2.3.3. $P(X) = X^5 + 2X^4 + 2024X + 6 \in \mathbb{Q}[X]$. On a que P est 2-Eisenstein et donc irréductible.

Corollaire 2.26. *Si de plus P est primitif de $A[X]$, alors P est irréductible dans $A[X]$.*

Démonstration. Quitte à diviser par $c(P)$, on peut supposer P primitif et de degré ≥ 2.
Si P n'est pas irréductible, il s'écrit $P = RQ$, avec $R, Q \in A[X]$ de degré > 0 et non inversibles.
On écrit

$$Q = b_s X^s + \cdots + b_0$$

et

$$R = c_r X^r + \cdots + c_0$$

Soit $B = A/ < p >$ intègre et on a $A[X]/pA[X] \simeq B[X]$.
Dans $B[X]$, on a $\bar{P} = \bar{R}\bar{Q}$, or d'après les hypothèses on a $\bar{P} = \bar{a}_n X^n$ et $\bar{a_n} \neq 0$ dans B.
Donc $\bar{b_s} \neq 0$ et $\bar{c_r} \neq 0$ et $\bar{b_s}\bar{c_r} = \bar{a_n}$ dans B, et $\bar{Q}$ et $\bar{R}$ sont de degré > 0 et $\bar{Q}\bar{R} = \bar{a_n} X^n$ dans $B[X]$.
On voit la relation $\bar{a_n} X^n = \bar{Q}\bar{R}$ dans $B[X]$ qui est principal et donc factoriel.
Et donc $\bar{Q}$ et $\bar{R}$ ont pour seul facteur irréductible X dans $(Frac\ B)[X]$.
Donc en particulier p divise b_0 et c_0, donc p^2 divise $b_0 c_0 = a_0$, ce qui est absurde. □

Exemple 2.3.4. $A = \mathbb{Z}$, p premier,
$Q \in \mathbb{Z}[X] \implies \bar{Q} \in \mathbb{Z}/p\mathbb{Z}[X]$.
$\bar{Q}$ est défini par la classe $mod\ p$ de ses coefficients.

$$X \mid \bar{Q} \text{ dans } \mathbb{Z}/p\mathbb{Z}[X] \iff p \mid Q(0) \text{ dans } \mathbb{Z}$$

$$\begin{array}{rcl} \mathbb{Z}[X] & \to & \mathbb{Z}/p\mathbb{Z}[X] \\ \sum a_i X^i & \mapsto & \sum \bar{a}_i X^i \end{array}$$

Exemple 2.3.5. $\Phi_p(x) = x^{p-1} + \cdots + x + 1 = \frac{x^p - 1}{x - 1} \in \mathbb{Z}[X]$. On applique le critère d'Eisenstein à $\Phi_p(X + 1)$.

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{k=1}^{p} \binom{p}{k} X^{k-1} = \sum_{k=0}^{p-1} \binom{p}{k+1} X^k$$

- Le coefficient dominant de X^{p-1} est $\binom{p}{p} = 1$ et p ne divise pas 1.
- Pour tout $k < p-1$, le coefficient de X^k est $\binom{p}{k+1} = \frac{p!}{(k+1)!(p-k-1)!} = p \underbrace{\frac{(p-1)!}{(k+1)!(p-k-1)!}}_{\in A}$. p divise $p! = k!(p-k)!\binom{p}{k}$ et p premier à $k!(p-k)!$, donc p divise $\binom{p}{k}$.
- $\binom{p}{1} = p$ et p^2 ne divise pas p.

Donc $\Phi_p(X+1)$ est irréductible dans $\mathbb{Q}[X]$ et donc $\Phi_p(X)$ est irréductible dans $\mathbb{Q}[X]$.

Proposition 2.27. *Soit $P \in \mathbb{Z}[X]$ primitif de coefficient dominant non multiple de p, où p est un premier. Si $\bar{P}$ est irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, alors P est irréductible dans $\mathbb{Z}[X]$.*

Démonstration. On suppose par l'absurde P primitif, irréductible sur $\mathbb{Z}/p\mathbb{Z}[X]$ et non irreductible sur $\mathbb{Z}[X]$
Alors il existe $Q, R \in \mathbb{Z}[X]$ non constants, tels que $P = QR$ et donc $\bar{P} = \bar{Q}\bar{R}$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. De plus, on a :

- $\deg Q = \deg \bar{Q}$
- $\deg R = \deg \bar{R}$

car leurs coefficients dominants ne divisent pas p.
Donc $\bar{P} = \bar{Q}\bar{R} \implies \bar{P}$ n'est pas irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$, ce qui contredit l'hypothèse. □

2.4 Fonctions polynomiales

Définition 2.28 (Fonction polynomiale). Soit $P \in A[X]$, $P = \sum_{i=0}^{n} a_i X^i$.
On appelle fonction polynomiale associée à P la fonction $\tilde{P} : A \to A$ définie par :

$$\tilde{P}(x) = \sum_{i=0}^{n} a_i x^i$$

Exemple 2.4.1. $A = \mathbb{Z}/p\mathbb{Z}$, $P = X^p - X$, avec p premier. Alors

$$\tilde{P}(x) = x^p - x = 0 \quad \text{(petit théoreme de Fermat)}$$

Donc $\tilde{P}$ est nulle sur $\mathbb{Z}/p\mathbb{Z}$ mais P n'est pas nul dans $\mathbb{Z}/p\mathbb{Z}[X]$.

Proposition 2.29. *Soient P, Q deux polynômes de $A[X]$.*

- $\tilde{P} + \tilde{Q} = \widetilde{P+Q}$
- $\tilde{P} \cdot \tilde{Q} = \widetilde{P \cdot Q}$

Et l'application $P \mapsto \tilde{P}$ est un morphisme d'anneaux de $A[X]$ dans l'anneau des applications polynomiales. (En général il n'est pas injectif : voir exemple ci-dessus).

Définition 2.30 (Polynôme composé). Soit $P = \sum_{i=0}^{n} a_i X^i \in A[X]$ un polynôme de $A[X]$ et $Q \in A[X]$.
On appelle le polynôme composé de P par Q le polynôme

$$P(Q) = a_n Q^n + a_{n-1} Q^{n-1} + \cdots + a_0$$

(On remplace l'indéterminé X par le polynôme Q).

Proposition 2.31 (Admis). $\widetilde{P(Q)} = \tilde{P} \circ \tilde{Q}$

Par soucis de simplification, on va noter $P(a)$ au lieu de $\tilde{P}(a)$.

Définition 2.32 (Racine d'un polynôme). Soit $P \in A[X]$.
On dit que $a \in A$ est une racine de P si et seulement si $P(a) = 0$.

Proposition 2.33.

$$P(a) = 0 \iff (X - a) \mid P \quad \textit{dans} \quad A[X]$$

Démonstration. — Si $P = (X - a)Q$, avec $Q \in A[X]$, alors $P(a) = 0$.
— Réciproquement, si $P(a) = 0$

$$\begin{aligned} P(X) &= \sum_{i=0}^{n} b_i X^i \\ &= \sum_{i=0}^{n} b_i (X)^i - P(a), \quad \text{car} \quad P(a) = 0 \\ &= \sum_{i=0}^{n} b_i (X^i - a^i) \end{aligned}$$

On a que $X^i - a^i = (X - a)(X^{i-1} + X^{i-2}a + \cdots + Xa^{i-2} + a^{i-1})$.
Donc $X - a$ divise P.

□

Définition 2.34 (Multiplicité d'une racine). On dit que $a \in A$ est une racine de P de multiplicité m si et seulement si $(X-a)^m \mid P$ et $(X-a)^{m+1} \nmid P$.

Proposition 2.35. *Soit A est un anneau intègre, alors $P \in A[X]$ admet au plus $\deg(P)$ racines distinctes dans A.*
Si $A = \mathbb{C}$ l'inégalité est une égalité.

Démonstration. On montre par récurrence sur $n = \deg(P)$ que $\sum_{a \in A} m_p(a) \leq n$, où $m_p(a)$ est la multiplicité de a dans P.

— Initialisation : $n = 0$, $P = a_0 \in A$, $a_0 \neq 0$. Alors P n'a pas de racines dans A.
— Hérédité : Supposons que $\sum_{a \in A} m_p(a) \leq n$. Soit $P \in A[X]$ de degré $n + 1$.
  — Premier cas, P n'a pas de racines dans A. Alors $\sum_{a \in A} m_p(a) = 0 \leq n + 1$.

— **Deuxième cas,** il existe $b \in A$ tel que $P(b) = 0$. Alors il existe $Q \in A[X]$ tel que $P = (X - b)Q$ et $\deg(Q) = n$. De plus

$$m_P(a) = \begin{cases} m_Q(a) + 1 & \text{si } a = b \\ m_Q(a) & \text{sinon} \end{cases}$$

et donc $\sum_{a \in A} m_P(a) = \sum_{a \in A} m_Q(a) + 1 \leq n + 1$.

On a montré donc le résultat par récurrence.

□

Corollaire 2.36. *Si A est intègre et possède un nombre infini d'éléments, alors les polynômes de $A[X]$ sont entièrement déterminés par leur fonctions polynomiales associées.*

Définition 2.37 (Dérivée d'un polynôme). Soit $P \in A[X]$, $P = \sum_{i=0}^{n} a_i X^i$.

On appelle dérivée de P le polynôme $P' = \sum_{i=1}^{n} i a_i X^{i-1}$.

Et on définit par récurrence $P^{(k)} = (P^{(k-1)})'$ et $P^{(0)} = P$.

Proposition 2.38. *On a la relation suivante :*

$$(PQ)' = P'Q + PQ'$$

Lemme 2.39. *Soit A un anneau intègre, $P \in A[X]$ et $a \in A$. Alors :*

$$m_p(a) = n \implies P^{(k)}(a) = 0, \forall\, 0 \leq k \leq n - 1$$

Démonstration. On démontre le résultat par récurrence sur n, la multiplicité de a dans P.

— Initialisation : Pour $n = 1$, $X - a \mid P$ et donc $P(a) = 0$

— Posons n tel que c'est vrai pour tout polynôme de multiplicité n. Soit P tel que $m_p(a) = n + 1$. Il existe $Q \in A[X]$ tel que $P = (X - a)^{n+1} Q$.

$$P' = (n+1)(X-a)^n Q + (X-a)^{n+1} Q' = (X-a)^n((n+1)Q + (X-a)Q')$$

Comme $Q(a) \neq 0$, on applique l'hypothèse de récurrence à P et on obtient que

$$\forall k \leq n - 1 \quad (P')^{(k)}(a) = P^{(k+1)}(a) = 0$$

□

Proposition 2.40 (Admis). *Soit A un anneau de caractéristique 0, alors on a une formule de Taylor exacte pour les polynômes.*

$$\forall a \in A, \quad P(X) = \sum_{k=0}^{n} \frac{P^{(k)}(a)}{k!} (X - a)^k$$

pour tout $n \geq \deg(P)$.

