JOUVE ADAM

Mémoire Master 2 : Mathématiques et applications, parcours Mathématiques générales.

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

Université Claude Bernard

2024 — 2025

Table des matières

1 Rapport du Jury

Les généralités sur les algèbres de polynômes à une variable sont supposées connues. Le bagage théorique permettant de définir corps de rupture et corps de décomposition doit être présenté. Ces notions doivent être illustrées dans différents types de corps (réels, rationnels, corps finis) ; 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 les polynômes minimaux de quelques nombres algébriques, par exemple les polynômes cyclotomiques. 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 sont incontournables. Des applications du corps de décomposition doivent être mentionnées, par exemple en algèbre linéaire. Pour aller plus loin, on peut montrer que l'ensemble des nombres algébriques sur le corps Q des rationnels est un corps algébriquement clos, s'intéresser aux nombres constructibles à la règle et au compas, et éventuellement s'aventurer en théorie de Galois.

2 Plan

Dans toute la suite, A désignera un anneau intègre (commutatif), $\mathbb{K}$ un corps, et E un $\mathbb{K}-$espace vectoriel de dimension $n \in \mathbb{N}^*$.

2.1 Irréductibilité

2.1.1 Définitions et premières propriétés

Définition 1 *$P \in A[X] \backslash A$ sera dit irréductible sur A si $P = QR$ implique $Q \in A[X]^\times$ ou $R \in A[X]^\times = A^\times$.*

Remarque 2 *L'irréductibilité d'un polynôme est intrinsèque à l'anneau A. Par exemple $2X$ n'est pas irréductible sur $\mathbb{Z}$ mais il est irréductible sur $\mathbb{Q}$.*

Proposition 3 *Soit $P \in \mathbb{K}[X]$*

1. *$deg(P) = 1 \implies P$ est irréductible sur $\mathbb{K}$.*
2. *Si $deg(P) > 1$ alors (P irréductible sur $\mathbb{K} \implies P$ est sans racines dans $\mathbb{K}$).*
3. *Si $deg(P) \in \{2, 3\}$ alors (P est irréductible si et seulement si P n'a pas de racines dans $\mathbb{K}$).*

Preuve 1

1. *Immédiat en considérant le degré.*
2. *Si P avait une racine $\alpha \in \mathbb{K}$ alors $X - \alpha | P(X)$, donc $\exists Q \in \mathbb{K}[X]$ tel que $P = (X - \alpha)Q(X)$. Et $Q \notin \mathbb{K}^\times$ pour des raisons de degré, donc P n'est pas irréductible sur $\mathbb{K}$.*
3. *L'implication directe découle du point 2. Concernant l'implication réciproque, si $deg(P) = 2$, alors comme P n'a pas de racines, si $P = QR$ forcément[a], toujours pour des raisons de degré, Q ou R est de degré 0, c'est-à-dire constant donc P irréductible sur $\mathbb{K}$.*
   Si $deg(P) = 3$, raisonnement analogue.

a. Un polynôme de degré 1, sur un corps, a toujours une racine.

Contre Exemple 4 *$P = (X^2 + 1)^2 \in \mathbb{R}[X]$ n'a pas de racine dans $\mathbb{R}$, mais il n'est pas irréductible sur $\mathbb{R}$.*

Théorème 5 *Si A est factoriel alors $A[X]$ est factoriel.*

Preuve 2 *ADMISE.*

Remarque 6 *Ainsi tout polynôme à coefficients dans un anneau factoriel se décompose de manière unique (à la multiplication d'une unité près) en un produit de polynômes irréductibles sur ce même anneau. Ce qui est l'une des motivations de l'étude des polynômes irréductibles.*

2.1.2 Premiers critères d'irréductibilité

Dans toute la suite A est supposé être un anneau factoriel.

Proposition 7 *Pour $P = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[\mathbb{X}]$, si $\frac{p}{q} \in \mathbb{Q}$ (avec p et q premiers entre eux) est une racine de P alors $p|a_0$ et $q|a_n$.*

Preuve 3 *$\frac{p}{q}$ est une racine de P donc $a_n p^n + a_{n-1}p^{n-1}q + ... + a_0 q^n = 0$ donc $q|a_n p^n$ et comme $\gcd(p,q) = 1$, d'après le lemme de Gauss, $q|a_n$. Raisonnement analogue pour $p|a_0$.*

Définition 8 *Pour $P \in A[X]$, on appelle contenu de P, noté $c(P)$, un pgcd des coefficients de P (défini donc à multiplication près d'une unité).*
De plus, P sera dit primitif si $c(P) = 1$.

Lemme 9 *1. Le produit de deux polynômes primitifs est primitif.*
2. $\forall P, Q \in A[X]\backslash A, c(PQ) = c(P)c(Q)$.

Théorème 10 **k** $= Frac(A)$ [a] *.Pour $P \in A[X]\backslash A$,*
P irréductible sur $A \iff P$ irréductible sur **k** *et P primitif.*

a. **k** $= Frac(A)$ désigne le corps des fractions de l'anneau intègre A.

Preuve 4 *Supposons P irréductible sur A. Alors puisque $c(P) \mid P$ dans $A[X]$, forcément $c(P) \in A^\times$, dit encore autrement P est primitif. Supposons $P = QR$ où Q et R sont deux polynômes non constants de $\mathbb{K}[X]$. On considère a un ppcm des dénominateurs des coefficients non nuls de Q et R. Dès lors, $a^2P = (aQ)(aR) = UV$ (δ) où $U := aQ \in A[X]$ et $V := aR \in A[X]$.*
De plus, on récupère $a^2c(P) = C(U)C(V)$. Maintenant on « factorise » U et V par leur contenu, $U = c(U)U_1$ et $V = c(V)V_1$ où $U_1, V_1 \in A[X]$ et tous deux primitifs. En reportant dans (δ), on obtient $a^2P = c(U)U_1c(V)V_1 = a^2c(P)U_1V_1$; et puisque $a \in A\backslash\{0\}$, $P = c(P)U_1V_1$. Ce qui constitue une contraction avec l'irréductibilité de P sur A (ABSURDE), car $c(P)U_1$ et V_1 sont tous deux de degré au moins 1 et dans $A[X]$.

Réciproquement, supposons que P soir irréductible sur $\mathbb{K}$ et primitif sur A. Supposons $P = QR$ avec Q et R dans $A[X]$. $Q, R \in A[X] \subseteq \mathbb{K}[X]$, et comme P est irréductible sur $\mathbb{K}$, ou bien $Q \in \mathbb{K}^*$ ou $R \in \mathbb{K}^*$. Sans perte de généralité, supposons que $Q \in \mathbb{K}^*$. Donc $Q \in A\backslash\{0\}$, ainsi $Q \mid c(P)$ dans A. Or P étant primitif, $Q \in A^\times$. Ainsi P irréductible sur A.

Exemple 11 *Les polynômes irréductibles de $\mathbb{Z}[X]$ sur $\mathbb{Z}$ sont les polynômes primitifs et irréductibles sur $\mathbb{Q}$.*

Théorème 12 (Critère D'Eisenstein) *Pour $P(X) = \sum_{k=0}^{n} a_k X^k \in A[X]$ de degré $n \geq 1$, s'il existe $q \in A$ irréductible tel que $\forall k \in \{0, ..., n-1\}, q | a_k$, $q \nmid a_n$ et $q \nmid a_0^2$, alors P est irréductible sur* **k**.

Preuve 5 *Si, par l'absurde, $P = UV$ où U et V ne sont pas constants dans $\mathbb{K}[X]$. Comme dans la preuve précédente, on peut écrire $P = RS$ où R et S sont dans $A[X]$ et de degré au moins égal à 1. $R(X) = \sum_{i=0}^{r} b_i X^i$ et $S(X) = \sum_{j=0}^{s} c_j X^j$ avec donc $r, s \geq 1$ et $a_n = b_r c_s \neq 0$. Puisque $r + s = n$, forcément $r, s \leq n - 1$.*
On introduit l'anneau quotient $B = A/(q)$ qui est intègre car q irréductible donc premier (A factoriel).

Soit $\Phi : A \longrightarrow B$ le morphisme surjectif canonique, que l'on étend naturellement en morphisme surjectif (que l'on continue d'appeler Φ) de $A[X] \longrightarrow B[X]$. Il vient $\Phi(P(X)) = \sum_{i=0}^{r} \Phi(b_i) X^i \times \sum_{j=0}^{s} \Phi(c_j) X^j$.

