Mémoire sur la leçon 141
Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

Jean Vereecke
sous la supervision de Lionel Fourquaux

20 mars 2024

Table des matières

Rapports du jury concernant la leçon 141

Extrait du rapport du jury 2023 de l'agrégation externe de mathématiques [mat23] à propos de la leçon 141 :

La présentation du bagage théorique permettant de définir corps de rupture, corps de décomposition, ainsi que des illustrations dans différents types de corps (réel, rationnel, corps finis) sont inévitables. Les corps finis peuvent être illustrés par des exemples de polynômes irréductibles de degré 2, 3, 4 sur $\mathbb{F}_2$ ou $\mathbb{F}_3$. Il est nécessaire de présenter des critères d'irréductibilité de polynômes et des polynômes minimaux de quelques nombres algébriques.

Il faut savoir qu'il existe des corps algébriquement clos de caractéristique nulle autres que $\mathbb{C}$; il est bon de savoir montrer que l'ensemble des nombres algébriques sur le corps $\mathbb{Q}$ des rationnels est un corps algébriquement clos. Le théorème de la base téléscopique, ainsi que les utilisations arithmétiques (utilisation de la divisibilité) que l'on peut en faire dans l'étude de l'irréductibilité des polynômes, est incontournable.

Des applications du corps de décomposition doivent être mentionnées, par exemple en algèbre linéaire.

Introduction

Les polynômes sont un objet fondamental des mathématiques. Étudiés depuis l'époque médiévales pendant laquelle les mathématiciens entraient en compétition afin de déterminer les racines de ces derniers, ils offrent en analyse un moyen d'approcher la plupart des fonctions quxquelles nous sommes confrontés régulièrement et leur étude est à l'origine de nombre de concepts abstraits aujourd'hui encore étudiés tels que les groupes, les anneaux, les corps... Nous nous intéressons ici à l'étude des polynômes irréductibles à une indéterminée et aux corps de rupture qui permettent d'ajouter au corps d'étude du polynôme une racine.

Dans la suite, on considère A un anneau commutatif intègre et K son corps des fractions. On considère également L une extension de K.

I Polynômes irréductibles et éléments algébriques

Dans cette première partie, on rappelle la définition de polynôme irréductibles et on s'intéresse également à la notion d'éléments algébriques.

Définition 1 (Polynôme irréductible)**.** On dit que $P \in A[X]$ est *irréductible sur* A si, et seulement si, P n'est pas inversible et que pour tout $(Q, R) \in A[X]^2$, si $P = QR$, alors Q est inversible ou R est inversible dans $A[X]$.

Les polynômes irréductibles jouent le rôle d'atomes pour l'ensemble des polynômes en décomposant n'importe quel polynôme en produit de polynômes irréductibles.

Remarques 2. On peut remarquer que si P est irréductible et si $P(a) = 0$, alors $P = u \cdot (X - a)$ où $u \in A^\times$, de cela suit :

— les polynômes de la forme $X - \alpha$ sont irréductibles sur tout anneau intègre ;

— un polynôme de degré 2 est irréductible sur un anneau intégre si, et seulement si, il n'a pas de racine.

Exemple 3. L'ensemble des polynômes irréductibles sur $\mathbb{R}$ est l'ensemble suivant :

$$\{aX + b : a \in \mathbb{R}^*, b \in \mathbb{R}\} \cup \left\{aX^2 + bX + c : (a, b, c) \in \mathbb{R}^3, b^2 - 4ac < 0\right\}.$$

Déterminer si un polynôme donné est irréductible peut parfois s'avérer difficile et pour cela, on peut chercher des conditions suffisantes d'irréductibilité des polynômes tel que le critère d'Eisenstein (cf. théorème 4).

Théorème 4 (Critère d'Eisenstein)**.** *Soient $P = a_0 + \cdots + a_n X^n \in \mathbb{Z}[X]$ et p un nombre premier. Si p ne divise pas a_n mais divise $a_0, a_1, \ldots, a_{n-1}$ et si p^2 ne divise pas a_0, alors P est irréductible sur $\mathbb{Q}$.*

Ainsi plutôt que revenir à la définition de polynômes irréductibles, ce critère revient à un simple problème de divisibilité sur $\mathbb{Z}$.

Exemple 5. Le polynôme $X^n - 2$ est irréductible sur $\mathbb{Q}$ pour tout $n \in \mathbb{N}^*$.

Quand on cherche à déterminer les polynômes irréductibles sur un anneau A, on peut se demander leur lien avec ceux sur K, c'est l'objet de la proposition 6.