2.5 Classification des idéaux premiers de $A[X]$, avec A anneau principal

Théorème 2.41. *Soit A un anneau principal. Alors les idéaux premiers non nuls de $A[X]$ sont les idéaux de la liste suivante :*

- $\mathfrak{p}_\pi =< \pi >$ *où π est un élément irréductible de A.*
- $\mathfrak{p}_f =< f >$*, où $f \in A[X]$ est un polynôme irréductible de degré ≥ 1.*
- $\mathfrak{m}_{\pi,f} =< \pi, f >$*, où π est un élément irréductible de A et $f \in A[X]$ unitaire, irréductible modulo π.*

Les deux premiers sont les idéaux principaux engendrés par un irréductible de $A[X]$.
De plus,

- $\mathfrak{p}_\pi$ *n'est pas maximal.*
- *Si A possède une infinité d'éléments irréductibles deux à deux disjoints non associés, alors p_f est premier mais pas maximal.*
- $\mathfrak{m}_{\pi,f}$ *est maximal.*

Rappel 2.5.1 (Irréductibilité). — *Si π est un élément irréductible de A, alors $A/ < \pi >$ est un corps parce que dans un anneau principal l'idéal engendré par un élément irréductible est maximal.*

- *Soit $f \in A[X]$ et $\bar{f}$ la classe de f dans $A/ < \pi > [X] = A[X]/ < \pi >$.*
  alors f irréductible modulo π signifie que $\bar{f}$ est irréductible dans $A/ < \pi > [X]$.

Rappel 2.5.2. *Si f est un polynôme primitif de $A[X]$ de coefficient dominant inversible modulo π, et $\bar{f}$ est irréductible dans $A/ < \pi > [X]$, alors f est irréductible dans $A[X]$.*

Démonstration. — Si π est un irréductible de A. Soit $g \in A[X]$ et on note $\bar{g} \in (A/ < \pi >)[X]$ la classe de g modulo π. On rappelle

$$A[X]/ < \pi > \cong (A[X]/ < \pi > A[X])$$

Comme A est principal, $A/ < \pi >$ est un corps et donc $(A/ < \pi >)[X]$ est un anneau intègre (qui n'est pas un corps car les éléments inversibles sont des polynômes constants). Donc $< \pi >$ est un idéal de $A[X]$ premier mais pas maximal.

- Soit $f \in A[X]$ de dégré ≥ 1 et irréductible. A principal $\implies A$ factoriel $\implies A[X]$ factoriel. Tout élément irréductible de $A[X]$ engendre un idéal premier.
  Si de plus A possède une infinité d'éléments irréductibles

deux à deux disjoints non associés, alors il existe $\pi \in A$ irréductible de A tel que π ne divise pas le coefficient dominant de f.
Alors $< f > \subset < \pi, f >$, et c'est une inclusion stricte.
En effet, si on avait $\pi \in < f >$ alors

$$\exists g \in A[X] \quad \pi = fg$$

ce qui n'est pas possible quand on regarde les degrés
Montrons que $< \pi, f > \neq A[X]$. Supposons que $< \pi, f >= A[X]$, autrement dit, il existe $g, h \in A[X]$ tels que $\pi g + fh = 1$.
$\bar{f}\bar{g} = 1$ dans $(A/ < \pi >)[X]$.
Comme $\bar{f}$ est inversible dans $(A/ < \pi >)[X]$ et comme $A/ < \pi >$ est intègre on a que $\deg \bar{f} = 0$.
Comme π ne divise pas le coefficient dominant de f, on a $\deg \bar{f} = \deg f = 0$, ce qui contredit $\deg f \geq 1$.
Donc $< \pi, f > \neq A[X]$ et $\mathfrak{p}_f = < f >$ est un idéal premier mais pas maximal.

— Soit π irréductible de A, f unitaire de $A[X]$ irréductible modulo π.

$$A[X] \longrightarrow A/ < \pi > [X] \longrightarrow (A/ < \pi > [X])/ < f >$$

$$A[X] \xrightarrow{\phi} (A/ < \pi > [X])/ < f >$$

Le morphisme ϕ est surjectif de noyau $< \pi, f >$.

$$A[X]/\mathfrak{m}_{\pi,f} \cong (A/ < \pi > [X]/ < \bar{f} >)$$

Et donc $A/ < \pi > [X]$ est principal. A est principal donc $< \pi >$ est maximal donc $A/ < \pi >$ est un corps. Comme $A/ < \pi >$ est un corps donc $(A/ < \pi >)[X]$ est principal.
Comme $\bar{f}$ est un irréductible de $(A/ < \pi >)[X]$, on a que $A/ < \pi > [X]/ < \bar{f} >$ est un corps.
Donc $A[X]/\mathfrak{m}_{\pi,f}$ est un corps, donc $\mathfrak{m}_{\pi,f}$ est maximal.

Réciproquement, on choisit $\mathfrak{p}$ un idéal non nul de $A[X]$ qui est premier.
$\mathfrak{p} \cap A$ est un idéal de A premier. Comme A est principal, soit $\mathfrak{p} \cap A = \{0\}$, soit il existe π irréductible de A tel que $\mathfrak{p} \cap A = < \pi >$.

— Supposons que $\mathfrak{p} \cap A = < \pi >$.
On prend $\bar{\mathfrak{p}}$ l'image de $\mathfrak{p}$ dans $A/ < \pi > [X]$ qui est principal.
$\bar{\mathfrak{p}}$ est un idéal premier de l'anneau principal $A/ < \pi > [X]$.

— Soit $\bar{\mathfrak{p}} = \{0\} \implies \mathfrak{p} = < \pi >$.
— Soit $\bar{\mathfrak{p}}$ est engendré par un polynôme unitaire et irréductible de $A/ < \pi > [X]$.

$$\bar{\mathfrak{p}} = < \bar{f} >$$

f est un polynôme unitaire de $A[X]$ tel que $\bar{f}$est irréductible.
Donc il existe $g \in \mathfrak{p}$ telle que $\bar{g} = \bar{f}$.

$$\exists h \in A[X] \quad f = g + \pi hk$$

Comme $\pi \in \mathfrak{p}$, on a $f \in \mathfrak{p}$. Donc $\mathfrak{m}_{\pi,f} \subset \mathfrak{p} \subsetneq A$ donc $\mathfrak{m}_{\pi,f} = \mathfrak{p}$.

— Supposons que $\mathfrak{p} \cap A = \{0\}$.
On choisit f un élément non nul de $\mathfrak{p}$ de degré minimal et par hypothèse, $\deg f \geq 1$.
On écrit $f = \alpha f_0$, avec $f_0 \in A[X]$ primitif et $\alpha \in A$.
Nous avons donc que $\alpha \in \mathfrak{p}$ ou $f_0 \in \mathfrak{p}$.
Or $\alpha \notin \mathfrak{p}$ car $\mathfrak{p} \cap A = \{0\}$, donc $f_0 \in \mathfrak{p}$.
Supposons $g \in \mathfrak{p}$ non nul, alors $\deg g \geq \deg f \geq 1$. On écrit $g = hf + r$, avec $h \in K[X]$, ou K est le corps des fractions de A et $r \in K[X]$ de degré $< \deg f_0$. (Division euclidienne dans $K[X]$). On a $h \neq 0$ par minimalité du degré de f_0. On aurait sinon $g = r$ et $\deg r < \deg f_0$, ce qui est absurde.
On choisit $d \in A$ tel que dh et df_0 soient dans $A[X]$.

$$dr = \underbrace{d}_{\in A}\underbrace{g}_{\in \mathfrak{p}} - \underbrace{dh}_{\in A[X]}\underbrace{f_0}_{\in \mathfrak{p}} \in \mathfrak{p}$$

$$dg = f_0 hd \quad \text{et} \quad c(dg) = c(f_0)c(dh) = c(dh) = dc(g)$$

donc $h \in A[X]$ car $g = f_0 h$ et donc $\mathfrak{p} =< f_0 >$.

□

2.6 Fractions rationelles

Définition 2.42. On écrit tous les éléments de $K(X)$ sous la forme $\frac{P}{Q}$ avec $P, Q \in K[X]$ et $Q \neq 0$.

Théorème 2.43 (Décomposition en éléments simples). *Soit K un corps. toute fraction rationelle $F = \frac{P}{Q} \in K(X)$ admet une décomposition comme somme d'éléments simples, c'est-à-dire comme la somme d'un polynôme $T \in K[X]$ (appelé partie entière de F\) et de fractions $\frac{J}{H^k}$ où $J, H \in K[X]$, H irréductible, $k \geq 1$ et $\deg J < \deg H$.*

De plus si $Q = H_1^{k_1} \cdots H_q^{k_q}$ et P et Q premiers entre eux, alors

$$F = \frac{P}{Q} = T + F_1 + \cdots + F_q$$

Où $F_i = \frac{J_{i,1}}{H_i} + \frac{J_{i,2}}{H_i^2} + \cdots + \frac{J_{i,n_i}}{H_i^{n_i}}$

3 Corps

Définition 3.1. Un corps est un anneau commutatif dans lequel tout élément non nul de $K^* = k \setminus \{0\}$ est inversible.

Définition 3.2. La caractéristique de K est l'entier n tel que le noyau du morphisme d'anneaux

$$\begin{aligned} \mathbb{Z} &\to K \\ 1 &\mapsto 1_K \end{aligned}$$

soit $\mathbb{Z}/n\mathbb{Z}$, notée $car\ K$.

Exemple 3.0.1. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sont des corps de caractéristique 0.

- Lorsque p est premier, $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z}(T)$(corps des fractions) est un corps pour tout p. Notons que $\mathbb{Z}/p\mathbb{Z}(T)$ est infini.
- $\mathbb{Q}[i] = \{a + bi, \quad \text{où} \quad a, b \in \mathbb{Q}\} = Frac(\mathbb{Z}[i])$ est corps de $car\ 0$

3.1 Corps et espaces vectoriels

Définition 3.3. Soit K un corps. Une extension de K est un corps L tel que K soit un sous corps de L.

Remarque 3.1.1. *Si L est une extension de K, (noté L/K), alors L est muni ipso facto d'une structure de K-espace vectoriel via la loi $\times$ dans L.*
En effet, la loi externe définissant la multiplication par un scalaire (élément de K) est la loi interne de multiplication dans L.
D'autre part, si $\phi : K \to L$ est un morphisme de corps, il est injectif :
Le noyau de ϕ est un idéal de K. Comme K est un corps, ses seuls idéaux sont $\{0\}$ et K.
On note qu'il ne peut pas être K car $\phi(1_K) = 1_L$.
Alors on peut identifier K à $\phi(K)$. L est une extension de $\phi(K)$. On étend la définition précédente en disant que L est une extension de K.

Exemple 3.1.1. $K(T)$ est une extension de K.

Définition 3.4. Soit L une extension de dimension finie sur K. Alors la dimension de ce K-espace vectoriel est un entier supérieur à 0 qu'on appelle le degré de L sur K que l'on note $[L : K]$. On dit dans ce cas que L est fini sur K.

Théorème 3.5 (de la base télescopique)**.** *Soit M un corps, L un sous corps de M et K un sous corps de L.*

Alors lorsque $(e_i)_{i\in I}$ *est une base de* L *sous* K *et* $(f_i)_{i\in I}$ *est une base de* M *sous* L*, alors la famille* $(e_if_j)_{(i,j)\in I\times J}$ *est une base de* M *sous* K*.*

Exemple 3.1.2. $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$ est une extension sur $\mathbb{Q}$ de degré 2.
$M = \{x+iy \mid x,y\in\mathbb{Q}(\sqrt{2})\}$ est une extension de $\mathbb{Q}(\sqrt{2})$ de degré 2.
M est une extension de $\mathbb{Q}$ de dimension 4 et une base est $\{1,i,\sqrt{2},i\sqrt{2}\}$.