Comme tous les $\Phi(a_k) = 0$ (pour $k \in \{0, ...n-1\}$, car $q \mid a_k$), on a $\Phi(P(X)) = \Phi(a_n)X^n$. En considérant le terme de degré 0, on récupère que $\Phi(b_0)\Phi(c_0) = 0$, B étant un anneau intègre, $\Phi(b_0) = 0 ou\ \Phi(c_0) = 0$. Ils ne peuvent pas être nuls simultanément car $a_0 = b_0 c_0$, ce qui voudrait dire que $q^2 \mid a_0$. Sans perte de généralité, et pour fixer les idées, supposons que $\Phi(b_0) = 0$ et $\Phi(c_0) \neq 0$. Si tous les $\Phi(b_i) = 0$ alors en particulier $\phi(b_r) = 0$ et donc $\Phi(a_n) = \phi(b_r)\phi(c_r) = 0$, ce qui est exclu.
Ainsi il existe un unique $i \in \{0, ..., r-1\}$ tel que $\phi(b_i) = 0$ et $\phi(b_{i+1}) \neq 0$ et $\Phi(c_0) \neq 0$, donc $\Phi(a_{i+1}) \neq 0$). Absurde puisque $i + 1 \leq r < n$, donc on est censé avoir $\Phi(a_{i+1}) = 0$.

Exemple 13
1. *$\forall n \in \mathbb{N}, X^n - 2$ est irréductible sur $\mathbb{Q}$.*
2. *$X^4 + 1$ est irréductible sur $\mathbb{Q}$.*

Proposition 14 *$P \in \mathbb{K}[X]$ est irréductible sur $\mathbb{K} \iff \mathbb{K}[X]/(P)$ est un corps.*

Preuve 6 *Cela vient du fait qu'un anneau quotienté par un idéal est un corps si et seulement si l'idéal est maximal. Or comme* $\mathbb{K}[X]$ *est principal, l'irréductibilité de* P *équivaut à la maximalité de* (P).

Exemple 15 $\mathbb{R}[X]/(X^2+1)$ *est un corps* ($\cong \mathbb{C}$). *Il s'agit d'une construction du corps des nombres complexes.*

Théorème 16 *Pour* $P = \sum_{k=0}^{n} a_k X^k \in A[X]$, I *un idéal premier de* A, *si* $a_n \notin I$ *et* P *est irréductible modulo* I, *alors* P *irréductible sur* $\mathbf{k}$.

Corollaire 17 *Un polynôme* $P \in \mathbb{Z}[X]$ *irréductible modulo un nombre premier est irréductible sur* $\mathbb{Q}$. *De plus, si* P *est unitaire, alors il est irréductible sur* $\mathbb{Z}$.

Exemple 18 $X^3 + 462X^2 + 2435X - 57821$ *est irréductible sur* $\mathbb{Z}$.

2.2 Extensions de Corps

2.2.1 Éléments et extensions algébriques

Définition 19 *Soit* $\mathbb{K}$ *et* $\mathbb{L}$ *deux corps. Si* $\mathbb{K} \hookrightarrow \mathbb{L}$, *on dira que* $\mathbb{L}$ *est une extension de* $\mathbb{K}$, *et on note* $\mathbb{L}/\mathbb{K}$.

Exemple 20 $\mathbb{C}/\mathbb{R}$, $\mathbb{K}(X)/\mathbb{K}$ *et* $\frac{\mathbb{K}[X]/(P)}{\mathbb{K}}$

Définition 21 *Pour une extension* $\mathbb{L}/\mathbb{K}$, *on appelle degré la dimension de* $\mathbb{L}$ *vu comme un* $\mathbb{K}$*-espace vectoriel. On note* $[\mathbb{L} : \mathbb{K}]$.

Théorème 22 (théorème de la base téléscopique) *Soit* $\mathbb{M}/\mathbb{L}/\mathbb{K}$, *une tour d'extensions, tel que* $(e_i)_i$ *soit une* $\mathbb{K}-$*base de* $\mathbb{L}$, *et* $(f_j)_j$ *une* $\mathbb{L}$*-base de* $\mathbb{M}$, *alors* $(e_i f_j)_{i,j}$ *est une* $\mathbb{K}$*-base de* $\mathbb{M}$.

Preuve 7 *Caractère libre : si* $\sum_{i,j} \alpha_{i,j} e_i f_j = 0$ *Alors* $\sum_j (\sum_i \alpha_{i,j} e_i) f_j = 0$, *comme* f_j *est une famille libre de* $\mathbb{M}$ *vu comme un* $\mathbb{L}$*-ev, on a* $\forall j \quad \sum_i \alpha_{i,j} e_i = 0$ *; comme* e_i *est une famille libre de* $\mathbb{L}$ *vu comme un* $\mathbb{K}$*-ev, on a* $\forall j \quad \forall i \quad \alpha_{i,j} = 0$.

Caractère générateur : Pour $x \in \mathbb{M}$, x *peut s'écrire comme* $\mathbb{L}$ *combinaison linéaire des* f_j *(car base de* $\mathbb{M}$ *vu comme un* $\mathbb{L}$*-ev), et chaque coefficient de cette combinaison linéaire s'écrit en* $\mathbb{K}$ *combinaison linéaire des* e_i *(car base de* $\mathbb{L}$ *vu comme un* $\mathbb{K}$*-ev).*

En clair $x \in \mathbb{M}$ peut s'écrire en $\mathbb{K}$ combinaison linéaire des $e_i f_j$.

Corollaire 23 *Pour $\mathbb{M}/\mathbb{L}/\mathbb{K}$, une tour d'extensions, on a $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$. (Les quantités peuvent, éventuellement, être infinies)*

Preuve 8 *Preuve directe avec le théorème précédent. Il suffit de compter le cardinal de la base donnée par le théorème précédent.*

Définition 24 *Pour $\mathbb{L}/\mathbb{K}$, et $A \subseteq \mathbb{L}$, on note $\mathbb{K}(A)$ le plus petit sous corps de $\mathbb{L}$ contenant $\mathbb{K}$ et A. C'est une extension de $\mathbb{K}$. Si $A = \{\alpha\}$, on dit que que $\mathbb{K}(\alpha)/\mathbb{K}$ est une extension simple.*

Exemple 25 $\mathbb{R}(i) = \mathbb{C}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

Définition 26 *Soit $\alpha \in \mathbb{L}$.* $\begin{array}{rccc} \theta_\alpha & : & \mathbb{K}[X] & \to & \mathbb{L} \\ & & P & \mapsto & P(\alpha) \end{array}$ *est un morphisme d'anneaux et on note $\mathbb{K}[\alpha] = Im(\theta_\alpha)$.*

1. *α sera dit transcendant sur $\mathbb{K}$ si θ_α est injective.*
2. *Sinon α sera dit algébrique sur $\mathbb{K}$. Et dans ce cas, on note $Irr_{\mathbb{K}}(\alpha)$ le générateur unitaire du noyau $\ker(\theta_\alpha)$.*

Exemple 27 *$\sqrt[3]{2}$ est algébrique sur $\mathbb{Q}$ car annulé par le polynôme $X^3 - 2 \in \mathbb{Q}[X]$.*

Proposition 28 *Pour $\alpha \in \mathbb{L}$, algébrique sur $\mathbb{K}$*

1. *$\mathbb{K}[\alpha]$ est un corps et $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$.*
2. *$\deg(Irr_{\mathbb{K}}(\alpha)) = [\mathbb{K}(\alpha) : \mathbb{K}] = [\mathbb{K}[\alpha] : \mathbb{K}]$.*
3. *$Irr_{\mathbb{K}}(\alpha)$ est irréductible sur $\mathbb{K}$.*

Preuve 9 *On applique le 1 er théorème d'isomorphisme à θ_α, pour obtenir l'isomorphisme d'algèbre : $k[\alpha] \simeq \mathbb{K}[X]/(Irr_{\mathbb{K}}(\alpha))$ donc $\mathbb{K}[\alpha]$ est un corps qui contient $\mathbb{K}$ et α, par définition de $\mathbb{K}(\alpha)$, forcément $\mathbb{K}(\alpha) \subseteq \mathbb{K}[\alpha]$, mais l'inclusion réciproque est immédiate, donc $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$ et donc $\deg(Irr_{\mathbb{K}}(\alpha)) = [\mathbb{K}(\alpha) : \mathbb{K}] = [\mathbb{K}[\alpha] : \mathbb{K}]$*

Supposons que $Irr_{\mathbb{K}}(\alpha) = PQ$ où $P, Q \in \mathbb{K}[X]$. En évaluant en α, on a $PQ(\alpha) = 0$ ce qui implique P ou Q annule α. Si $P(\alpha) = 0$ alors P est dans l'idéal de $Irr_{\mathbb{K}}(\alpha)$; $Irr_{\mathbb{K}}(\alpha)$ divise donc P, or P divise $Irr_{\mathbb{K}}(\alpha)$. Donc $deg(P) = deg(Irr_{\mathbb{K}}(\alpha))$ ce qui implique que Q est forcément constant. Raisonnement analogue si c'est $Q(\alpha) = 0$.

Théorème 29 *Pour $\mathbb{L}/\mathbb{K}$ et $\alpha \in \mathbb{L}$, on a : α algébrique sur $\mathbb{K} \iff [\mathbb{K}(\alpha) : \mathbb{K}] < +\infty$*

Preuve 10 *α algébrique sur $\mathbb{K}$ implique que $\deg(Irr_{\mathbb{K}}(\alpha)) = [\mathbb{K}(\alpha) : \mathbb{K}]$.*

Et réciproquement, si $[\mathbb{K}(\alpha) : \mathbb{K}] < +\infty$, alors la famille $\{\alpha^j / j \in \mathbb{N}\}$ est liée. Ce qui veut exactement dire qu'il existe un polynôme non nul à coefficients dans $\mathbb{K}$ annulant α.