Proposition 6. *Si A est un anneau factoriel, alors les polynômes irréductibles sur A sont les constantes irréductibles et les polynômes dont le pgcd des coefficients est inversible et qui sont irréductibles sur K.*

Exemple 7. Pour tout $n \in \mathbb{N}^*$, $X^n - 2$ est irréductible sur $\mathbb{Z}$.

Application 8. Si A est factoriel, alors $A[X]$ est factoriel. En particulier, $K[X]$ est factoriel.

Application 9 (Développement 1). Soit E un K-espace vectoriel de dimension finie. On dit que $u \in \mathcal{L}(E)$ est *semi-simple* si, et seulement si, u vérifie l'une des conditions équivalentes suivantes :

i) tout sous-espace de E stable par u admet un supplémentaire stable par u ;

ii) π_u, le polynôme minimal de u, est sans facteur carré.

En particulier, $u \in \mathcal{L}(\mathbb{R}_n)$ est semi-simple si, et seulement si, u est diagonalisable dans $\mathcal{L}(\mathbb{C}_n)$.

En considérant une extension de corps, il se peut quand les éléments ajoutés par l'extension soit en fait des racines des polynômes dont les coefficients vivent dans le corps de base. Ces éléments sont alors appelés les éléments algébriques du corps (cf définition 10).

Définition 10 (Élément algébrique)**.** Soient $A \subset B$ deux anneaux et $b \in B$. On dit que b est *algébrique sur* A si, et seulement si, il existe $P \in A[X] \setminus \{0\}$ tel que $P(b) = 0$. Si de plus le polynôme P est unitaire alors b est dit *entier* sur A.

Remarque 11. Si $A = K$, alors les notions coïncident.

Exemple 12. $\sqrt[n]{2}$ est entier sur $\mathbb{Z}$.

Lorsque l'on étudie la structure correspondant à l'ensemble des éléments algébriques d'un anneau, on se rend compte du fait suivant :

Proposition 13. *L'ensemble des éléments de B entiers sur A est un anneau ; l'ensemble des éléments de L algébriques sur K est un corps.*

Exemples 14. $\sqrt[3]{5\sqrt[3]{6}}$ est entier sur $\mathbb{Z}$; l'ensemble des éléments de $\mathbb{C}$ algébriques sur $\mathbb{Q}$ est un corps noté $\overline{\mathbb{Q}}$.

Puisque les éléments algébriques sont des racines de polynômes, on peut définir la notion de polynôme minimal pour ces éléments.

Définition 15 (Polynôme minimal d'un élément algébrique)**.** Soit $\alpha \in L$ algébrique sur K, on appelle *polynôme minimal de α* sur K le polynôme unitaire de $K[X]$ de plus bas degré qui s'annule en α ; on le note alors $\pi_{\alpha,K}$.

Application 16. Si $K \subsetneq K(\alpha) = L$, alors le degré d de $\pi_{\alpha,K}$ est le degré de l'extension L/K (ie la dimension de L comme K-espace vectoriel) et $(1, \alpha, \ldots, \alpha^{d-1})$ est une K-base de L.

II Adjonction de racines

Dans cette deuxième partie, on s'intéresse au fait d'ajouter à un polynôme une ou plusieurs racines, mais est-ce toujours possible ? La proposition-definition 17 nous affirme que oui.

Proposition-Définition 17 (Corps de rupture)**.** *Si P est irréductible sur K alors il existe une extension L de K telle que P a une racine dans L et $L = K(\alpha)$. On dit alors que L est un* corps de rupture *de P sur K.*

Remarque 18. L'existence de l'extension est donnée par l'injection de K dans le corps quotient $K[X]/(P)$ et la racine α est donnée par l'image de X par l'injection canonique.

Exemple 19. $\mathbb{C}$ est un corps de rupture de $X^2 + 1$ sur $\mathbb{R}$.

Exemple 20. $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$ sont des corps de rupture de $X^3 - 2$ sur $\mathbb{Q}$.

Dans la suite du document, la notation suivante est utilisée afin d'alléger l'écriture.

Notation 21. Si $\phi : K \to K'$ est un morphisme de corps, on note aussi $\phi : K[X] \to K'[X]$ le morphisme d'anneaux qui a $P = a_0 + \cdots + a_n X^n \in K[X]$ associe le polynôme $\phi(P) = \phi(a_0) + \cdots + \phi(a_n)X^n \in K'[X]$.