Démonstration. — Montrons que (e_if_j) est libre.
Soient $\lambda_{i,j}\in K$ tels que

$$\sum_{i,j\in I\times J}\lambda_{i,j}e_if_j = 0$$

et $(\lambda_{i,j})$ est une famille presque nulle. Alors on a

$$\sum_{j\in J}\left(\sum_{i\in I}\lambda_{i,j}e_i\right)f_j$$

(f_j) est une famille libre de M sous L, ce qui implique que pour tout $j\in J$.

$$\sum_{i\in I}\lambda_{i,j}e_i = 0$$

La liberté de la famille (e_i) sous K implique que pour tout $j\in J$ et tout $i\in I$, $\lambda_{i,j}=0$.

— Montrons que (e_if_j) est génératrice de M sur K.
La famille f_j est génératrice de M sur L.
Soit $x\in M$, $\exists x_j$ une famille presque nulle de L telle que $x=\sum_{j\in J}x_jf_j$.
La famille e_i est génératrice de L sur K.
Pour tout $x_j\neq 0$, $\exists(\lambda_{i,j})_{i\in I}$ presque nulle telle que $x_j=\sum_{i\in I}\lambda_{i,j}e_i$.
Pour tout j tel que $x_j=0$, on choisit $\lambda_{i,j}=0$.
On a $x=\sum_{(i,j)\in I\times J}\lambda_{i,j}e_if_j$, avec $(\lambda_{i,j})$ une famille presque nulle.

□

Corollaire 3.6 (important)**.** *Si* L/K *est fini et* M/L *est fini, alors* M/K *est fini et*

$$[M:K] = [M:L][L:K]$$

Définition 3.7. On considère L/K une extension de corps et $\alpha\in L$.

— On note $K[\alpha]$ le sous-anneau de L engendré par K et α. C'est aussi l'ensemble des $P(\alpha)$ avec $P \in K[X]$.
— $K(\alpha)$ le sous corps de L engendré par K et α. C'est aussi l'ensemble des $F(\alpha)$ où $F \in K(X)$.

Définition 3.8. Soit L/K une extension de corps et $\alpha \in L$.
On a un morphisme d'anneaux et de K-espaces vectoriels :

$$\begin{aligned} \phi : K[X] &\to L \\ P &\mapsto P(\alpha) \end{aligned}$$

— Si ϕ est injectif, alors $K[\alpha] \cong K[X]$ et $K(\alpha) \cong K(X)$. On dit que α est transcendant sur K.
— Si ϕ est non injectif, on note π le générateur de $\ker \phi$. On dit que α est algébrique sur K et on note π le polynôme minimal de α sur K. Ce polynôme est unique et unitaire.

Remarque 3.1.2. *Bien noter que les notions d'éléments algébriques ou transcendants dépendent du corps de base K. Tout élément de L est algébrique sur L.*
Notons que π est irréductible sur K. Comme L est intègre, alors si le produit de deux polynômes de $K[X]$ s'annule en α, alors l'un d'eux s'annule en α.

Exemple 3.1.3. — i est algébrique sur $\mathbb{Q}$ de polynôme minimal X^2+1, $L = \mathbb{C}, K = \mathbb{Q}$.
— Si $P \in K[X]$ unitaire tel que $P(\alpha) = 0$, alors P est le polynôme minimal de α si et seulement si P est irréductible sur K.

Remarque 3.1.3. *Le nombre d'éléments de $\mathbb{C}$ algébriques sur $\mathbb{Q}$ est dénombrable. Donc il y a une infinité d'éléments transcendants sur $\mathbb{Q}$.*
e est transcendant sur $\mathbb{Q}$.

Proposition 3.9. *Soit L/K une extension de corps et $\alpha \in L$.*
Il y a équivalence entre les assertions suivantes :

— *α est algébrique sur K*
— $K[\alpha] = K(\alpha)$
— *$K[\alpha]$ est un K-espace vectoriel de dimension finie.*

Si on a l'une de ces assertions, alors l'entier $[K(\alpha) : K]$ est le degré du polynôme minimal de α sur K et on l'appelle le degré de α sur K.

Démonstration. — $1 \implies 2$
Si α algébrique sur $K[\alpha] \cong K[X]/(\pi)$ et π est un irréductible de $K[X]$ on a que $K[X]/(\pi)$ est un corps.
$K[X]$ est un corps qui est égal à son corps des fractions.

— Réciproquement, α est transcendant sur K. $K[\alpha] \cong K[T]$ qui n'est pas un corps, donc on n'a pas $K[\alpha] = K(\alpha)$.

— $1 \implies 3$
Si π est un polynôme minimal de α sur K, alors $K[\alpha] \cong K[X]/(\pi)$ qui est un K-espace vectoriel de dimension le degré de π. Ceci utilise la division euclidienne dans $K[X]$:
On a que $1, \bar{X}, \ldots, \bar{X}^{\deg \pi - 1}$ est une famille génératrice de $K[X]/(\pi)$.
On prend $P \in K[X]$ et on fait la division euclidienne de P par π : $\exists Q, R \in K[X]$ tels que $P = Q\pi + R$ avec $\deg R < \deg \pi$ et $R(\bar{X}) = P(\bar{X})$.
S'il existe P de degré $< \deg \pi$ tel que $P(\alpha) = 0$, alors π divise P et donc $P = 0$. Ainsi la famille $(1, \bar{X}, \ldots, \bar{X}^{\deg \pi - 1})$ est libre.

— Réciproquement,
Si α est transcendant sur K, le K-espace vectoriel $K[\alpha]$ est isomorphe a $K[X]$ qui est de dimension infinie.

□

Définition 3.10. Une extension L/K est dite algébrique si tout élément de L est algébrique sur K.

Remarque 3.1.4. *Ainsi, toute extension finie est algébrique.*
Soit L/K finie et $\alpha \in L$, $K[\alpha] \subset L$ et donc c'est un espace vectoriel de dimension finie. Donc d'après la proposition précédente, α est algébrique sur K.

Théorème 3.11. *Soit L/K une extension de corps.*
On note M l'ensemble des éléments de L qui sont algébriques sur K.

— *M est un sous corps de L.*

— *Tout élément qui est algébrique sur M est dans M. On dit que M est la clôture algébrique de L dans K.*

— *Si L est algébriquement clos, M est algébriquement clos. On dit que M est la clôture algébrique de K.*

Exemple 3.1.4. $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$.

Exemple 3.1.5. $\mathbb{C}$ n'est pas une clôture algébrique de $\mathbb{Q}$.
Si on note $\bar{\mathbb{Q}}$ l'ensemble des éléments de $\mathbb{C}$ algébriques sur $\mathbb{Q}$, on a que $\bar{Q} \neq \mathbb{C}$. On peut montrer que $\bar{\mathbb{Q}}$ est dénombrable.

Démonstration. — $0, 1 \in M \implies K \subset M$

— Montrons que si $x \in M, x \neq 0,\ x^{-1} \in M$ et $-x \in M$.
Si $x \in M,\ x \in L$ et $P \in K[X],\ P \neq 0$ tel que $P(x) = 0$.
$x^{-1} \in L$ et $-x \in L$. Si $d = \deg P$ on a $Q(X) = X^d P(1/x) \in K[X]$ et $Q(x^{-1}) = 0$.
$S(x) = P(-x) \in K[x]$ et $S(-x) = 0$.
Ici on a construit explicitement les polynômes Q et S à partir de P.
Alors x^{-1} et $-x \ \in M$

— Montrons que si $x, y \in M,\ x + y$ et $x * y \in M$.
$K[x]$ est un K-espace vectoriel de dimension finie,
y est algébrique sur K, donc a fortiori $K(x) = K[x]$, donc $K[x][y]$ est de dimension finie.
$x + y$et $x * y \in K[x][y]$ donc $K[x + y]$ et $K[x * y]$ sont des K-espaces vectoriels de dimension finie car ce sont des sous espaces vectoriels de $K[x][y]$

Alors M est un sous-corps de L

— Soit $\alpha \in L$ algébrique sur M.
Il existe $P \in M[X]$

$$P = X^n a_n + \cdots + a_0$$

tel que $P(\alpha) = 0$. Comme chaque a_j est algébrique sur K, on a par itération que $K' = K[a_0, \cdots, a_{n-1}]$ est un corps qui est une extension finie de K.
$K'[\alpha]$ est une extension finie de K' puisque $P(\alpha) = 0$ et$P \in K'[X]$.
f

$$[K[\alpha] : K] = [K[\alpha] : K'] [K' : K] < \infty$$

donc α est algébrique sur K et donc $\alpha \in M$.

— Si $P \in M[X]$ non constant, il admet une racine $\alpha \in L$ (car L est algébriquement clos).
α est algébrique sur $M \Longrightarrow \alpha$ algébrique sur K $\Longrightarrow \alpha \in M$ par le point précédent.
M est dont algébriquement clos.

□

Remarque 3.1.5. *Si $\alpha \in M$, $K[X]$ est un K-espace vectoriel mais la clôture algébrique sur K n'est pas forcement un K-espace vectoriel de dimension finie.*

Remarque 3.1.6. $\bar{\mathbb{Q}}$ *est dénombrable car* $\mathbb{Q}$ *est dénombrable.*
$\mathbb{C}$ *n'est pas dénombrable ce qui démontre l'existence de nombres transcendants sur* $\mathbb{Q}$.

3.2 Corps de rupture et corps de décomposition

Étant donnés K un corps et $P \in K[X]$, on cherche une extension L de K telle que P ait une racine dans L ou toutes ses racines

dans L.

Définition 3.12. Soit P un polynôme irréductible dans $K[X]$. On dit qu'une extension L de K est un corps de rupture de P sur K s'il existe une racine $\alpha \in L$ de P telle que $L = K[\alpha] = K(\alpha)$. Ainsi, un corps de rupture est une extension dans laquelle P a une racine et qui est minimale pour cette propriété.

Théorème 3.13. *Pour tout polynôme irréductible P de $K[X]$ il existe un corps de rupture L. De plus, L est unique à un K-isomorphisme près.*

Remarque 3.2.1. *L'unicité n'est pas vraie si P est non irréductible.*

$$P(X) = (X^2 - 2)(X^2 - 3) \in \mathbb{Q}[X]$$

$\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(\sqrt{3})$ ne sont pas $\mathbb{Q}$ isomorphes car $\mathbb{Q}(\sqrt{3})$ ne contient pas les racines de $X^2 - 2$.
En effet, $\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \mid a, b \in \mathbb{Q}\}$

$$(a + b\sqrt{2})^2 = a^2 + 2ab\sqrt{3} + 3b \neq 2 \quad \textit{sauf si} \quad ab = 0$$

Si $b = 0$, $a = \sqrt{2} = \frac{p}{q}$ ce qui n'est pas possible.
Si $a = 0$, $b\sqrt{3} = \sqrt{2} \Longrightarrow \sqrt{6} \in \mathbb{Q}$ ce qui n'est pas possible non plus.