Proposition 30 *$[\mathbb{L} : \mathbb{K}] < +\infty \implies \mathbb{L}/\mathbb{K}$ algébrique.*

Preuve 11 *Soit $\alpha \in \mathbb{L}$, alors, comme $[\mathbb{L} : \mathbb{K}] < +\infty$, la famille $\{\alpha^j / j \in \mathbb{N}\}$ est liée. Ce qui veut exactement dire qu'il existe un polynôme non nul à coefficients dans $\mathbb{K}$ annulant α.*

Remarque 31 *Réciproque fausse ; en considérant $\mathbb{K} = \mathbb{Q}$ et $\mathbb{L} = \bigcup_{n \in \mathbb{N}^*} \mathbb{Q}_n$ où $\mathbb{Q}_n = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n})$ avec $(p_j)_j$ la suite des nombres premiers (rangés dans l'ordre croissant).*

2.2.2 Corps de rupture, corps de décomposition

Définition 32 *Pour $P \in \mathbb{K}[X]$ irréductible, un corps $\mathbb{L}$ extension de $\mathbb{K}$ sera dit corps de rupture de P, si $\exists \alpha \in \mathbb{L}$ tel que $P(\alpha) = 0$ et $\mathbb{L} = \mathbb{K}(\alpha)$.*

Exemple 33
1. *$\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $X^3 - 2 \in \mathbb{Q}[X]$.*
2. *$\mathbb{K}[X]/(P)$ est un corps de rupture de $P \in \mathbb{K}[X]$ avec P est irréductible.*

Proposition 34 *Pour $P \in \mathbb{K}[X]$ irréductible, il existe un unique corps de rupture de P, à $\mathbb{K}$-isomorphisme près.*

Preuve 12 *Soit $\mathbb{K}(\alpha)$ et $\mathbb{K}(\gamma)$ deux corps de rupture de $P \in \mathbb{K}[X]$ irréductible. Il suffit alors de considérer l'application $\begin{array}{rccc} \phi_{\alpha,\gamma} & : & \mathbb{K}(\alpha) & \to & \mathbb{K}(\gamma) \\ & & P(\alpha) & \mapsto & P(\gamma) \end{array}$ qui est un $\mathbb{K}$-isomorphisme.*

Définition 35 *Pour $P \in \mathbb{K}[X]$, on appelle corps de décomposition tout corps extension minimale de $\mathbb{K}$ sur laquelle P est scindé.*

Théorème 36 *Pour $P \in \mathbb{K}[X]$, il existe un unique corps de décomposition de P, à $\mathbb{K}$-isomorphisme près.*

Preuve 13 ***Existence*** *: On fait une récurrence sur $\deg(P) = n \in \mathbb{N}^*$.*
INITIALISATION : Si $n = 1$, $\mathbb{K}$ convient car un polynôme de degré 1 est toujours scindé.
HÉRÉDITÉ : Soit $n \in \mathbb{N}^*$. Supposons le résultat vrai au rang n. Montrons qu'il est vrai au rang $n+1$. Soit $f \in \mathbb{K}[X]$ un facteur irréductible de P. On considère $\mathbb{K}(\alpha)$ un corps de rupture de f. α est une racine de f donc de P, ainsi $X - \alpha \mid P$ dans $\mathbb{K}(\alpha)$. Ainsi $\exists\ g \in \mathbb{K}(\alpha)[X]$ tel que $f(X) = g(X)(X - \alpha)$ avec $\deg(g) = n - 1$. On applique l'hypothèse de récurrence à g : il existe $\mathbb{E}$ une extension minimale de $\mathbb{K}(\alpha)$ où g est scindé. Montrons que $\mathbb{E}$ est un corps de décomposition de P sur $\mathbb{K}$. Il est clair que P est scindé sur $\mathbb{E}$. D'autre part si P est scindé sur $\mathbb{E}_{\not\vdash}$ avec $\mathbb{K} \subseteq \mathbb{E}_{\not\vdash} \subseteq \mathbb{E}$, alors la racine $\alpha \in \mathbb{E}_{\not\vdash}$. Donc $\mathbb{E}_{\not\vdash} \supseteq \mathbb{K}(\alpha)$. Donc f est scindé sur $\mathbb{E}_{\not\vdash}$ et alors comme $g \mid f$, g est scindé sur $\mathbb{E}_{\not\vdash}$. Mais $\mathbb{E}$ étant corps de décomposition de g (sur $\mathbb{K}(\alpha)$), on a $\mathbb{E}_{\not\vdash} = \mathbb{E}$. Ce qui conclut l'existence.

L'unicité *: Admise. Cf [GOZ] page 63 (par exemple).*

Exemple 37 *« Le » corps de décomposition du $X^3 - 2 \in \mathbb{Q}[X]$ est $\mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2})$.*

Proposition 38 *$P \in \mathbb{K}[X]$ est irréductible si et seulement si P n'a aucune racine dans toute extension $\mathbb{L}$ de $\mathbb{K}$ de degré au plus $\frac{deg(P)}{2}$.*

Preuve 14 *Supposons que P a une racine α dans $\mathbb{L}$ une extension de $\mathbb{K}$ de degré au plus $\frac{\deg(P)}{2}$. Alors $Irr_{\mathbb{K}}(\alpha) | P$ et $1 \leq \deg(Irr_{\mathbb{K}}(\alpha)) = [\mathbb{K}(\alpha) : \mathbb{K}] \leq^a [\mathbb{L} : \mathbb{K}] = \frac{deg(P)}{2} < \deg(P)$. Donc P n'est pas irréductible sur $\mathbb{K}$.*
Inversement, supposons que P ne soit pas irréductible et notons $Q \in \mathbb{K}[X]$, un facteur irréductible de P, et α une racine de Q qui est aussi une racine de P. Alors $[\mathbb{K}(\alpha) : \mathbb{K}] = \deg(Irr_{\mathbb{K}}(\alpha)) \leq \frac{deg(P)}{2}$. Donc P admet une racine dans $\mathbb{K}(\alpha)$ qui est une extension de $\mathbb{K}$ de degré au plus $\frac{\deg(P)}{2}$

a. car $\mathbb{K}(\alpha) \subseteq \mathbb{L}$

Remarque 39 *Ce critère est surtout utilisé dans le cadre des corps finis.*

Exemple 40 *Pour tout nombre premier p, $X^4 + 1 \in \mathbb{F}_p$ est réductible sur $\mathbb{F}_p$. Et notons qu'il est pourtant irréductible sur $\mathbb{Z}[X]$.*

Proposition 41 *Soit $P \in \mathbb{K}[X]$ tel que $deg(P) = n$ et $\mathbb{L}$ une extension de $\mathbb{K}$ telle que $[\mathbb{L} : \mathbb{K}] = m$. Si P est irréductible sur $\mathbb{K}$ et $\gcd(m, n) = 1$ alors P est irréductible sur $\mathbb{L}$.*

Preuve 15 *Soit α une racine de P. ALors $\mathbb{K}(\alpha)$ est un corps de rupture de P sur $\mathbb{K}$.*
Donc $[\mathbb{K}(\alpha) : \mathbb{K}] = n$. On écrit maintenant, d'une part :
$[\mathbb{L}(\alpha) : \mathbb{K}] = [\mathbb{L} : \mathbb{K}(\alpha)][\mathbb{K}(\alpha) : \mathbb{K}] \iff [\mathbb{L}(\alpha) : \mathbb{K}] = [\mathbb{L}(\alpha) : \mathbb{K}(\alpha)]n$
Et de l'autre part :
$[\mathbb{L}(\alpha) : \mathbb{K}] = [\mathbb{L}(\alpha) : \mathbb{L}][\mathbb{L} : \mathbb{K}] \iff [\mathbb{L}(\alpha) : \mathbb{K}] = [\mathbb{L}(\alpha) : \mathbb{L}]m$

Alors $[\mathbb{L}(\alpha) : \mathbb{K}(\alpha)]n = [\mathbb{L}(\alpha) : \mathbb{L}]m$.
Ainsi par le lemme de Gauss $n \mid [\mathbb{L}(\alpha) : \mathbb{L}] = \deg(Irr_{\mathbb{L}}(\alpha))$.
Donc $\deg(Irr_{\mathbb{L}}(\alpha)) \geq \deg(P) = n$
Mais P étant un polynôme à coefficients dans $\mathbb{L}$ qui annule α,$Irr_{\mathbb{L}}(\alpha) \mid P$, donc $\deg(Irr_{\mathbb{L}}(\alpha)) \leq \deg(P) = n$.
Donc on a affaire à deux polynômes unitaires ayant le même degré et l'un divisant l'autre, ils sont donc égaux d'où P irréductible sur L, puisque $P = Irr_{\mathbb{L}}(\alpha)$ est par définition irréductible sur $\mathbb{L}$.