Remarque 22. Si P est irréductible, alors $\phi(P)$ est irréductible.

À partir de la notation précédente, un résultat important concernant les isomorphismes de corps est énoncé comme suit :

Proposition 23. *Soit $\phi : KK'$ est un isomorphisme de corps, soit P un polynôme irréductible sur K et soient deux corps de rupture $K(\alpha)$ et $K'(\alpha')$ de P sur K et de P' sur K'. Il existe un unique isomorphisme que l'on note également $\phi : K(\alpha) \to K'(\alpha')$ qui prolonge ϕ et tel que $\phi(\alpha) = \alpha'$.*

Dans la suite, on va considèrer un type particulier de morphismes de corps : les K-morphismes de corps.

Définition 24 (K-morphisme de corps)**.** Soient L et L' deux extensions de K, alors $\phi : L \to L'$ est un K-morphisme de corps si et seulement si $\phi(x) = x$ pour tout $x \in K$.

De cette notion découle le résultat suivant.

Corollaire 25. *Si $K(\alpha)$ et $K(\beta)$ sont deux corps de rupture de P, alors il existe un unique K-isomorphisme de corps $K(\alpha) \to K(\beta)$ transformant α en β.*

Exemple 26. Le corps $\mathbb{C}$ est le corps de rupture de X^2+1 sur $\mathbb{R}$.

Exemple 27. Les corps $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(j^2\sqrt[3]{2})$ sont $\mathbb{Q}$-isomorphes.

Si le corps de rupture permet d'obtenir une racine de polynôme, on peut chercher à obtenir toutes les racines de ce polynôme, d'où la notion de corps de décomposition.

Proposition-Définition 28. *Si $P \in K[X]$ est unitaire et de degré n, alors il existe une extension $K(\alpha_1, \cdots, \alpha_n)$ de K telle que $P = (X-\alpha_1)\cdots(X-\alpha_n)$ et une telle extension est appelée corps de décomposition de P sur K.*

Exemple 29. $Q(j, \sqrt[3]{2})$ est un corps de décomposition de X^3-2 sur $\mathbb{Q}$.

De même que les corps de rupture, on obtient le résultat suivant qui nous dit qu'à isomorphisme près il n'existe qu'un corps de décomposition.

Proposition 30. *Soit $\phi : K \to K'$ un isomorphisme de corps, soit $P \in K[X]$ de degré $n \geq 1$. Soient L et L' deux corps de décomposition de P sur K et de $\phi(P)$ sur K'. Alors il existe un isomorphisme de corps $\phi : L \to L'$ qui prolonge ϕ.*

Corollaire 31. *Deux corps de décomposition d'un polynôme non constant sont isomorphes.*

Dans le contexte des corps finis, on obtient l'application suivante.

Application 32 (Corps finis (Développement 2))*.* Soit p un nombre premier et $n \geq 1$, on note $q = p^n$ et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. On a les résultats suivants :

1. si $\Pi(n,p)$ est le nombre de polynômes unitaires de degré n irréductibles sur $\mathbb{F}_p$, alors $\Pi(n,p) \geq 1$ et $\Pi(n,p) = \frac{p^n}{n} + O_n\left(\frac{p^{n/2}}{n}\right)$;
2. il existe un unique corps $\mathbb{F}_q$ à q éléments : il s'agit du corps de décomposition de $X^q - X$ sur $\mathbb{F}_p$.

Remarque 33. On peut montrer de plus que pour tout entier n non nul, si $\Pi(n,q)$ est le nombre de polynômes unitaires de degré n irréductibles sur $\mathbb{F}_q$, alors $\Pi(n,q) \geq 1$ et $\Pi(n,q) = \frac{q^n}{n} + O_n\left(\frac{q^{n/2}}{n}\right)$.

III Extensions algébriques

Dans la section précédente, on s'est intéressé à la façon de scinder un polynôme. Nous allons nous intéresser dans cette section à la manière de scinder tous les polynômes à coefficient dans un corps. Tout d'abord, on définit la notion suivante.

Définition 34 (Corps algébriquement clos)**.** K est *algébriquement clos* si et seulement s'il vérifie les conditions équivalentes suivantes :

1. tout polynôme de $K[X]$ est scindé sur K ;
2. tout polynôme non constant de $K[X]$ admet au moins une racine dans K ;
3. les polynômes irréductibles sur K sont les polynômes de degré 1 ;
4. si L/K est algébrique alors $L = K$.

Exemples 35. $\mathbb{C}$ est algébriquement clos mais ce n'est pas le cas de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{F}_q$.