Démonstration. — Comme P est irréductible sur K on a :

$$L = K[X]/ < P > \quad \text{est un corps car } K[X] \text{est principal}$$

L est une extension de K donc le plongement :

$$\begin{aligned} \phi : K &\to L \\ \lambda &\mapsto \bar{\lambda} \end{aligned}$$

est un morphisme de corps.
Si on note $\alpha = \bar{X}$ la classe de X dans L. $P(\alpha) = 0, L = K[\alpha]$ donc L est un corps de rupture de P sur K.

— Si L est un corps de rupture de P dans K
Soit α' tel que $L' = K[\alpha']$ et $P(\alpha') = 0$, alors l'application

$$\begin{aligned} \phi : K[X] &\to L' \\ Q &\mapsto Q(\alpha') \end{aligned}$$

et surjective de noyau $< P >$ ($\ker \phi \supset < P >$)
Par un théorème de factorisation, on obtient un isomorphisme entre L et L' qui est un K-isomorphisme.

□

Exemple 3.2.1. $\mathbb{C}$ est le corps de rupture de X^2+1 dans $\mathbb{R}$.
$\mathbb{Q}(i)$ est le corps de rupture de X^2+1 dans $\mathbb{Q}$.
$\mathbb{Q}(\sqrt[3]{2})$ est le corps de rupture de X^3-2 dans $\mathbb{Q}$.
Mais c'est aussi le cas de $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$, avec $j=e^{\frac{2i\pi}{3}}$. De plus, $\mathbb{Q}(\sqrt[3]{2})\subset\mathbb{R}$, ce qui n'est pas le cas des autres.

Lorsque P est de degré 2, il n'y a qu'un seul corps de rupture. Si α est une racine de $P=X^2+aX+b$, alors $-a-\alpha$ est l'autre racine.

Remarque 3.2.2 (Important). *Si L est un corps de rupture pour P dans K, alors :*

$$[L:K]=\deg P$$

$P(\alpha)=0$, et donc $\left\{1,\alpha,\alpha^2,\ldots,\alpha^{\deg P-1}\right\}$ est une base de L sur K (génératrice grâce à la division euclidienne).

Définition 3.14. Soient K un corps et $P\in K[X]$ (on ne suppose pas forcément P irréductible).
On dit qu'une extension L de K est un corps de décomposition pour P sur K si et seulement si L vérifie les propriétés suivantes :

- P est scindé sur L (produit de polynômes de degré 1).
- L est engendré comme corps (ou comme anneau) par les racines de P sur K.

Ainsi un corps est décomposition est une extension minimale de K pour laquelle P est scindé.

Théorème 3.15. *Pour tout $P\in K[X]$, il existe un corps de décomposition pour P sur K qui est unique à K-isomorphisme près.*

Démonstration. — Existence :
On procède par récurrence sur le degré de P.

- Pour $\deg P\leq 1$, c'est évident : $L=K$
- Soit Q un facteur irréductible sur K de P. Comme Q est irréductible, il admet un corps de rupture sur K, $K'=[x]$, $Q(x)=0$.
  On écrit $P(X)=(X-x)P_1(X)$, avec $P_1\in\mathbb{K}'[X]$. On a $\deg P_1=\deg P-1$.
  On peut alors appliquer l'hypothèse de récurrence à P_1 sur K'.
  Il existe $L=K(x_2,\cdots,x_n)$ tel que P_1 est scindé sur L et $x_2,\cdots,x_n$ sont des racines de P. On a donc $L=K(x,x_2,\cdots,x_n)$ est bien un corps de décomposition pour P sur K :

— Unicité :
On démontre par recurrence sur le degré de P l'énoncé

suivant :
"Si $\phi : K \to K'$ est un isomorphisme de corps et P un polynôme de $K[X]$ et L et L' sont des corps de décomposition pour P (respectivement pour $\phi(P)$) sur K (respectivement sur K'), alors il existe un morphisme de corps $\psi : L \to L'$ qui prolonge ϕ" On obtiendra le résultat voulu en prenant $\phi = id_K$.

Si P est scindé, on a $L = K, L' = K'$ et l'affirmation est évidente.

Sinon, on considère $\alpha \in L$ une racine de P dans L/K de polynôme minimal Q (on sait que $Q \mid P$).
$\phi(Q)$ admet une racine $\alpha' \in L'$ et $K[\alpha]$ et $K'[\alpha']$ sont des corps de rupture sur Q(respectivement $\phi(Q)$) sur K (respectivement sur K').

On prolonge ϕ en $\phi_1 : K[\alpha] \to K'[\alpha']$ en posant $\phi_1(\alpha) = \alpha'$.

Soit $R \in K[X]$, $\phi_1(R(\alpha)) = \phi(R)(\alpha')$ ce qui a bien un sens puisque les polynômes minimaux de α et α' sur K et K' sont Q et $\phi(Q)$ respectivement.

On a $P(X) = (X - \alpha)P_1$ et $\phi(P)(X) = (X - \alpha'\phi_1(P_1)$, on a juste à appliquer l'hypothèse de récurrence à P_1 et $\phi_1(P_1)$ sur $K[\alpha]$ et $K'[\alpha']$.
On obtient bien $\psi : L \to L'$ qui prolonge ϕ_1 et donc ϕ.

□

Remarque 3.2.3. *L'unicité est "meilleure" que pour les corps de rupture.*
Si L et L' sont deux corps de décomposition pour P sur K,et que $l \subset M$ et $l' \subset M$, avec M/K une extension de corps, alors

$$L = L' = K(x_1, \ldots, x_n)$$

où $x_1, \ldots, x_n$ sont les racines de P dans M.

4 Corps finis

Un corps fini est un corps qui a un nombre fini d'éléments.
Sa caractéristique est forcément p premier. Si c'était 0, alors $\mathbb{Z}$ s'injecterait dans K et $\mathbb{Z}$ serait infini.

K peut être vu comme une extension de $\mathbb{F}_p$ via le morphisme :

$$\begin{aligned} \mathbb{F}_p &\to K \\ \bar{1} &\mapsto 1_K \end{aligned}$$

K est en particulier un espace vectoriel de dimension finie $K : \mathbb{F}_p$ et $|K| = p^{[K:\mathbb{F}_P]}$

Ici $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \times)$, p premier. A isomorphisme près, il y a un seul corps à p éléments.

$\mathbb{F}_p = (\mathbb{Z}/, \mathbb{Z}+, \times)$ est un corps si et seulement si n est premier.

Théorème 4.1. *Soit $q = p^n$, avec p premier et $n \geq 1$. Alors il existe un corps de cardinal q unique à isomorphisme près. C'est le corps de décomposition pour $X^q - X$ sur $\mathbb{F}_p$. On le note $\mathbb{F}_q$.*

Rappel 4.0.1 (Utile pour la preuve). *Si α annule P et sa multiplicité est supérieure ou égale à 2, alors $P'(\alpha) = 0$:*

$$P(X) = (X-\alpha)^2 Q(X) \implies P'(X) = 2(X-\alpha)Q(X) + (X-\alpha)^2 Q'(X) = 0$$

Démonstration. — Existence :

Soit K le corps de décomposition de $X^q - C$ sur F_p.

On note K' l'ensemble des racines dans K de $X^q - X$.

K' est en fait un corps : $0, 1 \in K'$. Si $x, y \in K''$.

Montrons que $(x+y)^q = x^q + y^q = x + y$.

Pour montrer l'identité précédente, on observe que pour tout > 0 et pour tout $x, y \in K$ on a $(x+y)^{p^k} = x^{p^k} + y^{p^k}$. Cela se montre par récurrence grâce à la formule $(x+y)^p = x^p + y^p$.

$p \mid \binom{p}{k}$ lorsque $1 \leq k \leq p-1$ aussi $(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p$

$x \in K'$, alors $-x$ est aussi dans K'. En effet, si $carK = 2$, $-x = x - 2x = x$.

Si $carK$ est impaire, $(-x)^q = -x^q = -x$.

Évidemment $x, y \in K' \implies xy \in K'$, car $(x * y)^q = x^q y^q = xy$

$x \in K' x \neq 0 \implies \frac{1}{x} \in K'$.

Alors K' est un sous corps de K.

Donc par la définition de corps de décomposition $K' = K$.

La dérivée de $X^q - X$ est $qX^{q-1} - X$ et $qX^{q-1} - 1 = 1$

Donc toutes les racines du polynôme sont simples et il y en a exactement q. K est bien un corps de cardinal q.

— Unicité :

On considère L un corps de cardinal q.

On sait que $\forall x \in L \setminus \{0\}, \quad x^{q-1} = 1$ (théorème de Lagrange

appliqué au groupe multiplicatif $L \setminus \{0\}$ et cardinal $q-1$), donc :

$$\forall x \in L, \quad x^q - x = 0$$

$X^q - X$ est scindé dans L (car il a q racines distinctes).
L contient un corps de décomposition pour $X^q - X$ sur $\mathbb{F}_p$.
Autrement dit, un K_1 qui est isomorphe à K (d'après les propriétés de décomposition).
$L_1 \subset L$ et $|K_1| = q = |L| \implies K_1 = L \cong K$.

□

Exemple 4.0.1. — $P = X^2 + X + 1$ est irréductible sur $\mathbb{F}_2$ et

$$\mathbb{F}_2[X]/ < x^2 + x + 1 > \cong F_4$$

On prend α une racine de $x^2 + x + 1$.

$$\mathbb{F}_2[X]/ < x^2 + x + 1 > = \{a + \alpha b \mid a, b \in \mathbb{F}_2\} \cong \mathbb{F}_4$$

La table de multiplication :

$*$	**0**	**1**	α	$1+\alpha$
0	**0**	**1**	α	$1+\alpha$
1	**1**	**1**	α	$\alpha+1$
α	α	α	$\alpha+1$	**1**
$1+\alpha$	$1+\alpha$	α	**1**	α

Car on a car $\mathbb{F}_4 = 2$ et donc $\alpha^2 = (\alpha^2+\alpha+1)+\alpha+1 = P(\alpha)+\alpha+1 = \alpha+1$.
De plus $\alpha(\alpha+1) = \alpha^2 + \alpha = \alpha + 1 + \alpha = 1$.

— $x^3 + x + 1$ est irréductible sur $\mathbb{F}_2$ et $\mathbb{F}_2[X]/ < x^3 + x + 1 > \cong F_6$.

— $\mathbb{F}_3[X]/ < x^2 + 1 > \cong F_9$

Exercice 4.0.1. Si K est un corps fini et $P \in K[X]$ irréductible sur K, alors le corps de rupture de P sur K est aussi un corps de décomposition pour P sur K.

Remarque 4.0.1. *$\mathbb{F}_{p^n}$ est une extension de $\mathbb{F}_{p^m}$ si et seulement si m divise n.*
Ainsi $\mathbb{F}_8$ n'est pas une extension de $\mathbb{F}_4$.

Démonstration. — $[F_{p^n} : F_{p^m}] = d \in \mathbb{N}$
$p^n = |F_{p^n}| = |F_{p^m}|^d = p^{md} \implies n = md$.

— Réciproquement, si $m \mid n$, on écrit $n = md$
On a $X^{p^m-1} - 1$ divise $X^{p^n-1} - 1$ et $X^{p^m} - X$ divise $X^{p^n} - X$
Toutes les racines de $X^{p^m} - X$ sont racines de $X^{p^n} - X$, donc $F_{p^m} \subset F_{p^n}$.