$[\mathbb{L}(\alpha) : \mathbb{L}] = \deg(Irr_{\mathbb{L}}(\alpha)) \leq \deg(P)$

Exemple 42
1. *$X^7 - 2$ est irreductible sur $\mathbb{Q}(j)$.*
2. *$X^3 + 4X + 2$ est irréductible sur $\mathbb{Q}(i)$.*

2.2.3 Clôture algébrique

Proposition 43 *Les 3 assertions suivantes sont équivalentes :*

1. *Les seuls polnômes de $\mathbb{K}[X]$ irréductibles sur $\mathbb{K}$ sont les polynômes de degré 1.*
2. *Tout polynôme de $\mathbb{K}[X]$ non constant a une racine dans $\mathbb{K}$.*
3. *Tout polynôme de $\mathbb{K}[X]$ est scindé sur $\mathbb{K}$.*

Dans ce cas, on dira que $\mathbb{K}$ est un corps algébriquement clos.

Preuve 16 1 $\implies$ 2 *: P est produit de polynômes de degré 1, qui ont toujours une racine dans $\mathbb{K}$, d'où P a une racine dans $\mathbb{K}$.*

2 $\implies$ 3 *Comme tous les polynômes non constants ont une racine dans $\mathbb{K}$, tous les facteurs irréductibles de P sont de degré 1, dit autrement P est scindé.*

3 $\implies$ 1, *Découle du fait qu'un polynôme ne peut pas, par définition même, être scindé et irréductible en même temps, sauf s'il est de degré 1.*

Proposition 44 *Un corps algébriquement clos est infini.*

Preuve 17 *Si $\mathbb{K} = \{\lambda_1, ..., \lambda_q\}$ est un corps fini alors le polynôme $\Delta(X) = \prod_{j=1}^{q}(X - \lambda_q) + 1 \in \mathbb{K}[X]$ et n'a aucune racine dans $\mathbb{K}$. Un corps fini ne peut pas être algébriquement clos.*

Théorème 45 (Théorème de D'Alembert-Gauss) $\mathbb{C}$ *est algébriquement clos.*

Preuve 18 *Il existe de nombreuses preuves de ce théorème. Les historiens des mathématiques considèrent que la première preuve fût donnée par Gauss en* 1799 *(peaufinée par lui-même en* 1815*). Ici, je présente la « plus classique » après un cursus de licence : la preuve qui utilise le théorème de Liouville (en analyse complexe).*

Par l'absurde, supposons que il existe $P \in \mathbb{C}[X]\backslash\mathbb{C}$, qui n'admet pas de racines dans $\mathbb{C}$. On note $n = \deg(P) \in \mathbb{N}^*$. On considère la fonction de la variable complexe $f : z \mapsto \frac{1}{P(z)}$. f est entière[a]*. Dès lors, d'après le théorème de Liouville, f est constante ou non bornée. Mais comme $n > 0$, $\lim_{|z|\to\infty} f(z) = 0$, f est alors bornée. Donc f est constante, donc P constant à son tour, ce qui est ABSURDE (car $P \notin \mathbb{C}$).*[b]

a. Ce qui veut dire que f est holomorphe sur tout $\mathbb{C}$.

b. On rappelle que comme $\mathbb{C}$ est un corps infini on peut confondre le polynôme P et la fonction polynômiale associée.

Définition 46 *Si $\mathbb{L}$ est un corps algébriquement clos et $\mathbb{L}/\mathbb{K}$ algébrique, on dira que $\mathbb{L}$ est une clôture algébrique de $\mathbb{K}$.*

Théorème 47 (théorème de Steinitz) $\mathbb{K}$ *admet une unique clôture algébrique, à $\mathbb{K}$-isomorphisme près.*

Preuve 19 *Admise. Cf [GOZ] page 63 (par exemple).*

2.3 Applications

2.3.1 Algèbre linéaire

u désignera un endomorphisme de E.

Lemme 48 *(Lemme des noyaux) Si* $(P_i)_{i\in\{1,2,...,r\}}$ *une famille de polynômes de* $\mathbb{K}[X]$ *premiers deux à deux. Alors, en notant* $P = P_1P_2...P_r$*, on a la somme directe suivante* $\ker(P(u)) = \bigoplus_{i=1}^{r} \ker(P_i(u))$.

Preuve 20 *On fait une récurrence sur* $r \geq 2$.

INITIALISATION : si $r = 2$.
Comme P_1 *et* P_2 *sont premiers entre eux, on a par le théorème de Bézout :* $P_1Q_1 + P_2Q_2 = 1$ *où* $Q_1, Q_2 \in \mathbb{K}[X]$.
On a alors en évaluant ces polynômes en u*, puis les endomorphismes obtenus en* $x \in E$*,* $P_1(u)(Q_1(u)(x)) + P_2(u)(Q_2(u)(x)) = x$ *Si* $x \in \ker(P(u))$*, alors* $x = y + z$*, avec* $y = P_1(u)(Q_1(u)(x)) \in \ker(P_2(u))$ *et* $z = P_2(u)(Q_2(u)(x)) \in \ker(P_1(u))$.
Donc $\ker(P(u)) = \ker(P_1(u)) + \ker(P_2(u))$*. Il ne manque plus qu'à prouver que l'intersection est vide. Si* $x \in \ker(P_1(u)) \cap \ker(P_2(u))$*, alors avec la relation de Bézout, écrite plus haut, on obtient* $x = 0$.
Finalement, on a bien : $\ker(P(u)) = \ker(P_1(u)) \bigoplus \ker(P_2(u))$ *et l'initialisation est vérifiée.*

HÉRÉDITÉ : Soit $r \geq 2$ *tel que la propriété soit vérifiée, et montrons qu'elle alors vérifiée au rang* $r + 1$*. Comme* $(P_i)_{i\in\{1,2,...,r+1\}}$ *une famille de polynômes de* $\mathbb{K}[X]$ *premiers deux à deux, alors* P_1 *et* $P_2P_3...P_{r+1}$ *sont deux polynômes premiers entre eux. En effet, soit* $Q \in \mathbb{K}[X]$ *un facteur irréductible commun à ces deux polynômes. Alors* $Q \mid P_2P_3...P_{r+1}$*, par irréductibilité de* Q*,*$\exists i \in \{2, 3..., r + 1\}$ *tel que* $Q \mid P_i$ *mais aussi* $Q \mid P_1$ *et* $\gcd(P_1, P_i) = 1$*, forcément* $Q = cste$*, donc* P_1 *et* $P_2P_3...P_{r+1}$ *sont deux polynômes premiers entre eux. On applique l'initialisation à ces deux polynômes, puis on applique l'hypothèse de récurrence à la famille de* r *polynômes* $(P_i)_{i\in\{2,...,r+1\}}$*, ce qui fournit :* $\ker(P(u)) = \bigoplus_{i=1}^{r+1} \ker(P_i(u))$*, ce qui est exactement la propriété au rang* $r + 1$*, d'où l'hérédité.*

On conclut en évoquant le principe de récurrence.

Définition 49 *u sera dit semi simple si tout sous espace de E, stable par u admet un supplémentaire stable par u.*

Théorème 50 (1er DVLP) *u est semi simple si et seulement si dans la décomposition de* π_u *(le polynôme minimal de u) en irréductibles est sans carrée.*

Exemple 51 *Par exemple, les rotations du plan* $\mathbb{R}^2$ *sont des endomorphismes semi simples.*

Corollaire 52 *u est semi simple sur $\mathbb{K} \iff \exists\, \mathbb{L}$ une extension de $\mathbb{K}$ telle que u est diagonalisable sur $\mathbb{L}$.*

Preuve 21 *Découle du fait que le pgcd et le polynôme minimal sont invariants par extensions de corps et donc que la semi simplicité est elle aussi invariante par extension de corps*[1]*. En effet,*

$\implies$ *alors u est semi simple dans $\mathbb{L}$ une clôture algébrique de $\mathbb{K}$. $\mathbb{L}$ étant algébriquement clos, la semi simplicité équivaut à la diagonalisabilité.*

$\impliedby$ *La diagonalisabilité implique toujours la semi simplicité, donc u est semi simple sur $\mathbb{L}$, donc semi simple sur $\mathbb{K}$.*

Proposition 53 (Décomposition de Dunford généralisée) *Pour* **k** *un corps parfait, on a une généralisation de Dunford : il existe deux uniques endomorphismes n et s tels que :*

1. *$u = n + s$*
2. *n nilpotent et s semi simple*
3. *n et s commutent*

2.3.2 Polynômes cyclotomiques

Définition 54 *On note $\pi_n^* = \{w^k / \gcd(k, n) = 1\} \subseteq \mathbb{U}_n$ où $w = e^{\frac{2i\pi}{n}}$. Et on appelle les éléments de cet ensemble les racines primitives $n-$ème de l'unité.*