À partir de cette définition, on définit la manière de scinder tous les polynômes sur un corps K.

Définition 36 (Clôture algébrique)**.** On dit qu'une extension Ω d'un corps K est une *clôture algébrique* de K si et seulement si Ω est algébriquement clos et si l'extension Ω/K est algébrique.

Exemples 37. $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$; $\overline{\mathbb{Q}}$ en est une pour $\mathbb{Q}$.

L'intérêt de cette notion apparaît avec le théorème de Steinitz : il existe un sur-corps de notre corps de base qui scinde tous les polynômes.

Théorème 38 (de Steinitz)**.** *Tout corps possède une clôture algébrique.*

Et à nouveau, tout comme les corps de rupture et les corps de décomposition, il n'existe qu'un clôture algébrique pour un corps donné.

Proposition 39. *Soit $\phi : K \to K'$ un isomorphisme de corps, soient Ω et Ω' deux clôtures algébriques de K et K'. Alors ϕ se prolonge en un isomorphisme de Ω sur Ω'.*

Corollaire 40. *Deux clôtures algébriques d'un même corps sont K-isomorphes.*

Revenons à la notion d'extensions de corps et d'éléments algébriques et définissons les notions suivantes.

Définitions 41. Soit L une extension de K. On définit les notions suivantes :

1. un élément $\alpha \in L$ algébrique sur K est *séparable* sur K si et seulement si α est une racine simple de $\pi_{\alpha,K}$;
2. une extension algébrique L de K est *séparable* si et seulement si tout $\alpha \in L$ est séparable sur K ;
3. K est dit *parfait* si et seulement si toute extension algébrique de K est séparable ;
4. on dit qu'une extension L/K est *simple* si et seulement s'il existe un élément $\alpha \in L$ tel que $L = K(\alpha)$. On dit alors que α est un *élément primitif* de l'extension.

Exemple 42. Les corps de caractéristique nulle et les corps finis sont parfaits.

Remarque 43. Si Ω est une clôture algébrique de K alors l'extension Ω/K est séparable si et seulement si K est parfait.

L'intérêt de la notion d'extension simple s'illustre par le théorème suivant.

Théorème 44 (de l'élément primitif)**.** *Si $\alpha_2, \ldots, \alpha_n$ sont séparables sur K alors $L = K(\alpha_1, \ldots, \alpha_n)$ est une extension simple de K.*

Et de ceci, on peut observer la chose suivante.

Application 45. Pour tout $n \geq 1$, on peut écrire $\mathbb{F}_{q^n} = \mathbb{F}_q(\alpha)$ et $\pi_{\alpha,\mathbb{F}_q}$ est de degré n et irréductible sur $\mathbb{F}_q$.

IV Applications

Dans cette dernière section, on s'intéresse à deux applications des notions développées dans ce document.

1 Racines de l'unité et polynômes cyclotomiques

On s'intéresse à la notion de racines de l'unité sur un corps quelconque.

Définition 46 (Racine n-ième de l'unité)**.** Pour $n \geq 1$, on dit que $\zeta \in K$ est une *racine n-ième de l'unité* si, et seulement si, $\zeta^n = 1$. On pose $\mathbb{U}_n(K) = \{\zeta \in K : \zeta^n = 1\}$.

Exemple 47. $\mathbb{U}_n(\mathbb{C}) = \left\{ e^{\frac{2ik\pi}{n}} : 0 \leq k \leq n-1 \right\}$, $\mathbb{U}_n(\mathbb{Q}) = \begin{cases} \{1\} & \text{, si } n \text{ est impair ;} \\ \{-1, +1\} & \text{, si } n \text{ est pair.} \end{cases}$

Dans le cas général, pour tout $n \geq 1$, le polynôme $X^n - 1$ n'est pas scindé, il peut être alors intéressant de regarder ce polynôme dans un corps de décomposition.

Notation 48. Soit K_n un corps de décomposition de $X^n - 1$ sur K tel que la caractéristique de K_n ne divise pas n.

Avec la notation précedente, on a alors la propriété suivante.

Proposition 49. *On a :*

$$\mathbb{U}_n(K_n) \simeq \mathbb{Z}/n\mathbb{Z}$$

Puisque $U_n(K_n)$ est cyclique, il peut être intéressant de regarder les générateurs de ce groupe.