□

Remarque 4.0.2 (Morphisme de Frobenius). *Soit K un corps de caractéristique $p>0$ et $\psi : K \to K$ définie par $\psi(x) = x^p$.*
Alors ψ est un morphisme de corps, donc injectif. Si K est fini, alors ψ est un automorphisme de corps.
Ainsi $\psi(x+y) = (x+y)^p = x^p + y^p, \forall x, y \in K$.
De plus $\{x \in K \mid x^p = x\} = \mathbb{F}_p$.
Cela fournit une famille de morphismes $K \to K$:

$$\psi, \quad \underbrace{\psi \circ \cdots \circ \psi}_{n \text{ fois}} = \psi^n : \begin{cases} K \to K \\ x \mapsto x^{p^n} \end{cases}$$

Pour $P \in F_q[X], \quad q = p^n$, on a $\psi(P(x)) = P(\psi(x))$, car F_q est de caractéristique p.

4.1 Polynômes irréductibles sur un corps fini

Soit $I(n,q)$ le plus petit polynôme unitaire de degré n irréductible sur $\mathbb{F}_q$.

Théorème 4.2. *Pour tout q puissance d'un nombre premier et $n \geq 1$ on a $I(n,q) > 0$.*

Plus précisément :

$$I(n,q) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d$$

où μ est la fonction de Möbius :

$$\mu(k) = \begin{cases} 0 & \text{s'il existe } l \text{ premier tel que } l^2 \text{ divise } k \\ (-1)^r & \text{si } k = p_1 \cdot p_2 \cdot \ldots \cdot p_r \text{ avec } p_i \text{ premiers distincts} \end{cases}$$

Lemme 4.3.

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{sinon} \end{cases}$$

Démonstration. On peut se ramener à n sous facteur carré $n = p_1 \ldots p_r$ avec p_i premiers distincts.

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{j=0}^{r} (-1)^j \#\{d \mid n : \text{nombre de facteurs premiers de } d \text{ est } j\} \\ &= \sum_{j=0}^{r} (-1)^j \binom{r}{j} \\ &= (1-1)^r = 0 \quad \text{si} \quad r > 1 \end{aligned}$$

□

Lemme 4.4. *Soient f et g des applications de $\mathbb{N}^*$ dans $\mathbb{C}$, alors :*

$$\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} f(d) \iff \forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} \mu(\frac{n}{d}) g(d)$$

Démonstration. Si $g(n) = \sum_{d|n} f(d)$ alors :

$$\begin{aligned}
\sum_{d|n} \mu(\frac{n}{d}) g(d) &= \sum_{d|n} \mu(\frac{n}{d}) \sum_{l|d} f(l) \\
&= \sum_{l|n} f(b) \underbrace{\sum_{d|n,\ l|d}}_{d=ld',\ d'|\frac{n}{l}} \mu(\frac{n}{d}) \\
&= \sum_{l|n} f(l) \sum_{d'|\frac{n}{l}} \mu(\frac{n}{ld'}) \\
&= \sum_{l|n} f(l) \underbrace{\sum_{m|\frac{n}{l}} \mu(m)}_{0,\ \text{sauf si } l=n} \\
&= f(n)
\end{aligned}$$

□

Démonstration du théorème. Il suffit de montrer que $q^n = \sum_{d|n} dI(d,q)$.

Considérons $Q = X^{q^n} - X$ et sa décomposition en produit de polynômes irréductibles unitaires :

$$Q = P_1 \dots P_r$$

Tous les p_j sont distincts car si $P_i = P_j (i \neq j)$.

$$P_j^2 | Q \implies P_j | Q' = -1$$

Montrons que les P_j sont exactement les polynômes irréductibles unitaires dont le degré divise n. Soit P un polynôme irréductible de degré d. Supposons $d|n$. Soit x dans un corps de rupture pour P tel que $P(x) = 0$. Ce corps est de degré d sur $\mathbb{F}_q$. Il est donc isomorphe à $\mathbb{F}_{q^d}$. Donc $x^{q^d} = x$.
Avec $d|n$, on a $x^{q^n} = x$. Soit $m = kd$. Si ψ_{q^d} est le morphisme de Frobenius $x \mapsto x^{q^d}$, alors

$$\psi_{q^d}^k(x) = \psi_{q^d} \circ \dots \circ \psi_{q^d}(x) = x^{q^n} = x$$

On a $Q(x) = 0$. Comme P est le polynôme minimal de x sur $\mathbb{F}_q$, on a donc $P|Q$.

Réciproquement, si $P|Q$ de degré d.
Toute racine x de P annule Q, donc $\mathbb{F}_{q^d}$ est le corps de décomposition de $\mathbb{Q}$ qui contient $\mathbb{F}_{q^d} = F_q[x]$, donc $d|n$ (comme pour le théorème de la base télescopique, $\mathbb{F}_q \subset \mathbb{F}_{q^d} \subset \mathbb{F}_{q^n}$).

En calculant le degré de Q on en déduit que

$$q^n = \sum_i \deg P_i = \sum_{d|n} dI(d,q)$$

□

Exemple 4.1.1. $q = 2, \quad n = 4, \quad 2^4 = 16$

$$X^16 - X = X(X-1)(X^2+X+1)(X^4+X+1)(X^4+X^3+1)(X^4+x^3+x^2+x+1)$$

$$I(2,2) = \frac{1}{2}\sum_{d|2} \mu(\frac{2}{d})2^d = \frac{1}{2}(4-2) = 1$$

$$I(4,2) = \frac{1}{4}\sum_{d|4} \mu(\frac{4}{d})2^d = \frac{1}{4}(2^4 - 2^2) = 3$$

Corollaire 4.5. *Pour tout n et tout q puissance d'un nombre premier :*

$$I(n,q) > 0$$

Démonstration.

$$\begin{aligned} nI(n,q) &= \sum_{d|n} \mu(\frac{n}{d})q^d \\ &> q^n - \sum_{d|n,\quad d<n} q^d \\ &> q^n - \sum_{1\le d\le \lfloor \frac{n}{2} \rfloor} q^d \\ &= q^n - q\frac{q^{\lfloor \frac{n}{2} \rfloor} - 1}{q-1} \\ &> 0 \end{aligned}$$

□

4.2 Critères de réductibilité sur $\mathbb{Q}$ et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Pour étudier la réductibilité d'un polynôme sur $\mathbb{Q}$ on peut toujours se ramener à un polynôme sur $\mathbb{Z}$ primitif.

Proposition 4.6. *Soit $P = a_n X^n + \ldots + a_0 \in \mathbb{Z}[X]$.*
Soit p un nombre premier tel que $p \nmid a_n$.
Si $\bar{P}$,la réduction modulo p, est irréductible sur $\mathbb{F}_p$, alors P est irréductible sur $\mathbb{Q}$. De plus, si P est primitif, alors P est irréductible sur $\mathbb{Z}$.

Remarque 4.2.1. *$a \nmid b$ est essentiel : $2X^2 - X + 1$ est irréductible sur $\mathbb{F}_2$ mais réductible sur $\mathbb{Q}$, 1 est une racine.*

Remarque 4.2.2. *Ce critère est une condition suffisante mais pas nécessaire.*

Démonstration. On suppose P primitif, réductible sur $\mathbb{Q}$ et donc aussi sur $\mathbb{Z}$.
Alors il existe $R, S \in \mathbb{Q}[X]$, tels que $P = RS$

$$\exists a, b \in \mathbb{N}* \text{ tels que } aR, bS \in \mathbb{Z}[X]$$

$$abP = aRbS$$

$$c(abP) = ab = c(aR)c(vS)$$

$$P = \frac{c(aR)}{c(aR)} \frac{c(bS)}{c(bS)}$$

Modulo p $\bar{P} = \bar{Q}\bar{R}$. De plus, on a :

- $\deg Q = \deg \bar{Q}$
- $\deg R = \deg \bar{R}$

car leurs coefficients dominants ne divisent pas p.
Donc $\bar{P} = \bar{Q}\bar{R} \implies \bar{P}$ n'est pas irréductible dans $\mathbb{Z}/p\mathbb{Z}[X]$.
On a donc montré la contraposée de la proposition. □

Proposition 4.7. *Soit $P \in K[X]$ et $\deg P = n$, Si P n'a pas de racines dans toute extension de K de degré au plus $\frac{n}{2}$, alors P est irréductible sur K.*

Remarque 4.2.3. *Si $n = 2$ ou $n = 3$ ce résultat dit que si P n'a pas de racines dans K, alors P est irréductible.*

Démonstration. Soit P réductible sur K. Alors il existe Q irréductible de degré $\leq \frac{n}{2}$ qui divise P.
Soit un corps de rupture pour Q sur K.

$$[L : K] = \deg Q \leq \frac{n}{2}$$

L contient une racine de Q et donc une racine de P. □

Exemple 4.2.1. $P(X) = X^4 + 1 \in \mathbb{F}_p[X]$ avec p premier n'est pas irréductible sur $\mathbb{F}_p$ alors que X^4+1 est irréductible sur $\mathbb{Q}$.

Montrons que P a toujours une racine dans $\mathbb{F}_{p^2}$: F_{p^2} est le corps de décomposition de $X^{p^2} - X = X(X^{p^2-1} - 1)$ sur $\mathbb{F}_p$. Donc les éléments non nuls de F_{p^2} sont les racines de $X^{p^2-1} - 1$.
p est impair, donc $p^2 - 1 \equiv 0$ mod 8 car $1, 3, 5$ et 7 au carré donnent 1 modulo 8.

On choisit x une racine de $X^{p^2-1} - 1$ d'ordre 8 mais qui ne soit pas d'ordre 4.
$x^8 - 1 = 0 = (X^4 - 1)(X^4 + 1)$, donc $x^4 + 1 = 0$.
Donc P a une racine dans $\mathbb{F}_{p^2}$ et donc P est réductible sur $\mathbb{F}_p$.

5 Réductions d'endomorphisme et polynômes d'endomorphisme

E désignera un K-espace vectoriel.

5.1 Polynômes d'endomorphisme

On note $\mathcal{L}(E)$ l'ensemble des endomorphismes de E.