Définition 55 *On appelle $n-$ème polynôme cyclotomique, le polynôme $\phi = \prod_{z \in \pi_n^*}(X - z)$ où $w = e^{\frac{2i\pi}{n}}$.*

Lemme 56 *Soit $P, A, B \in \mathbb{Q}[X]$ avec P et A unitaires. Si $P = AB \in \mathbb{Z}[X]$, alors $A, B \in \mathbb{Z}[X]$.*

Preuve 22 *$\exists a, b \in \mathbb{N}^*$ tels que $aA, bB \in \mathbb{Z}[X]$. Et donc $abP = aAbB$ Comme P est unitaire et le contenu multiplicatif, on récupère que $ab = c(aA)c(bB)$, Ainsi $P = \frac{aAbB}{c(aA)c(bB)}$ [a]. Comme P est unitaire, et $\frac{aA}{c(aA)}, \frac{bB}{c(bB)} \in \mathbb{Z}[X]$, en comparant les coefficients dominants, le coefficient dominant du polynôme $\frac{aA}{c(aA)}$ est égal à ± 1. Et comme $\frac{aA}{c(aA)} = A \times \frac{a}{c(aA)}$, A étant unitaire, toujours en comparant les coefficients dominants, forcément $\frac{a}{c(aA)} = \pm 1$. Ainsi $\frac{aA}{c(aA)} \times (\pm 1) = A$ et donc $A \in \mathbb{Z}[X]$. On raisonne de*

1. C'est aussi en ce sens que la semi simplicité est une généralisation « agréable » de la diagonalisabilité. La diagonalisabilité n'est pas invariante par extension de corps.

manière similaire pour B.

a. On a écrit P comme produit de deux polynômes de $\mathbb{Z}[X]$ primitifs.

Proposition 57

1. $\forall n \in \mathbb{N}^*$, $X^n - 1 = \prod_{d|n} \phi_d$.
2. $\forall n \in \mathbb{N}^*, \phi_n \in \mathbb{Z}[X]$.

Preuve 23 *On raisonne par récurrence forte sur $n \in \mathbb{N}^*$.*

$\phi_1 = X - 1 \in \mathbb{Z}[X]$, donc l'initialisation est vérifiée.

Soit $n \geq 2$ et on suppose le résultat vrai aux rangs $k \in \{0, 1, ..., n-1\}$. Montrons le résultat au rang n.

$X^n - 1 = \prod_{d|n} \phi_d = \phi_n \prod_{d|n,\ d\neq n} \phi_d$. Donc d'après l'hypothèse de récurrence $\prod_{d|n,\ d\neq n} \phi_d \in \mathbb{Z}[X] \subseteq \mathbb{Q}[X]$ et unitaire. On fait « une » division euclidienne de $X^n - 1 \in \mathbb{Z}[X]$ par $\prod_{d|n,\ d\neq n} \phi_d$ unitaire. $\exists R, Q \in \mathbb{Z}[X]$ tels que $X^n - 1 = Q \prod_{d|n,\ d\neq n} \phi_d + R$ avec $\deg(R) < \deg(\prod_{d|n,\ d\neq n} \phi_d)$. En faisant la différence, on obtient $R = (\phi_n - Q) \times (\prod_{d|n,\ d\neq n} \phi_d)$. Donc forcément $\phi_n - Q = 0$. D'ou $\phi_n \in \mathbb{Z}[X]$.

On conclut par principe de récurrence que : $\forall n \in \mathbb{N}^*, \phi_n \in \mathbb{Z}[X]$.

Théorème 58 (2 eme DVLP)

1. *Les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$.*
2. ***Petit théorème de Dirichlet*** *Il existe une infinité de nombres premiers congrus à 1 modulo $m \in \mathbb{N}^*$.*

Corollaire 59 *Un groupe abélien fini G est isomorphe au quotient d'un groupe de $(\mathbb{Z}/N\mathbb{Z})^*$ pour un certain N.*

Preuve 24 *Par le théorème de structure des groupes finis, $G \simeq \prod_{k=1}^{r} (\mathbb{Z}/m_k\mathbb{Z})$. Pour chaque $k \in \{1, 2..., r\}$, prenez un nombre premier p_k congrus à 1 modulo m_k tels que $p_1 < p_2 < ... < p_r$. On pose $N = \prod_{k=1}^{r} p_k$. Par le théorème chinois, $(\mathbb{Z}/N\mathbb{Z})^* \simeq \prod_{i=1}^{r} (\mathbb{Z}/p_k\mathbb{Z})^* \simeq \prod_{k=1}^{r} \mathbb{Z}/(p_k - 1)\mathbb{Z}$. Ensuite chaque $m_k \mid p_k - 1$, il existe une surjection (qui est un morphisme aussi) canonique de $\mathbb{Z}/(p_k - 1)\mathbb{Z}$ dans $\mathbb{Z}/m_k\mathbb{Z}$ et donc ensuite de G dans $(\mathbb{Z}/N\mathbb{Z})^*$. Donc par le premier théorème d'isomorphisme, G est un quotient de $(\mathbb{Z}/N\mathbb{Z})^*$.*

Corollaire 60 *Si G est un groupe abélien fini, alors il existe $\mathbb{K}/\mathbb{Q}$ une extension galoisienne finie de $\mathbb{Q}$ tel que $Gal(\mathbb{K}/\mathbb{Q}) \simeq G$.*

Preuve 25 *Considérons le N donné par la preuve précédente. L'extension $\mathbb{Q}(w)/\mathbb{Q}$ où $w = e^{\frac{2i\pi}{N}}$ est galoisienne de groupe $(\mathbb{Z}/N\mathbb{Z})^*$. Ainsi G est quotient de $Gal(\mathbb{Q}(w)/\mathbb{Q})$. Ainsi il existe H un sous groupe distingué de $Gal(\mathbb{Q}(w)/\mathbb{Q})$. D'après la correspondance de Galois, il existe un corps intermédiaire $\mathbb{L}$ de $\mathbb{Q}(w)/\mathbb{Q}$, tel que $Gal(\mathbb{Q}(w)/\mathbb{L}) = \mathbb{H}$. Comme $Gal(\mathbb{Q}(w)/\mathbb{L})$, est distingué , $L/\mathbb{Q}$ est galoisienne et $Gal(\mathbb{Q}(w)/\mathbb{Q})/Gal(\mathbb{Q}(w)/\mathbb{L}) \simeq Gal(\mathbb{L}/\mathbb{Q})$. Ce qui conclut.*

3 Motivation du plan

Le plan présenté est assez classique. Découpé en trois parties, il s'attarde d'abord sur l'introduction de la notion d'irréductibilité, en présentant des premiers critères. Les polynômes irréductibles, donnant naissance à des idéaux maximaux dans les anneaux de polynômes, la notion d'extension de corps apparaît naturellement et plus encore quand on se met à chercher leurs racines. La partie 2 propose alors d'explorer ce sujet, en récupérant au passage quelques critères. Enfin dans une dernière partie, on présente des applications. En premier lieu en algèbre linéaire avec les endomorphismes semi simples que l'on peut dire reconnaissables via la décomposition en irréductibles de leur polynôme minimal. Et enfin, la cyclotomie est un bon exemple d'illustration qui permet d'utiliser et de pratiquer la notion irréductibilité, tout en montrant un résultat sur une famille de polynômes connus et usuels. On aurait pu rajouter une dernière sous partie qui s'attarde sur la construction des corps finis via les polynômes irréductibles et présenter le troisième développement que j'ai rédigé.

4 Développements

4.1 1er développement : Caractérisation des endomorphismes semi simples

Théorème 61 (1er DVLP) *u est semi simple si et seulement si dans la décomposition de π_u (le polynôme minimal de u) en irréductibles est sans carrée.*

Preuve 26 *On suppose u semi simple.*
Par l'absurde sur supposons que $\pi_u = PQ^2$ où $Q \in \mathbb{K}[X]\backslash K$ et $P \in \mathbb{K}[X]$. On considère le sous espace vectoriel $F = \ker(Q(u))$. F est stable par u, comme u est semi simple, il existe un supplémentaire G lui aussi stable par u.

Par définition de F, $PQ(u)(F) \subseteq \{0\}$. (δ) Comme G est stable par u, G est aussi stable par $PQ(u)$, donc $PQ(u)(G) \subseteq G$. Comme π_u annule u, $PQ(u)(E) \subseteq F$, en particulier $PQ(u)(G) \subseteq F$. Donc $PQ(u)(G) \subseteq F \cap G = \{0\}$ car $F \bigoplus G$ $(\delta\delta)$ Comme $E = F + G$, avec (δ) et $(\delta\delta)$, on a $PQ(u)(E) \subseteq \{0\}$ Donc le polynôme PQ annule u et est de degré strictement inférieur à π_u... ABSURDE. Donc $Q \in \mathbb{K}$, et donc π_u n'a pas de facteur carré dans sa décomposition en irréductibles.