Définition 50 (Racine primitive n-ième de l'unité)**.** $\zeta \in \mathbb{U}_n(K_n)$ est une *racine primitive n-ième de l'unité* si, et seulement si, ζ engendre $U_n(K_n)$. On note $\mathbb{U}_n^\circ(K_n)$ l'ensemble des racines primitives n-ième de l'unité.

De l'isomorphisme de groupes précédents, on en déduit ce qui suit.

Proposition 51. *On a $|\mathbb{U}_n^\circ(K_n)| = \phi(n)$, où ϕ est la fonction d'Euler, et, si $k \geq 1$ et $\zeta \in \mathbb{U}_n^\circ(K_n)$, alors $\zeta^k \in \mathbb{U}_n^\circ(K_n)$ si, et seulement si, $k \wedge n = 1$.*

Proposition 52. *On a :*

$$\mathbb{U}_n(K_n) = \bigsqcup_{d|n} \mathbb{U}_d^\circ(K_n)$$

À partir des racines de l'unité, on peut définir les polynômes cyclotomiques comme suit.

Définition 53 (Polynôme cyclotomique)**.** Le *n-ième polynôme cyclotomique* sur K est le polynôme défini par :

$$\phi_{n,K} = \prod_{\zeta \in \mathbb{U}_n^\circ(K_n)} (X - \zeta).$$

De la définition et de la proposition 52, on déduit ce lien entre les polynômes cyclotomiques et $X^n - 1$

Proposition 54. *On a :*

$$X^n - 1 = \prod_{d|n} \phi_{d,K}.$$

En prenant un peu de recul, on peut se demander s'il existe un lien entre les polynômes cyclotomiques selon les corps, on l'obtient avec la proposition suivante.

Proposition 55. *On note θ le morphisme d'anneaux canonique de $\mathbb{Z}$ dans K et P le sous-corps premier de K ie le sous-corps de K engendré par 1. On a alors $\phi_{n,K} = \theta(\phi_{n,\mathbb{Q}}) \in P[X]$ et $\phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$.*

n	1	2	3	4	5	6
$\phi_{n,\mathbb{Q}}$	$X-1$	$X+1$	X^2+X+1	X^2+1	$X^4+X^3+X^2+X+1$	X^2-X+1

FIGURE 1 – Les 6 premiers polynômes cyclotomiques sur $\mathbb{Q}$

Exemple 56. Les premiers polynômes cyclotomiques sur $\mathbb{Q}$ se retrouvent en figure 1.

Puisque tous les polynômes cyclotomiques sont issus de ceux sur $\mathbb{Q}$, on peut s'intéresser à étudier ceux-ci.

Proposition 57 (Développement 3)**.** *$\phi_{n,\mathbb{Q}}$ est le polynôme minimal d'une racine primitive n-ième de l'unité et est donc irréductible sur $\mathbb{Q}$.*

Remarque 58. $\phi_{n,K}$ n'est pas toujours irréductible sur K. En effet, on a par exemple $\phi_{4,\mathbb{F}_5} = (X-2)(X+2)$.

Corollaire 59. *Si $\zeta \in \mathbb{U}_n^\circ(\mathbb{C})$, alors $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$.*

Corollaire 60. *$\mathbb{Q}(\zeta)$ est le corps de décomposition de $X^n - 1$ sur $\mathbb{Q}$.*

2 Corps de nombres algébriques

Une dernière notion qui peut être abordée est celle de corps de nombres.

Définition 61 (Corps de nombres)**.** Un *corps de nombres* est un sous-corps K de $\mathbb{C}$ de degré fini sur $\mathbb{Q}$; si l'extension est de degré 2, on dit qu'il s'agit d'un corps quadratique.
On note O_K l'anneau des éléments de K entiers sur $\mathbb{Q}$.

En particulier pour certains corps de nombres particuliers, leur étude mène à la proposition suivante.

Proposition 62. *Soit $K = \mathbb{Q}(\sqrt{d})$ où $d \in \mathbb{Z}$ est sans facteur carré, alors :*

1. *l'anneau OK des entiers de K est :*
   - $\mathbb{Z}[\sqrt{d}]$, *si* $d = 2, 3[4]$,
   - $\mathbb{Z}[\frac{1+\sqrt{d}}{2}]$, *si* $d = 1[4]$,
2. *si $d < 0$, alors les inversibles de O_K forment un groupe cyclique,*
3. *si $d > 0$, alors les inversibles positifs de O_K forment un groupe isomorphe à $\mathbb{Z}$.*

Références

[FG95] Serge Francinou et Hervé Gianella. *Exercices de mathématiques pour l'agrégation. Algèbre 1.* Masson, 1995.