Définition 5.1. Soit $u \in \mathcal{L}(E)$. Pour tout polynôme $P \in K[X] = a_0 + a_1X + \ldots + a_nX^n$, on définit $P(u)$ par :

$$P(u) = a_0 Id_E + a_1 u + \ldots + a_n u^n$$

L'application $P \mapsto P(u)$ est un morphisme d'algèbres (d'anneaux) de $K[X]$ dans $\mathcal{L}(E)$.

$$(PQ)(u) = P(u) \circ Q(u)$$

Proposition 5.2. *Soit* $u \in \mathcal{L}(E)$ *et* $P, Q \in K[X]$. *Alors :* $P(u)$ *et* $Q(u)$ *commutent :* $P(u) \circ Q(u) = Q(u) \circ P(u)$

Démonstration. Grâce à la linéarité, il suffit de le montrer pour $P = X^m$ et $Q = X^n$.

$$u^m \circ u^n = u^{m+n} = u^{n+m} = u^n \circ u^m$$

□

5.2 Polynômes annulateurs et polynôme minimal

Définition 5.3. Soit $u \in \mathcal{L}(E)$ et $P \in K[X]$. On dit que P est un polynôme annulateur de u si $P(u) = 0_{\mathcal{L}(E)}$

Proposition 5.4. *Tout endomorphisme dans un espace vectoriel de dimension finie admet un polynôme annulateur non nul.*

Démonstration. $\left\{u^k \mid 0 \leq k \leq n^2\right\}$ est une famille liée car $\dim \mathcal{L}(E) = n^2$. □

Remarque 5.2.1. *Le théorème de Cayley-Hamilton nous dira que le polynôme caractéristique est un polynôme annulateur.*

Remarque 5.2.2. *Si E n'est pas de dimension finie, cela n'est pas vrai en general :*
Soit $D : K[X] \to K[X]$ l'application qui à un polynôme associe sa dérivée. Alors D n'a pas de polynôme annulateur.
Soit $Q = \sum_{i=0}^{n} a_i X^i \in K[X]$.

$$Q(D)(P) = \sum_{k=0}^{n} i a_i P^{(k)}$$

Proposition 5.5. *L'ensemble I_u des polynômes annulateurs de $u \in \mathcal{L}(E)$ est un idéal de $K[X]$. Si $I_u \neq \{0\}$, alors il admet un générateur unique appelé polynôme minimal de u et noté μ_u.*

Définition 5.6. Un endomorphisme u est dit nilpotent s'il existe $n \in \mathbb{N}$ tel que $u^n = 0_{\mathcal{L}(E)}$.
Dans ce cas, le polynôme minimal de u est de la forme X^n et on appelle n l'indice de nilpotence de u.

Remarque 5.2.3. *Si u admet un polynôme minimal μ_u de degré d, alors* $\dim K[u] = d$.

Démonstration.

$$\phi : \begin{array}{ccc} K[X] & \to & K[u] \\ P & \mapsto & P(u) \end{array}$$

$$\ker \phi = < \mu_U(u) >$$

$$K[u] \cong K[X]/ < \mu_U >$$

Donc $\dim K[u] = \deg \mu_U = d$ □

Exemple 5.2.1. Si u est une homothétie de rapport λ, autrement dit si $u = \lambda id_E$, alors $\mu_u = X - \lambda$.

Remarque 5.2.4. *On dit que p est un projecteur si et seulement si $p^2 = p$. $\mu_p = X^2 - X$ sauf si $p = id_E$ ou $p = 0_{\mathcal{L}(E)}$.*

Proposition 5.7. *Soit $u \in \mathcal{L}(E)$ admettant un polynôme minimal μ_u, alors u est inversible si et seulement si $\mu_u(0) \neq 0$*

Démonstration. □

5.3 Lemme des noyaux

5.3.1 Etude du $\ker P(u)$

Proposition 5.8. *Soient $P,$ et $Q \in K[X]$ tels que $\text{pgcd}(P,Q) = D$ et $u \in \mathcal{L}(E)$. Alors*

$$\ker P(u) \cap \ker Q(u) = \ker D(u).$$

Démonstration. — $D \mid P \implies \ker D(u) \subset \ker P(u)$
En effet, $P = RD$, $P(u)(x) = R(u)(D(u)(x)) = 0$.
Donc $D(u)(x) = 0 \implies P(u)(x) = 0$

$$\ker D(u) \subset \ker P(u) \cap \ker Q(u).$$

— Montrons l'autre inclusion.
Le théorème de Bézout affirme l'existence de U et $V \in K[X]$ tels que $U(X)P(X) + V(X)Q(X) = D(X)$.
Donc $\forall x \in E$,

$$D(u)(x) = U(u)P(u)(x) + V(u)Q(u)(x) = 0$$

Donc $x \in \ker P(u) \cap \ker Q(u) \implies x \in \ker D(u)$.

□

Corollaire 5.9. *Soit $u \in \mathcal{L}(E)$ de polynôme minimal de μ_u. Soit $P \in K[X]$.*

$$\ker P(u) = \ker D(u)$$

Où $D = \text{pgcd}(P, \mu_u)$.

Remarque 5.3.1. *Ce résultat nous permet de nous restreindre à des P tels que $P \mid \mu_u$.*

Démonstration. Par définition $\ker \mu_u(u) = E$, car $\mu_u(u) = 0_{\mathcal{L}(E)}$, donc

$$\begin{aligned} \ker P(u) &= \ker P(u) \cap E \\ &= \ker P(u) \cap \ker \mu_u(u) \\ &= \ker D(u) \end{aligned}$$

□

Corollaire 5.10. *Soit $u \in \mathcal{L}(E)$ de polynôme minimal μ_u et $P \in K[X]$ unitaire, avec $P \mid \mu_u$.*
Soit $v = u_{\restriction \ker P(u)}$.
Alors $\mu_v = P$.

Démonstration. Pour tout P, $\ker P(u)$ est stable par u.
En effet, si $x \in \ker P(u)$, alors $P(u)(x) = 0$, donc

$$\begin{aligned} P(u)(u(x)) &= (P(u) \circ u)(x) \\ &= (u \circ P(u))(x) \\ &= u(P(u)(x)) \\ &= 0_{\mathcal{L}(E)} \end{aligned}$$

Donc $u(x) \in \ker P(u)$.

Montrons que $F = \ker P(u), \quad \forall x \in F, \quad P(v(x)) = P(u)(x) = 0$.

$P(0) = 0_{\mathcal{L}(E)}$, $\mu_v \mid P$.
Prenons $Q \in K[X]$ tel que $\mu_v = QP$.
$\mu_v(u) = 0_{\mathcal{L}(E)} \implies \ker Q(u) \subset \ker P(u)$.

□

5.3.2 Lemme des noyaux

Soit $u \in \mathcal{L}(E)$.
Il permet de décomposer un espace vectoriel en somme directe d'espaces vectoriels stables par u et adaptés à la réduction de u.

Lemme 5.11 (des noyaux). *Soit (P_k) une famille de polynômes 2 à 2 premiers entre eux. Soit $u \in \mathcal{L}(E)$.*

$$\ker\left(\left(\prod_{k=1}^{N} P_k\right)(u)\right) = \bigoplus_{k=1}^{N} \ker P_k(u)$$

De plus, la projection de $\ker\left(\left(\prod_{k=1}^{N} P_k\right)(u)\right)$ sur l'un des $\ker P_j(u)$ parallèlement à la somme des autres est un polynôme en u.

Démonstration. Par récurrence sur N.

— Montrons que si P_1 et P_2 sont premiers entre eux, alors $\ker(P_1P_2)(u) = \ker P_1(u) \oplus \ker P_2(u)$.

□

5.3.3 Conséquence : Décomposition en sous espaces vectoriels stables

Soit $u \in \mathcal{L}(E)$ avec un polynôme minimal μ_u. On décompose μ_u en produit d'irréductibles :

$$\mu_u = \prod_{k=1}^{N} p_k^{\alpha_k}$$

où $\alpha_k \geq k$, les p_k sont irréductibles unitaires et 2 à 2 distincts.

Corollaire 5.12.

$$E = \bigoplus_{k=1}^{N} \ker\left(P_k^{\alpha_k}(u)\right)$$

Démonstration. La preuve consiste à utiliser le lemme des noyaux, sachant que

$$\ker \mu_u(u) = E$$

. Les sous-espaces vectoriels $\ker\left(P_k^{\alpha_k}(u)\right)$ sont stables par u. Il suffit pour réduire u de se restreindre à chacun de ces sous espaces vectoriels. □

5.4 Rappels d'algèbre linéaire

5.4.1 Déterminants

Soit $n = \dim E$, pour tout $u \in \mathcal{L}(E)$, on peut associer $\det u \in K$. Il y a plusieurs façons de le définir.

— De manière canonique : pour toute forme n linéaire alternée f sur E on a :

$$f \circ u = \det(u) * f$$

En effet, l'espace de ces formes n linéaires alternées est de dimension 1. De cette manière, f et $f \circ u$ sont proportionnelles.

On qualifie cette définition de canonique car elle ne nécessite pas le choix d'une base de E.

— Soit de manière matricielle : $\det u$ est un polynôme explicite en les coefficients de la matrice de U prise dans une base de E. Ce déterminant ne dépend pas du choix de la base.

D'après 1, $det(Id_E) = 1$.
Si u et $v \in \mathcal{L}(E)$,

$$\begin{aligned} f \circ u \circ v &= \det(u \circ v) f \\ &= \det(v) f \circ u \\ &= \det(v) \det(u) f \end{aligned}$$

Alors,

$$\det(u \circ v) = \det(u) \det(v) = \det(v \circ u)$$

En particulier, si v est inversible, alors

$$\det(v^{-1}) = (\det v)^{-1}$$

Le déterminant induit un morphisme de groupe :

$$\begin{aligned} \det(GL(E), \circ) &\to (K^\times, *) \\ u &\mapsto \det(u) \end{aligned}$$

u est inversible si et seulement si $det(u) \neq 0$

5.4.2 Polynôme caractéristique d'un endomorphisme

On apelle polynôme caractéristique de u le polynôme χ_u défini par

$$\chi_u(X) = \det(XId_e - u)$$

On fixe une base B de E, on définit $M = Mat_B u$. Dans ce cas $\chi_u(X) = \det(CI_n - M)$ (c'est un polynôme en X de degré n unitaire).
La définition de $\chi_u(X) = \det(XI_n - M)$ ne dépend pas du choix de la base. Si P inversible, alors :

$$\begin{aligned} \det(XI_n - PMP^{-1}) &= \det(P(XI_n - M)P^{-1}) \\ &= \det(P) \det(X - I_n M) \det P^{-1} \\ &= \det(XI_n - M) \end{aligned}$$

De cette manière, si v inversible :

$$\chi_{v \circ u \circ v^{-1}} = \chi_u$$

5.4.3 Notion de valeur propre

$\lambda \in K$ tel que $\exists x \in E$ non nul vérifiant $u(x) = \lambda x$.

5.4.4 Notion de vecteur propre associé à une valeur propre

$$E_\lambda = \{x \in E : u(x) = \lambda x\} = \mathbf{ker}(u - \lambda Id_E)$$

Proposition 5.13. *Les vecteurs propres associés à des valeurs propres 2 à 2 disjoints forment une famille libre.*

Corollaire 5.14. *Soit E de dimension finie n et $u \in \mathcal{L}(E)$, alors u a au plus n valeurs propres distinctes.*

Proposition 5.15. *Les sous-espaces vectoriels correspondant à deux valeurs propres distinctes sont en somme directe.*
Autrement dit,

$$E_{\lambda_1} \cap E_{\lambda_2} = \{0\} \quad \textit{si} \quad \lambda_1 \neq \lambda_2$$

Proposition 5.16. *Soit $u \in \mathcal{L}(E)$ et $P \in K[X]$: Pour toute valeur propre λ de u :*

$$P(u) = 0_{\mathcal{L}(E)} \implies P(\lambda) = 0_K$$

Démonstration. Si $x \in E_\lambda, P(u)(x) = P(\lambda)x$ □

Proposition 5.17. *Soit $u \in \mathcal{L}(E)$ de polynôme minimal μ_u,*

$$\lambda \textit{ valeur propre de } u \iff \mu_u(\lambda) = 0$$

Démonstration. — $\Rightarrow$: λ valeur propre de u (on dit aussi $\lambda \in \mathbf{Spec}(u)$)

$$\exists x \in E \text{ non nul tel que } u(x) = \lambda x \quad \mu_u(u)(x) = \mu_u(\lambda)x = 0$$

— $\Leftarrow$: $\mu_u(\lambda) = 0 \implies \exists Q \in K[X]$ tel que $\mu_u(X) = (X - \lambda)Q(X)$
Si λ n'était pas une valeur propre, alors $u - \lambda Id_E$ serait inversible

$$(u - \lambda Id) \circ Q = 0 \iff Q(u) = 0_{\mathcal{L}(E)}$$

Ce qui contredit la minimalité de μ.