On traite d'abord le cas ou π_u est un polynôme irréductible. On suppose $\pi_u \in \mathbb{K}[X]$ irréductible et montrons que u est semi simple. Soit F un sous espace u-stable. Si $F = E$, c'est clair : $G = \{0\}$ convient. Sinon $F \neq E$ et $\exists x_1 \in E\backslash F$. $I_{x_1} = \{P \in \mathbb{K}[X]/P(u)(x_1) = 0\}$ est un idéal de $\mathbb{K}[X]$ qui est un anneau principal donc il existe un unique polynôme unitaire tel que $I_{x_1} = (\Pi_{x_1})$ [a]. $\Pi_u \in I_{x_1} = (\Pi_{x_1})$ donc $\pi_{x_1,u} \mid \pi_u$, et par irréductibilité de π_u, $\pi_u = \pi_{x_1,u}$. et donc $\pi_{x_1,u}$ est irréductible. $E_{x_1} = \{P(u)(x_1)/P \in \mathbb{K}[X]\}$ (le sous espace cyclique de u associé à x_1). Montrons que $E_{x_1} \cap F = \{0\}$. Si $y \in E_{x_1} \cap F$ et non nul. $y \in E_{x_1} \exists P \in \mathbb{K}[X]$ tel que $y = P(u)(x_1) \neq 0$. Ainsi $P \notin (\pi_{x_1,u})$ ce qui veut dire que $\pi_{x_1,u} \nmid P$, et comme $\pi_{x_1,u}$ est irréductible, P et $\pi_{x_1,u}$ sont premiers entre eux. Avec le théorème de Bézout, on obtient dès lors que $\exists U, V \in \mathbb{K}[X]$ tels que $U\pi_{x_1,u} + VP = 1$. En évaluant cette égalité de polynômes par l'endomorphisme u, puis en évaluant les endomorphismes obtenus en x_1, on a que $x_1 = (VP)(u)(x_1) = V(u)(y) \in F$ car $y \in F$ qui u-stable. Mais par définition $x_1 \notin F$... ABSURDE. Donc $E_{x_1} \cap F = \{0\}$, on peut écrire $E_{x_1} \bigoplus F$.
Maintenant ou bien $E = E_{x_1} \bigoplus F$ et c'est terminé. Sinon on refait le procédé que l'on vient de faire mais cette fois ci avec le sous espace $E_{x_1} \bigoplus F$. En itérant ainsi le procédé on obtient $k \in \mathbb{N}^*$, des vecteurs $x_1, x_2, ..., x_k$ tels que $E = \underbrace{E_{x_1} \bigoplus E_{x_2} \bigoplus ... \bigoplus E_{x_k}}_{\textbf{le sous espace } u\textbf{-stable cherché}} \bigoplus F$.
Le processus est bien fini car $\dim(E_{x_i}) \geq 1$ [b] donc comme E est de dimension finie, le processus s'arrête au bout d'un nombre fini d'étapes.

Maintenant on traite le cas général, supposons que $\pi_u = P_1P_2...P_r$ décomposition en irréductible de π_u sans facteurs carrés. Soit F un sous espace u-stable. En appliquant

le lemme des noyaux à u, on récupère $E = \bigoplus_{i=1}^{r} F_i$ où $F_i = \ker(P_i(u))$. $\pi_{u_i} = P_i$ car P_i annule u_i et P_i irréductible. π_{u_i} est alors irréductible , par ce qui a été fait précédemment on obtient u_i est semi-simple, donc en considérant $F_i \cap F$ qui est stable par u_i, on a G_i u_i-stable tel que $F_i = (F_i \cap F) \bigoplus G_i$
u_F est annulé par π_u , en réappliquant le lemme des noyaux mais cette fois ci avec u_{F_i}, on récupère que $F = \bigoplus_{i=1}^{r} \ker(P_i(u_F)) = \bigoplus_{i=1}^{r} F_i \cap F$.

$$E = \bigoplus_{i=1}^{r} F_i = \bigoplus_{i=1}^{r}((F_i \cap F) \bigoplus G_i) = \underbrace{(\bigoplus_{i=1}^{r}(F_i \cap F))}_{=F} \bigoplus \underbrace{(\bigoplus_{i=0}^{r} G_i)}_{\textbf{sous espace } u\textbf{-stable}} .$$

On conclut quant à l'équivalence souhaitée.

a. On appelle ce polynôme **polynôme local de u en x_1**
b. Puisque (E_{x_i} contient $x_i \neq 0$)

Motivation du développement :
Ce théorème est intéressant pour deux principales raisons. La première c'est qu'il illustre la puissance de pouvoir décomposer des polynômes en produit d'irréductibles. Et la seconde c'est qu'il permet de voir que la question d'irréductibilité n'est pas un « monde d'entre soi » et qu'elle se manifeste dans d'autres domaines des maths (résonnant au titre application de la leçon).

4.2 2eme développement : Irréductibilité des polynômes cyclotomiques et théorème faible de Dirichlet

Théorème 62 (2 eme DVLP) *1. Les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$.*
*2. **Petit théorème de Dirichlet** Il existe une infinité de nombres premiers congrus à 1 modulo $m > 1$.*

Preuve 27 *Soit $w \in \pi_n^*$, et on note $f = Irr_{\mathbb{Q}}(w) \in \mathbb{Q}[X]$ =. On va montrer $f = \phi_n(X)$ ce qui prouvera l'irréductibilité recherchée. Comme $X^n - 1$ annule w, $f \mid X^n - 1 \in \mathbb{Z}[X]$ donc $X^n - 1 = h(X)f(X)$ et f est polynôme unitaire. Par le lemme 56, $h, f \in \mathbb{Z}[X]$.*

Montrons maintenant le fait suivant : Si u est une racine de f, alors pour tout nombre premier p ne divisant pas n, u^p est aussi racine de f.

Soitu une racine de f et p un tel nombre. u est une racine nème de l'unité car $f \mid X^n - 1$, donc u^p est aussi racine n-ème de l'unité. Donc $f(u^p)h(u^p) = 0$. Si, par l'absurde, $f(u^p) \neq 0$, alors $h(u^p) = 0$, donc u est une racine du polynôme $h(X^p)$. Et, comme f est irréductible sur $\mathbb{Q}$ et annule u, on récupère que $f = Irr_{\mathbb{Q}}(u)$, donc $f \mid h(X^p)$ dit autrement $\exists g \in \mathbb{Q}[X]$, tel que $h(X^p) = g(X)f(X)$. Et encore d'après le lemme n°56 , $g(X) \in \mathbb{Z}[X]$. En réduisant l'égalité modulo p, on en déduit que $\overline{h(X^p)} = \overline{h(X)}^p = \overline{f(X)}\ \overline{g(X)}$. Soit $\theta \in \mathbb{F}_p[X]$ un facteur irréductible de

$\overline{f(X)}$. Alors $\theta \mid \overline{h(X)}^p$ (dans $\mathbb{F}_p[X]$). Or θ étant irréductible sur $\mathbb{F}_p$, $\theta \mid \overline{h(X)}$. Et puis comme $X^n - \bar{1} = \overline{f(X)}\ \overline{h(X)}$, $\theta^2 \mid X^n - \bar{1}$. Mais $X^n - \bar{1}$ n'a pas de racine multiple puisque$(X^n - \bar{1})' = nX^{n-1} \neq 0$ (car $p \nmid n$) et $\gcd((X^n - \bar{1})', (X^n - \bar{1})) = 1$. Ce qui constitue alors une contradiction (θ^2 a des racines multiples). Donc $f(u^p) = 0$.

Comme w est racine de f, et comme toute racine primitive n-ème de l'unité, c'est-à-dire les w^k avec k premier avec n, peut s'obtenir en élevant w à des puissances de p qui ne divisent pas n , ce que l'on vient de montrer c'est que $\{$racines de $f\} \supseteq \pi_n^*$ et ainsi $\varphi(n) \leq \deg(f)$. Mais $f \mid \phi_n$ (car ϕ_n annule w), d'où $\deg(f) \leq \varphi(n)$, donc $\deg(f) = \varphi(n) = \deg(\phi_n)$. Deux polynômes unitaires , de même degré, dont l'un divise l'autre sont nécessairement égaux, donc on conclut $f = \phi_n = \prod_{gcd(k,n)=1}(X - w^k)$ et ϕ_n irréductible sur $\mathbb{Q}$ et aussi sur $\mathbb{Z}$ car ϕ_n unitaire.