[Goz09] Ivan Gozard. *Théorie de Galois (2ème édition).* Ellipses, 2009.

[Gou21] Xavier Gourdon. *Les maths en tête, Algèbre, Probabilité (3ème édition).* Ellipses, 2021.

[Rom21] Jean-Étienne Rombaldi. *Mathématiques pour l'agrégation - Algèbre et géométrie (2ème édition).* Deboeck, 2021.

[mat23] Jury de l'agrégation externe de mathématiques. *Rapport du jury de l'agrégation externe de Mathématiques.* 2023.

V Preuves

1 Preuve du développement 1

[Gou21]

Faisons la preuve de l'équivalence des conditions i) et ii).

On écrit $\pi_u = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ la décomposition de π_u en produit de polynômes irréductibles avec les P_i deux à deux distincts et les α_i dans $\mathbb{N}^*$ et pour tout $i \in [\![1, r]\!]$, on note $F_i = \ker P_i^{\alpha_i}$.

Soit F un sous-espace stable de E par u, on a alors :

$$F = \bigoplus_{i=0}^{r} (F_i \cap F).$$

En effet, on sait, d'après le théorème de Cayley-Hamilton, que $E = \bigoplus_{i=0}^{r} F_i$. Notons, pour $i \in [\![1, r]\!]$, p_i la projection sur F_1 parallèlement à $\bigoplus_{j \neq i} F_j$. Comme p_i est un polynôme en u et que F est stable pas u, F est stable par p_i ie $p_i(F) \subset F$. De plus, $p_i(F) \subset p_i(E) = F_i$ donc $p_i(F) \subset F_i \cap F$ et comme $\mathrm{id}_E = p_1 + \cdots + p_r$, on a :

$$F \subset p_1(F) + \cdots + p_r(F) = p_1(F) \oplus \cdots \oplus p_r(F) \subset (F \cap F_1) \oplus \cdots \oplus (F \cap F_r).$$

L'inclusion réciproque est facile puique $F_i \subset F \subset F$.

De plus, si π_u est irréductible, alors u est semi-simple.

En effet, soit F un sous-espace stable par u, montrons l'existence d'un supplémentaire S stable par u. Si $F = E$, alors $S = \{0\}$ convient.

Sinon si $F \neq E$, il existe $x_1 \in E \setminus F$. On considère $E_{x_1} = \{P(u)(x_1), P \in K[X]\}$ qui est un sous-espace vectoriel de E stable par u, montrons que $F \cap E_{x_1} = \{0\}$. L'ensemble $I_{x_1} = \{P \in K[X] : P(u)(x_1) = 0\}$ est un idéal de $K[X]$, non réduit à $\{0\}$ donc il existe π_{x_1} unitaire tel que $I_{x_1} = (\pi_{x_1})$. Comme $\pi_u \in I_{x_1}$ et est irréductible, $\pi_{x_1} = \pi_u$. Pour $y \in E_{x_1} \cap F$, il existe $P \in K[X]$ tel que $y = P(f)(x_1)$. Supposons par l'absurde que $y \neq 0$, alors $P \notin I_{x_1}$, donc $\pi_x \not| P$ donc ils sont premiers entre eux (comme π_x est irréductible). Il existe donc $U, V \in K[X]$ tels que $UP + V\pi_{x_1}$, donc

$$x_1 = U(u) \circ P(u)(x_1) + V(u) \circ \pi_{x_1}(u)(x_1) = U(f)(y)$$

or $y \in F$, F est stable par u donc $x_1 \in F$ ce qui est une contradiction. Ainsi $y = 0$. Ainsi $F \oplus E_{x_1}$ et E_{x_1} est stable par u.

Si jamais $F \oplus E_{x_1} \neq E$, on peut itérer le processus de construction précedent afin d'obtenir une suite nécessairement finie (car E est de dimension finie) d'espaces en somme directe qui donne le supplémentaire voulu.

Finalement montrons que u est semi-simple si, et seulement si, $\pi_u = P_1 \cdots P_r$.

Supposons tout d'abord que u est semi-simple et supposons par l'absurde qu'il existe un i tel que $\alpha_i \geq 2$ et notons $P = \pi_u / P_i$. Considérons alors $F = \ker P_i(u)$. F est stable par u donc il existe S un supplémentaire de F dans E stable par u. Soit $x \in S$, $P(u)(x) \in F$ car $P_i P = \pi_u$ annule u et $P(u)(x) \in S$ car S est stable pas u donc $P(u)(x) = 0$. De plus, pour $x \in F$, $P(u)(x) = 0$ car $M | P$. Donc $P(u)$ s'annule sur tout E et divise strictement π_u, ce qui est une contradiction. Donc nécessairement $\pi_u = P_1 \cdots P_r$.