□

Proposition 5.18. *Soit $u \in \mathcal{L}(E)$, E de dimension n. F un sous-espace vectoriel de E stable par u. On peut définir $v \in \mathcal{L}(E)$ par $v = u_{\restriction F}$. On a alors :*

$$\chi_v \textit{ divise } \chi_u$$

Démonstration. □

Proposition 5.19. *Soit $u \in \mathcal{L}(E)$ et $E = F \oplus G$ avec F et G stables par u avec $n = \dim E$.*

$$\chi_u(X) = \chi_v(X)\chi_w(X)$$

avec $v = u_{|F}$ et $w = u_{|G}$

Démonstration. La même que précédemment, on posant (f_{p+1}, f_n) une base de E. Dans ce cas-là, $B = 0$, $D = mat_{(f_{p+1},\dots,f_n)} w$ $det(XI_{n_p} - D) = \chi_w(X)$ □

5.5 Endomorphismes cycliques

Soit $u \in \mathcal{L}(E)$ et $x \in E$ non nul. Le sous espace vectoriel cyclique $E_{u,x}$ est le plus petit sous espace vectoriel de E contenant x et stable par u.

Il est engendré par les $u^k(x),\ k \in \mathbb{N}$ et si la dimension de cet espace est p, alors la famille $(x, u(x), \dots, u^{p-1}(x))$ est une base de $E_{u,x}$.

Démonstration. — Soit $F \subset vect(x, u(x), \dots, u^{p-1}(x))$.
$x \in F$ et F est stable par u.
Donc $E_{u,x} \subset F$.

— Réciproquement, les $u^k(x) \in E_{u,x}$ car $x \in E_{u,x}$ et $E_{u,x}$ est stable par u. Donc $F \subset E_{u,x}$.

On en conclut que $E_{u,x} = vect(x, u(x), \dots, u^{p-1}(x))$. □

On désigne par $\mu_{u,x}$ le polynôme minimal de u en x, c'est à dire le générateur unitaire de l'idéal

$$\{P \in K[X] \mid P(u)(x) = 0_E\}$$

Comme $\dim E$ est fini cet idéal est **non** réduit à $\{0\}$.

Si $\mu_{u,x} = X^d + \sum_{k=0}^{d-1} a_k X^k$ alors la famille $(x, u(x), \dots, u^{d-1}(x))$ est libre.

La famille est génératrice.

En effet, si on écrit $v = \sum \beta_k u^k(x) = P(u)(x)$, avec $P = \sum \beta_k X^k$.

On fait la division euclidienne de P par $\mu_{u,x}$:

$$P = Q\mu_{u,x} + R, \quad \deg R \leq d - 1$$

$$v = P(u)(x) = Q(u)\mu_{u,x}(u)(x) + R(u)(x) = R(u)(x)$$

Car $\mu_{u,x}(u)(x) = 0$ par définition.

$$P(u)(x) \in vect(x, u(x), \dots, u^{d-1}(x))$$

On a aussi $(u^k(x))_{k\in\mathbb{N}}$ base de $E_{u,x}$, donc en particulier, $d = \dim E_{u,x} - p$.

Définition 5.20. $u \in \mathcal{L}(E)$ est dit cyclique si et seulement si $\exists x \in E$ tel que $E = E_{u,x}$.

Exemple 5.5.1. Si $\dim E = 2$, u est soit une homothétie, soit un endomorphisme cyclique.

— Soit pour tout $x \in E$ non nul, $\dim(x, u(x)) = 1$.
$\forall x \in E, \exists \lambda_x \in K, u(x) = \lambda_x x$.

— λ_x ne dépend pas de x. En effet, si x et y sont non colinéaires :

$$u(x+y) = \lambda_{x+y}(x+y) = \lambda_x x + \lambda_y y \implies (\lambda_{x+y} - \lambda_x)x = (\lambda_{x+y} - \lambda_y)y$$

Donc $\lambda_{x+y} = \lambda_x = \lambda_y$.

— Si x et y sont colinéaires, alors $\exists z$ non colinéaire à x et donc à y. D'après ce qui précède, $\lambda_x = \lambda_z = \lambda_y$.

Donc $\lambda_x = \lambda$ ne dépend pas de x, et donc u est une homothétie.

— Sinon $\exists x \in E$ tel que $(x, u(x))$ est une base de E et dans ce cas u est cyclique

Exemple 5.5.2. Soit $u \in \mathcal{L}(E)$, $\dim E = n$, On suppose que u admet n valeurs propres distinctes. Alors u est cyclique.
Soit x_j un vecteur propre associé à la valeur propre λ_j.
La matrice de passage entre $(x_1, \dots, x_n)$ et $(x, u(x), \dots, u^{n-1}(x))$ est une matrice de Vandermonde.
$u(x) = \lambda_1^k x_1 + \cdots + \lambda_n^k x_n \quad u^k(x) = \lambda_1^k x + \cdots + \lambda_n^k x$

$$M = \begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^{n-1} \\ 1 & \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \cdots & \lambda_n^{n-1} \end{pmatrix}$$

On a que $\det M = 0$ si et seulement si les λ_j sont disjoints et

$$\det M = \prod_{i<j} (\lambda_j - \lambda i)$$

Proposition 5.21. *Soit $u \in \mathcal{L}(E)$ cyclique avec $\dim E = n$, alors le degré du polynôme minimal μ_u est égal a n.*

Démonstration. Soit $x \in E, \quad E_{u,x} = \mathrm{Vect}\left(\{u^k(x), \in \mathbb{N}\}\right) = E$. Si $\deg \mu_u < n$, cela implique que la famille $\{x, u(x), \dots, u^{n-1}(x)\}$ est liée, ce qui contredit $E_{u,x} = E$. En effet si $\deg \mu_u < n$ alors $\exists(\lambda_k) \quad \sum_{k=0}^{\deg \mu_u} \lambda_u^k = 0$ En prenant l'image de x, $\sum_{k=0}^{\deg \mu_u} \lambda_u^k(x) = 0$. Donc $\deg \mu_k \geq n$.
La famille $\{x, u(x), \dots, u^{n-1}(x)\}$ est une base de E. Donc il existe $a_0, \dots, a_{n-1} \in K$ tels que

$$u^n(x) = \sum_{k=0}^{n-1} a_k u^k(x)$$

Montrons que $P(X) = X^n - \sum_{k=0}^{n-1} a_n X^k$ est un polynôme annulateur de u. Il suffit de montrer que $P(u)(u^(x)) = 0_E$ pour tout $0 \leq k \leq n-1$ car $\{x, \dots, u^{n-1}(x)\}$ est une base de E. C'est vrai pour $k = 0$ d'après (*)

$$\begin{aligned} P(u)(u^k(x)) &= (P(u) \circ u^k)(x) \\ &= (u^\circ P(u))(x) \end{aligned}$$

car les polynômes d'endomorphismes commutent.

$$P(u)(u^k(x)) = U^k(\underbrace{P(u)}_{=0}(x)) = 0_E$$

P est u polynôme annulateur de u. $\mu_u \mid P$ donc $\deg \mu_u \leq \deg P = n$. □

Proposition 5.22. *Soit $u \in \mathcal{L}(E)$ et $\dim E = n = \deg \mu_u$, alors u est cyclique.*

Démonstration. On sait que $\exists x \in E$, $\mu_u = \mu_{u,x}$. $\dim E_{u,x} = \deg \mu_{u,x} = n$ donc u est cyclique. □

5.6 Matrices compagnons

Définition 5.23. La matrice compagnon ou matrice de Frobenius d'un polynôme unitaire $P(X) = X^n - \sum_{k=0}^{n-1} a_k X^k$ est la matrice

$$C_P = \begin{pmatrix} 0 & 0 & \dots & 0 & a_0 \\ 1 & 0 & \dots & 0 & a_1 \\ 0 & 1 & \dots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & a_{n-1} \end{pmatrix}$$

Remarque 5.6.1. *Soit u l'endomorphisme de E tel que C_p soit la matrice de u dans une base $\mathcal{B} = (e_1, \dots, e_n)$.*

- $u(e_1) = e_2$
- $u(e_j) = e_{j+1}$ *pour* $j \in \{2, \dots, n-1\}$
- $u(e_n) = \sum_{k=0}^{n-1} a_k e_{k+1}$

$u^k(e_i) = e_{k+1}$ *pour* $i \in \{1, \dots, n-1\}$

$$(u^n - \sum_{k=0}^{n-1} a_k u^k)(e_1) = 0_E$$

Remarque 5.6.2. *Un endomorphisme $u \in \mathcal{L}(E)$ est cyclique s'il existe une base $\mathcal{B}$ de E telle que la matrice de u dans cette base soit une matrice compagnon.*

Démonstration. — Soit $x \in E$ tel que $E_{u,x} = E$, et on choisit $\mathcal{B} = (x, u(x), \dots, u^{n-1}(x))$.

□

5.6.1 Polynôme caractéristique

Proposition 5.24. *Le polynôme caractéristique de C_P, la matrice compagnon associée à P, est P.*

Démonstration. $\Delta(a_1, \dots, a_n)(X) = \det(XI_n - C_P) = \begin{vmatrix} X & 0 & \dots & 0 & -a_0 \\ -1 & X & \dots & 0 & -a_1 \\ 0 & -1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & -1 & X - a_{n-1} \end{vmatrix}$

On développe par rapport à la premiere ligne.

$$\Delta(a_1, \dots, a_n)(X) = (-1)^{1+1} X \Delta(a_1, \dots, a_n - 1)(X) + (-1)^{1+n}(-1)^{n-1} a_0$$

et donc $\Delta(a_1, \dots, a_n)(X) = X\Delta(a_1, \dots, a_n - 1)(X) - a_0$ Et par itération on obtient $\Delta(a_1, \dots, a_n)(X) = X^n - \sum_{k=0}^{n-1} a_k X^k$ □

Proposition 5.25. *Soit $u \in \mathcal{L}(E)$ cyclique et $x \in E$ tel que $E_{u,x} = E$. On choisit les $a_k \in$ tels que*

$$u^n(x) = \sum_{k=0}^{n-1} a_k u^k(x)$$

Alors $\chi_u(X) = X^n - \sum_{k=0}^{n-1} a_k X^k$

Remarque 5.6.3. *Un corollaire direct de cet énoncé dit que tout polynôme unitaire de degré n dans $\mathbb{K}[X]$ est le polynôme caractéristique d'une matrice de $\mathcal{M}_n(\mathbb{K})$.*

Théorème 5.26 (Cas cyclique du théorème de Cayley-Hamilton)**.** *Soit $u \in \mathcal{L}(E)$ cyclique, alors χ_u le polynôme caractéristique de u est un polynôme annulateur de u.*

Démonstration. Cela découle du fait que dans $(x, u(x), \dots, u^{n-1}(x))$ la matrice de u est une matrice compagnon associée à un $P \in \mathbb{K}[X]$. P est construit pour que $P(u)(x) = 0_E$.
On a $P(u) = 0_{\mathcal{L}(E)}$ et $\chi_u = P$. □

Exemple 5.6.1. Une condition nécessaire et suffisante pour qu'un endomorphisme nilpotent soit cyclique est que son indice de nilpotence soit égal à $n = \dim E$.