On va montrer que pour tout nombre $k > m$, il existe un nombre premier $p > k$ congrus à 1 modulo m. Soit $k > m$ alors $\phi_m(k!) \geq 2$ car $|\phi_n(k!)| = \prod_{gcd(j,n)=1} |k! - w^j| > \prod_{gcd(j,n)=1} ||k!| - |w^j|| > \prod_{gcd(j,n)=1} ||k!| - 1| > \prod_{gcd(j,n)=1}(k! - 1) > 1$. On prend p un facteur premier quelconque de $\phi_m(k!)$ Si $p < k$ alors$p \mid \phi_m(k!) - \phi_m(0)$, donc $p \mid \pm 1$ ABSURDE[a] Donc $p > k > m$, d'ou p et m premiers entre eux. On doit maintenant prouver que $p \equiv 1[m] \iff m \mid p - 1$. Il suffit donc de trouver un élément $x \in \mathbb{F}_p^*$ d'ordre m. On pose $x = \overline{k!}$. On a $\overline{\phi_m(x)} = 0$, comme $\overline{\phi_m}(X) \mid X^m - \bar{1}$, on a bien $x^m = 1$ (dans $\mathbb{F}_p^*$). En notant c l'ordre de x, on a alors $c \mid m$ et suppose, par l'absurde que $c < m$. ALors puisque $x^c - 1 = 0$ on a que $\prod_{d|c} \overline{\phi_d}(x) = 0$. Donc il existe $d \mid c$ tel que $\overline{\phi_d}(x) = 0$. $(d < c < m)$. Donc $\overline{\phi_d}\ \overline{\phi_m} \mid \overline{X^m - 1}$. Donc $\overline{X^m - 1}$ a une double racine, mais par le même argument que précédemment, comme $p \nmid m$, ceci constitue une contradiction.

Finalement on a bien obtenu ce que l'on voulait il existe une infinité de nombres premiers congrus à 1 modulo $m \in \mathbb{N}^*$.

a. En effet $\phi_m(0) = \pm 1$ car c'est un entier relatif de module 1 car produit des racines de ϕ_m .

Motivation du développement :

Il s'agit d'un résultat remarquable sur une famille de polynômes connuss et classiques. Il met bien en évidence le bon comportement des éléments irréductibles en termes de division quand ils divisent un produit. Le bémol : on pourrait reprocher que le théorème faible de Dirichlet soit un peu hors sujet. Mais si cette peur apparaît, remplacez le théorème faible de Dirichlet par le calcul du degré d'une extension cyclotomique.

4.3 3eme développement : Compter les polynômes irréductibles unitaires de degré $n \in \mathbb{N}^*$ sur $\mathbb{F}_q$

Soit p un nombre premier et $r \in \mathbb{N}^*$, et on pose $q = p^r$. On introduit la quantité égale à $M(n,q) = \{P \in \mathbb{F}_q[X] / \deg(P) = n, \text{P irréductible et unitaires }\}$. Et on note

$$\mu(n) = \begin{cases} (-1)^r & \text{si n est produit r nombres premiers distincts} \\ 0 & \text{sinon.} \end{cases}$$

En plus de $I(n,q) = |M(n,q)|$.

On va montrer

Proposition 63 $X^{q^n} - X = \prod_{d|n} \prod_{P \in M(d,q)} P$

Preuve 28 *Soit $P \in M(d,q)$ avec $d \mid n$. On note $\mathbb{V} = \mathbb{F}_q[X]/(P)$ un corps de rupture de P sur $\mathbb{F}_q$, Comme V est de cardinal q^d, $\forall x \in V, x^{q^d} = x$. Or $d \mid n$ donc $\exists k \in \mathbb{N}$ tel que $n = kd$ et alors $x^{q^n} = x^{q^{kd}} = x^{\underbrace{q^d \times q^d \times \ldots \times q^d}_{k \text{ fois}}} = x^{q^d q^d q^{d \cdots}} = x$.*

En appliquant cette formule pour $x := X \mod (P)$, on a que le polynôme $X^{p^n} - X$ annule x dont le polynôme minimal sur $\mathbb{F}_q$ est P. D'où $P \mid X^{p^n} - X$ et par un lemme de Gauss on récupère que $(\prod_{d|n} \prod_{P \in M(d,q)} P) \mid X^{q^n} - X$

De plus ,

Soit $P \in \mathbb{F}_q[X]$ un facteur irréductible de degré $d \in \mathbb{N}^*$ de $X^{q^n} - X \in \mathbb{F}_q[X]$. Comme $P \in \mathbb{F}_{q^n}$ est le corps de décomposition sur $\mathbb{F}_q$ de $X^{q^n} - X$, $X^{q^n} - X$ est scindé sur $\mathbb{F}_{q^n}$, donc P est également scindé sur F_{q^n}. En notant $\mathbb{V} = \mathbb{F}_q[X]/(P)$ un corps de rupture sur $\mathbb{F}_q$ de P, on a d'après la formule de la base télescopique :

$[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{V}] \underbrace{[\mathbb{V} : \mathbb{F}_q]}_{=\deg(P)=d}$ *. Donc $d \mid n$. Il suffit donc maintenant de justifier que $X^{q^n} - X$ n'a pas de racine double. Et en effet $(X^{q^n} - X)' = q^n X^{q^n - 1} - 1 = -1 \neq 0$ et $\gcd(X^{q^n} - X, -1) = 1$, donc $X^{q^n} - X$ n'a pas de racine double.*

Bilan on a bien que $X^{q^n} - X = \prod_{d|n} \prod_{P \in M(d,q)} P$

Pour en déduire le corollaire suivant :

Théorème 64 $I(n,q) = \frac{1}{n} \sum_{d|n} \mu(\frac{n}{d}) q^d$.

Preuve 29 *En comparant les degrés on établit que* $q^n = \sum_{d|n} qI(d,q)$ *puis en utilisant la formule d'inversion de Mobius on récupère pile ce que l'on souhaitait :* $I(n,q) = \frac{1}{n}\sum_{d|n}\mu(\frac{n}{d})q^d$.

Pour cela on aura besoin d'un lemme.

Lemme 65 (Formule d'inversion) *On pose* $G(n) = \sum_{d|n} g(d)$ *avec* $g : \mathbb{N} \longrightarrow \mathbb{C}$. *Alors* $g(n) = \sum_{d|n} G(d)\mu(\frac{n}{d})$.

Preuve 30 *Déjà, remarquons que pour* $n \geq 2$, *on* $\sum_{d|n}\mu(d) = 0$. *En effet, en décomposant* n *en produits de nombres premiers,* $n = \prod_{k=1}^{s} p_i^{\alpha_i}$, *les diviseurs de* n *qui ,ne s'annulent pas en la fonction* μ *sont les* $d = \prod_{i=0}^{s} p_i^{\epsilon_i}$ *où* $\epsilon_i = 0$ *ou* 1. *Donc* $\sum_{d|n}\mu(d) = \sum_{i=0}^{s}\binom{s}{i}(-1)^i = (1-1)^s = 0$.

De plus, pour $d \mid n$, *on a* $d' \mid \frac{n}{d} \iff dd' \mid n$. *Ainsi* $\sum_{d|n} G(\frac{n}{d})\mu(d)$
$= \sum_{d|n}\mu(d)\sum_{d'|\frac{n}{d}} g(d') = \sum_{dd'|n} g(d')\mu(d) = \sum_{d'|n}\sum_{d|\frac{n}{d'}} g(d')\mu(d) = g(n)$.

Motivation du développement :

Ce développement est très joli et utile. Utile car il parle de polynômes irréductibles sur les corps finis, ce qui permet de construire les corps finis. En comptant les polynômes irréductibles, on peut alors construire de manière explicites des corps de types $\mathbb{F}_{q^n}$ comme extension de $\mathbb{F}_q$. De plus, il met en évidence, la notion de corps de rupture (illustrant à ce propos la leçon). Et la beauté est normalement subjective mais là quand même c'est assez unanime je pense.

5 Complément : autour du théorème de Selmer 1956

Enfin, je rédige une dernière partie sur un problème portant sur l'étude d'irréductibilité d'une famille de polynômes, un peu plus connu sous le nom de théorème de Selmon dont la présentation suit celle du papier de Keith Conrad (voir sources).

Théorème 66 (Selmer, 1956) *Pour $n > 1$, le polynôme $X^n - X - 1$ est irréductible sur $\mathbb{Q}$*

Aucun des tests classiques (tels que le critère d'Eisenstein ou l'irréductibilité passant modulo p) ne fonctionnent pour prouver l'irréductibilité de ce polynôme.

Cependant pour certaines valeurs particulières de n, certains de ces tests peuvent être appliqués.

Par exemple, pour $n = p$, un nombre premier, alors $X^p - X - 1$ est irréductible dans $\mathbb{F}_p[X]$ donc sur $\mathbb{Z}$ puis sur $\mathbb{Q}$.

Soit $f(X) = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0 \in \mathbb{K}[X]$, avec $\mathbb{K}$ un corps de caractéristique 0.

Définition 67 *On appelle* ***le polynôme réciproque*** *de f, $f^*(X) = X^{deg(f)} f(\frac{1}{X}) \in \mathbb{K}[X]$.*

Remarque 68 *Ce polynôme s'appelle polynôme réciproque car ses racines sont les inverses de celle de f, plus précisément, si $f(0) = a_0 \neq 0$, $f(X) = a_n(X - r_1)(X - r_2)...(X - r_n)$ et $f(X) = f(0)(X - \frac{1}{r_1})(X - \frac{1}{r_2})...(X - \frac{1}{r_n})$.*

Les propriétés sont les suivantes :

Proposition 69

1. *Si $f(0) \neq 0$ alors $deg(f) = deg(f^*)$ et $f^{**} = f$*
2. *$f = gh \implies f^* = g^* h^*$ (prop de multiplicativité)*
3. *Si $f(X) = \Sigma_{k=0}^{n} a_k X^k$ de degré n, alors le coefficient devant X^n de ff^* est $a_0^2 + a_1^2 + ... + a_n^2$*

On présente une preuve du théorème de Selmer en trois étapes :

Étape 1 : $\forall n \geq 2, P(X) = X^n - X - 1$ et son polynôme réciproque $P(X)^* = -X^n - X^{n-1} + 1$ n'ont aucune racine en commun.