Supposons maintenant que $\pi_u = P_1 \cdots P_r$. Soit F un sous-espace vectoriel stable par u, alors en notant $F_i = \ker P_i(f)$, on a $E = F_1 \oplus \cdots \oplus F_r$ et, au vu de ce qui précède, $F = \bigoplus_{i=1}^{r} (F_i \cap F)$. Les F_i sont stables par u et on note alors $u_i = u|_{F_i}$. On a alors $P_i(u_i) = 0$ et, comme M_i est irréductible, $\pi_{u_i} = P_i$. u_i est donc semi-simple et

$F \cap F_i$ est stable par u_i, il existe S_i stable par u_i un supplémentaire de $F \cap F_i$ dans F_i. Si on pose $S = S_1 \oplus \cdots \oplus S_r$, S est stable par u et on a alors

$$E = F_1 \oplus \cdots \oplus F_r = F \oplus S.$$

Ainsi u est semi-simple.

Remarquons que, dans le cas où le corps K est algébriquement clos (cf. définition 34), la définition de semi-simplicité coïncident avec celle de diagonalisabilité.

C'est pourquoi :

$$u \in \mathcal{L}(\mathbb{R}^n) \text{ est semi-simple} \iff u \text{ est diagonalisable dans } \mathcal{L}(\mathbb{C}^n).$$

2 Preuve du développement 2

[Rom21]

On note $\mathcal{U}_n(p)$ l'ensemble de tous les polynômes unitaires irréductibles de degré n dans $\mathbb{F}_p[X]$ et $I_n(p) = |\mathcal{U}_n(p)|$. On note également $\mathcal{D}_n = \{d \in [\![1, n]\!] : d|n\}$ et $P_n = X^q - X \in \mathbb{F}_p[X]$.

Quels sont les diviseurs irréductible de P_n ?

Soit P un diviseur irréductible de P_n dans $F_p[X]$ de degré d, alors $\overline{P_n} = 0$ dans $\mathbb{F}_{p^d} := \mathbb{F}_p[X]/(P)$ ie $\overline{X}^{p^n} = \overline{X}$. Soit $\overline{Q} = \sum_{k=0}^{d-1} a_k \overline{X}^k$ avec les a_k dans $\mathbb{F}_p$. On a alors $\overline{Q}^{p^n} = \sum_{k=0}^{d-1} a_k^{p^n} \left(\overline{X}^k\right)^{p^n} = \sum_{k=0}^{d-1} a_k \left(\overline{X}^k\right)^{p^n}$ d'après le théorème de Fermat. De plus, on a $\overline{X}^{p^n} = \overline{X}$ donc $\left(\overline{X}^k\right)^{p^n} = \overline{X}^k$. Ainsi $\overline{Q}^{p^n} = \overline{Q}$. On en déduit alors :

$$\forall \overline{Q} \in \mathbb{F}_{p^d}^*, \overline{Q}^{p^n - 1} = 1.$$

Le groupe $\mathbb{F}_{p^d}^*$ étant d'ordre $p^d - 1$, on en déduit que $p^d - 1 = p^n - 1$ ie $d|n$.

Soit $d|n$ et soit $P \in \mathcal{U}_d(p)$, alors $\mathbb{F}_{p^d} := \mathbb{F}_p[X]/(P)$ est un corps de cardinal p^d donc $\mathbb{F}_{p^d}^*$ est un groupe d'rdre $p^d - 1$ et d'après le théorème de Lagrange, on sait que $\overline{X}^{p^d - 1} = 1$ donc $\overline{X}^{p^d} = \overline{X}$, ainsi pour tout $k \in \mathbb{N}$, on a $\overline{X}^{p^{dk}} = \overline{X}$. Or $d|n$, il existe donc $q \in \mathbb{N}$ tel que $n = qd$ d'où $\overline{X}^{p^n} = \overline{X}$, ie $P|P_n$.