5.7 Théorème de Cayley-Hamilton

Théorème 5.27. *Soit $u \in \mathcal{L}(E)$ et $\dim E = n$. Alors le polynôme caractéristique de u est un polynôme annulateur de u.*

$$\chi_u(u) = 0_{\mathcal{L}(E)}$$

Démonstration. Soit $x \in E$ non nul. $E_{u,x} = \mathrm{Vect}\,((u^k(x)))$ stable par u. □

5.7.1 Sous-espaces caractéristiques

Corollaire 5.28. *Soit $u \in \mathcal{L}(E)$ tel que χ_u est scindé, i.e. $\chi_u = \prod_{i=1}^{r}(X-\lambda_i)^{m_i}$. Alors E est la somme directe des sous-espaces caractéristiques de u. En particulier, la dimension du sous-espace caractéristique est égale à la multiplicité algébrique de la valeur propre associée.*

Démonstration. $\chi_u(X) = \prod_{i=1}^{r}(X-\lambda_i)^{m_i}$ où les λ_i sont distincts, avec $P_i(X) = (X-\lambda_i)^{m_i}$. Les P_i sont premiers entre eux. D'après le lemme des noyaux, on a que $E = \bigoplus_{i=1}^{r} \ker P_i(u)$.

Soit $v_j = u_{|\ker P_j(u)}$. On a que $\chi_u = \prod_{j=1}^{r} \chi_{v_j}$. Or la seule racine de P_i est λ_i, u annule P_i et $\deg P_i = m_i$. Donc m_i est bien la dimension du sous-espace caractéristique associé à λ_i.

$$\deg \chi_{v_i} = \dim(\ker P_i(u)) = m_i$$

□

5.7.2 Multiplicités

$u \in \mathcal{L}(E)$, λ valeur propre, $\dim E = n$.

$m_a(\lambda)$ la multiplicité algébrique de λ est sa multiplicité en tant que racine du polynôme caractéristique χ_u.

$$M = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad m_a(1) = 3$$

$m_m(\lambda)$ la multiplicité minimale de λ est la multiplicité de λ en tant que racine du polynôme minimal μ_u. Dans l'exemple précédent, $m_m(1) = 2$.

On a que $\mu_u \mid \chi_u$ et donc $m_m(\lambda) \leq m_a(\lambda)$.

$\mu_u \in \{(X-1), (X-1)^2, (X-1)^3\}$

$M - I_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \neq 0$ Donc $\mu_u \neq X-1$. $(M-I_3)^2 = 0$ donc $\mu_u = (X-1)^2$, d'où $m_m(1) = 2$.

$m_g(\lambda)$ la multiplicité géométrique de λ est la dimension du sous-espace caractéristique associé à λ.
$E_1(M) = \ker(u - id) = \text{Vect}\,((1)\,e_1, e_3)$ donc $m_g(1) = 2$.

Proposition 5.29. *Soit $u \in \mathcal{L}(E)$ et λ une valeur propre de u. On sait que $1 \leq m_g(\lambda) \leq m_a(\lambda)$ et $1 \leq m_m(\lambda) \leq m_a(\lambda)$.*
Ceci est une conséquence du lemme suivant.

Lemme 5.30. *Soit $u \in \mathcal{L}(E)$. Les polynômes μ_u et χ_u ont les mêmes facteurs irréductibles.*

Démonstration. Le théorème de Cayley-Hamilton nous dit que $\mu_u \mid \chi_u$. Soit $M = \text{Mat}\ u$.

$$\mu_u(X)I_n = \mu_u(X)I_n - \mu_u(M)$$

$$\exists Q_M(X) \text{ tel que } \mu_u(X)I_n = (XI_n - M)Q_M(X)$$

$$X^k I_n - M^k = (XI_n - M)\sum_{i=0}^{k-1} X^i M^{k-1-i}$$

$$(\sum a_k X^k)I_n - \sum a_k M^k = (XI_n - M)\underbrace{(\sum a_k \sum_{i=0}^{k-1} X^i M^{k-1-i})}_{Q_M(X)}$$

$$\det(\underbrace{\mu_u(X)I_n}_{\mu_u(X)^n}) = \det(\underbrace{XI_n - M}_{\chi_u(X)})\det Q_M(X)$$

$\chi_u(X)$ divise $\mu_u(X)^n$. Donc les facteurs irréductibles de χ_u sont les facteurs irréductibles de μ_u. □

5.8 Diagonalisation

5.8.1 Critères de diagonalisation

Remarque 5.8.1. *Comme les vecteurs colonnes d'une matrice sont les images des vecteurs de la base, si la matrice est diagonale, alors la base choisie est une base de vecteurs propres de la matrice.*

Définition 5.31. Un endomorphisme est diagonalisable s'il existe une base dans laquelle sa matrice est diagonale, autrement dit, il existe une base de vecteurs propres pour cet endomorphisme ou encore, l'espace E est la somme directe des sous-espaces propres.

Rappel 5.8.1. *Soit $A, B \in \mathcal{M}_n(K)$, on dit que A et B sont semblables s'il existe $P \in \mathcal{M}_n(K)$ inversible telle que $A = PBP^{-1}$. C'est une relation d'équivalence.*

Exemple 5.8.1. Si M est diagonalisable et M admet une seule valeur propre, alors il existe $\lambda \in K$ tel que $M = \lambda I_n$. En effet, M et I_n sont semblables et donc égales car la classe d'équivalence de I_n est $\{I_n\}$.

Proposition 5.32. *Soit $u \in \mathcal{L}(E)$ et $n = \dim E$. Si u admet n valeurs propres distinctes, alors u est diagonalisable. En particulier, une matrice triangulaire supérieure avec des coefficients diagonaux 2 à 2 distincts est diagonalisable.*

Exemple 5.8.2. $\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ est diagonalisable car ses valeurs propres sont 1 et 3.
$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ n'est pas diagonalisable, sinon elle serait semblable à la matrice identité.

On a montré qu'une famille de n vecteurs propres associés à des valeurs propres distinctes est une famille libre.

Corollaire 5.33. *Soit $u \in \mathcal{L}(E)$. Si χ_u, le polynôme caractéristique de u, est scindé à racines simples, alors u est diagonalisable.*

Démonstration. Si λ est une racine de χ_u, alors λ est une valeur propre de u. Donc on a n valeurs propres distinctes et donc u est diagonalisable. □

Théorème 5.34. *Soit $u \in \mathcal{L}(E)$ et $n = \dim E$. Les assertions suivantes sont équivalentes :*

1. *u est diagonalisable.*
2. *u admet un polynôme annulateur scindé à racines simples.*
3. *μ_u, le polynôme minimal de u est scindé à racines simples.*

Démonstration.
— $(2) \implies (3)$: Si P est scindé à racines simples annulateur alors $\mu_u \mid P$ et donc on a (3).
— $(3) \implies (1)$: On a $\mu_u \prod_{i=1}^{n}(X - \lambda_i)$ avec les $\lambda_i \in K$. On applique le lemme des noyaux.

$$E = \ker \mu_u(u) \oplus \bigoplus_{i=1}^{n} \ker(u - \lambda_i \mathrm{id}_E)$$

Et donc u est diagonalisable.
— $(3) \implies (2)$: μ_u est annulateur de u et donc on a (2).

— $(1) \implies (2)$: Dans une base des vecteurs propres, la matrice de u s'écrit $D = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix}$, où les λ_i ne sont pas forcément distincts. Soit $P \in \mathbb{K}[X]$, dans cette base $P(u)$ a comme matrice

$$P(D) = \begin{pmatrix} P(\lambda_1) & 0 & \cdots & 0 \\ 0 & P(\lambda_2) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & P(\lambda_n) \end{pmatrix}$$

On choisit $P = \prod_{i=1}^{n}(X - \lambda_i)$, alors $P(D) = 0$ et donc χ_u est annulateur de u.
Une autre manière :

$$\begin{aligned} u \text{ diagonalisable} \implies E &= \bigoplus_{i=1}^{n} \ker(u - \lambda_i \mathrm{id}_E) \\ &= \ker P(u) \\ &\implies P(u) = 0 \end{aligned}$$

□

Exemple 5.8.3. Les projecteurs sont diagonalisables car ils annulent $X(X-1)$.

Les symétries vectorielles (qui vérifient $s^2 = \mathrm{id}$) sont diagonalisables si car$K \neq 2$, car elles annulent $X^2 - 1 = (X-1)(X+1)$ et $-1 \neq 1$.

Exemple 5.8.4. Soit $A \in \mathcal{M}_q(K)$, $C \in \mathcal{M}_{n-p}(K)$ et $B \in \mathcal{M}_{q,n-p}(K)$. On choisit $M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$.
M diagonalisable $\implies$ A et C diagonalisables.
$P(M) = \begin{pmatrix} P(A) & * \\ 0 & P(C) \end{pmatrix}$. Si P scindé à racines simples annule M, alors P annule A et C. D'après le théorème, A et C sont diagonalisables. La réciproque est fausse.

Proposition 5.35. *Soit $u \in \mathcal{L}(E)$ diagonalisable et F stable par U, alors $u_{\restriction F}$ est diagonalisable.*

Démonstration. $\exists P$ scindé à racines simples tel que $P(u) = 0$, donc $P(u_{\restriction F}) = 0$. Donc $u_{\restriction F}$ est diagonalisable. □

Théorème 5.36. *$u \in \mathcal{L}(E)$ est diagonalisable si et seulement si χ_u est scindé et la dimension de chaque sous-espace vectoriel est égale à la multiplicité algébrique de la valeur propre associée.*

Démonstration. u diagonalisable $\implies E = \bigoplus_{\lambda \in \mathbf{Spec}(u)} \mathbf{ker}(u - \lambda \mathbf{id}_E)$ et donc $\chi_u = \prod_{\lambda \in \mathbf{Spec}(u)} (X - \lambda)^{\mathbf{dim\,ker}(u - \lambda \mathbf{id}_E)}$
$E = \bigoplus_{\lambda \in \mathbf{Spec}(u)} \mathbf{ker}(u - \lambda \mathbf{id}_E)^{m_a(\lambda)}$.

□

Corollaire 5.37. *$u \in \mathcal{L}(E)$ est diagonalisable si et seulement si $\sum_{\lambda \in \mathbf{Spec}(u)} \mathbf{dim\,ker}(u - \lambda \mathbf{id}_E) = \mathbf{dim}\, E$.*

Démonstration. La dimension des sous-espaces propres $\leq$ la dimension du sous-espace caractéristique. □

5.9 Trigonalisation

Définition 5.38. Un endomorphisme $u \in \mathcal{L}(E)$ est trigonalisable s'il existe une base dans laquelle sa matrice est triangulaire supérieure.

Théorème 5.39. *Soit $u \in \mathcal{L}(E)$. u est trigonalisable si et seulement si il admet un polynôme annulateur scindé, si et seulement si son polynôme caractéristique est scindé.*

Démonstration. □