On a réussi à déterminer exactemet tous les diviseurs irréductibles de P_n et comme $P_n' \wedge P_n = 1$, on en déduit que P_n est produit de tous ses diviseurs irréductibles ie :

$$P_n = X^q - X = \prod_{d \in \mathcal{D}_n} \prod_{P \in \mathcal{U}_d(p)} P.$$

En considérant les degrés de P_n, on en déduit que :

$$q = p^n = \sum_{d \in \mathcal{D}_n} \sum_{P \in \mathcal{U}_d(p)} \deg(P) = \sum_{d \in \mathcal{D}_n} d \cdot \mathcal{I}_d(p) \quad \text{ie} \quad n \cdot \mathcal{I}_n(p) = p^n - \sum_{d \in \mathcal{D}_n \setminus \{n\}} d \cdot \mathcal{I}_d(p)$$

en sachant que $\mathcal{I}_1(p) = p$.

En notant μ la fonction de Möbius ie la fonction

$$\mu : \mathbb{N}^* \ni n \mapsto \begin{cases} 1 & \text{, si } n = 1 \text{ ;} \\ (-1)^r & \text{, si } n \text{ est sans facteur carré ;} \\ 0 & \text{, sinon.} \end{cases},$$

on déduit de la formule précédente par la formule d'inversion de Möbius que :

$$n\mathcal{I}_n(p) = \sum_{d \in \mathcal{D}_n} \mu\left(\frac{n}{d}\right) p^d = \sum_{d \in \mathcal{D}_n} \mu(d)\, p^{\frac{n}{d}}.$$

Montrons que pour tout $n \in \mathbb{N}^*$, $\mathcal{I}_n(p) \geq 1$ et que $\mathcal{I}_n(p) \sim \frac{p^n}{n}$.

Tout d'abord $I_1(p) = p \geq 2$ et $\mathcal{I}_2(p) = \frac{p(p-1)}{2} \geq 1$. Pour $n \geq 3$, on a

$$n\mathcal{I}_n(p) = p^n + \sum_{d \in \mathcal{D}_n \setminus \{n\}} \mu\left(\frac{n}{d}\right) p^d$$

ainsi

$$\left| \sum_{d \in \mathcal{D}_n \setminus \{n\}} \mu\left(\frac{n}{d}\right) p^d \right| \leq \sum_{k=1}^{\left[\frac{n}{2}\right]} p^d < p^{\frac{n}{2}+1},$$

par inégalité trianglaire et pour d diviseur strict positif de n, $2d \leq n$.

C'est pourquoi $n\mathcal{I}_n(p) > p^n - p^{n/2+1} > 0$ et :

$$\left| \frac{n\mathcal{I}_n(p)}{p^n} - \right| < \frac{p^{n/2+1}}{p^n} \xrightarrow[n \to +\infty]{},$$

ie on a montré ce que l'on voulait montrait.

Pour tout entier $n \in \mathbb{N}^*$, il existe donc un polynôme unitaire irréductible P de degré n dans $\mathbb{F}_p[X]$ et le quotient $\mathbb{F}_p[X]/(P)$ est un corps à p^n éléments, reste à montrer qu'à isomorphisme près c'est le seul.

Soit K un corps à p^n élément, alors K a pour caractéristique p et ainsi $\mathbb{F}_p$ peut-être identifié au sous-corps premier de K et un polynôme de $\mathbb{F}_p[X]$ peut-être identifié à un polynôme de $K[X]$.

Soit $P \in \mathcal{U}_n(p)$, montrons que P est scindé à racines simples dans $K[X]$. Le polynôme $P \in \mathcal{U}_n(p)$ divise $X^{p^n} - X$ dans $\mathbb{F}_p[X]$ d'après ce qui précède donc dans $K[X]$ également. De plus pour tout $\lambda \in K$, $\lambda^{p^n} - \lambda = 0$ et $P_n = X^{p^n} - X$ est donc scindé à racines simples donc $P | P_n$ est scindé à racines simples.

Pour toute λ racine de P, le morphisme d'anneaux $\varphi : \mathbb{F}_p[X] \ni R \mapsto R(\lambda) \in K$ a son noyau qui contient (P) car P est irréductible sur $\mathbb{F}_p$ et, ce noyau étant un idéal strict de $\mathbb{F}_p[X]$, il existe $Q \in \mathbb{F}_p[X]$ tel que $\ker(\varphi) = (Q)$ et $Q \neq 1$, ainsi, comme $(P) \subset (Q)$, $Q | P$ et donc $P = Q$ car P est irréductible dans $\mathbb{F}_p[X]$. Ainsi φ induit un morphsime d'anneaux injectif de $\mathbb{F}_p[X]/(P)$ dans K et par égalité des cardinaux, on obtient que les deux corps sont isomorphes.