En effet supposons par l'absurde que ces deux polynômes partagent une racine en commun disons $\alpha \neq 0$. Alors $\alpha^n = \alpha + 1$ et $\alpha^n = -\alpha^{n-1} + 1$ et $\alpha^n = -\alpha^{n-1} + 1$ donc $-\alpha^{n-1} = \alpha \iff \alpha^n = -\alpha^2$ En remplaçant dans la première équation on obtient $\alpha^2 + \alpha + 1 = 0$. Ce qui implique que $\alpha^3 = 1$, ainsi $\alpha^n \in \{1, \alpha, \alpha^2\}$. Avec la première équation, on deduit qu'on a forcément $\alpha^n = \alpha^2$, alors avec les deux premières équations, on récupère $\alpha + 1 = -\alpha + 1$, ce qui est absurde. On conclut que ces deux polynômes n'ont aucune racine en commun.

Étape 2 : Pour $f(X) \in \mathbb{Z}[X]$ tel que $f(0) \neq 0$ et que f et f^* n'ont aucune racine en commun. Si $f(X) = g(X)h(X)$ avec g et h à coefficients dans $\mathbb{Z}$, non constants, alors $\exists k(X) \in \mathbb{Z}[X]$ tel que $deg(k) = deg(f)$ et $ff^* = kk^*$ où $k \notin \{\pm f, \pm f^*\}$

Comme $f(0) \neq 0$, on a que $g(0) \neq 0$ et $h(0) \neq 0$, alors $deg(h) = deg(h^*)$ et $deg(g) = deg(g^*)$; on pose $k = gh^*$.

Si $k = \pm f$, alors $gh^* = \pm gh$ et ensuite $h = \pm h^*$, mais alors toutes les racines de h, qui sont les mêmes que celles de h^*, seraient des racines communes à $f = gh$ et $f^* = g^*h^*$. Or f et f^* n'ont pas de racines en commun... ABSURDE. Raisonnement similaire si $k = \pm f^*$.

Étape 3 [preuve de l'irréductibilité de $X^n - X - 1$ sur $\mathbb{Q}$]

Le cas $n = 2$ est facile. (car il n'y a pas de racine dans $\mathbb{Q}$, et le polynôme est de degré 2.)

On suppose $n > 2$.

Par l'absurde supposons que $f = gh$ où g et h ne sont pas inversibles dans $\mathbb{Z}[X]$. Notons $f(X) = X^n - X - 1$. En vertu de l'étape 1 et 2, $\exists k \in \mathbb{Z}[X]$ tel que $deg(k) = n$, $kk^* = ff^*$ et $\{\pm f, \pm f^*\}$. On écrit $k(X) = b_nX^n + b_{n-1}x^{n-1} + ... + b_1X + b_0$ alors $k(X)^* = b_oX^n + b_1X^{n-1} + ... + b_n$. De plus $kk^*(0) = ff^*(0) = -1 \times 1 = -1 = b_0b_n$, ainsi $b_n = \pm 1$ et $b_0 = -b_n$. quitte à remplacer k par $-k$, on peut supposer sans perte de généralité que $b_n = 1$ et $b_0 = -1$.

Or comme $ff^* = kk^*$, En comparant le coefficient devant X^n :

$1^2 + (-1)^2 + (-1)^2 = b_0^2 + b_1^2 + ... + b_n^2$, et comme $b_0^2 = b_n^2 = 1$, on a $b_1^2 + ... + b_{n-1}^2 = 1$ et les $b_i \in \mathbb{Z}$. La seule possibilité c'est qu'il existe un unique $i \in \{1, 2, ..., n-1\}$ tel que $b_i = \pm 1$ et $\forall j \in \{1, 2, ..., n-1\} - \{i\}, b_j = 0$; $\implies k(X) = X^n + b_iX^i - 1$.

Intéressons nous aux termes de degré supérieur (strictement) à n :

$ff^* = (X^n - X - 1)(-X^n - X + 1) = -X^{2n} - X^{2n-1} + X^{n+1} + ...$ $kk^* = (X^n + b_iX^i - 1)(X^n + b_iX^i + 1) = -X^{2n} + b_iX^{2n-i} - b_iX^{n+i} + ...$

donc $-X^{2n} + b_iX^{2n-i} - b_iX^{n+i} + ... = -X^{2n} - X^{2n-1} + X^{n+1} + ...$

Le terme à droite à 3 termes de degrés plus grand (strictement) que n, en effet comme on a $n > 2$, on a $2n > 2n - 1 > n + 1$. Le terme à gauche doit alors lui aussi avoir 3 termes plus grand que n ; pour cela on doit nécessairement avoir $2n - i \neq n + i$.

Alors

1. ou bien $2n - i > n + i$ et donc $2n - i = 2n - 1 \implies i = 1, b_i = -1 \implies k(X) = X^n - X - 1 = f$
2. ou bien $2n - i < n + i$ et donc $2n - 1 = n + i \implies i = n - 1 \implies k(X) = x^n + x^{n-1} - 1 = -f^*$

Ce qui dans les deux cas constitue une contradiction puisque $k \notin \{\pm f, \pm f^*\}$.

On conclut comme souhaité à l'irréductibilité du polynôme $X^n - X - 1$ sur $\mathbb{Z}$ puis sur $\mathbb{Q}$.

L'argument que l'on vient de donner peut presque être appliqué pour les polynômes $P_{m,n} = X^n \pm X^m \pm 1$. Plus précisément ce que l'on vient de faire se généralise en le théorème suivant :

Théorème 70 *Soit $1 < m < n$ tel que $m \neq \frac{n}{2}$. Le polynôme $P_{m,n} = X^n \pm X^m \pm 1$ est irréductible sur $\mathbb{Q}$ si et seulement si il n'a aucune racine en commun avec son polynôme réciproque.*

6 Questions (possibles) de jury

1. Démontrer quelques propositions et/ou détailler des exemples, applications du plan.
2. Le polynôme $X^n - X + 1$ est il scindé à racines simples ? Calculer $\sum_{x \ racines} \frac{1}{x}$.
3. (orientée algèbre linéaire) Démontrer que : Seuls E et $\{0\}$ sont des sous-espaces u-stables $\iff \chi_u \in \mathbb{K}[X]$ est irréductible sur $\mathbb{K}$.
4. Les éléments de la décomposition de Dunford d'une matrice réelle (vu comme une matrice complexe) sont réels. Reélle ou pas comme affirmation ? Et si la matrice est rationnelle ? C'est rationnel de penser que ça reste rationnel ?
5. Comparaison corps de rupture et corps de décomposition d'un polynôme irréductible sur $\mathbb{F}_q$.
6. Argument direct pour l'existence d'un polynôme irréductible de degré $m \geq 1$ sur $\mathbb{F}_q$.

Preuve 31 *1. Voir les preuves plus haut.*

2. On se place en caractéristique 0. *Déjà avec la proposition n°7 , on peut dire que* $X^n - X - 1$ *n'a pas de racines dans* $\mathbb{Q}$. *Il n'est pas scindé sur* $\mathbb{Q}$. *Ce polynôme est à racines simples car il est premier avec son polynôme dérivé qui est non nul. En effet supposons que* P *et* P' *ont une racine en commun. Alors* $\alpha^n - \alpha + 1 = 0$ *et* $n\alpha^{n-1} - 1 = 0 \iff n\alpha^n = \alpha$. *Donc en multipliant la première équation par* n *et en remplaçant* $n\alpha^n$ *par* α *; on obtient* $(1-n)\alpha + n = 0$, *donc* $\alpha = \frac{n}{1-n} \in \mathbb{Q}$... *Absurde* P *n'a pas de racine dans* $\mathbb{Q}$.

Concernant le calcul de la somme, un œil avisé aura vu qu'il est pertinent de faire appel aux relations coefficients-racines, mais la question reste de savoir comment récupérer l'inverse des racines. Astuce du jour : considérer le polynôme réciproque dont les racines sont exactement les $\frac{1}{x}$ *quand* x *parcourt les racines de* P.[2] *Ainsi la somme est égale au coefficient devant le* X^{n-1} *(au signe près) de* $P^* = X^n - X^{n-1} + 1$ *qui est* -1 . *En clair,* $\sum_{x \ racines} \frac{1}{x} = 1$.

3. On suppose E *n'est pas l'espace nul (sinon il n'a rien a montré).*

Supposons que χ_u *soit irréductible. Soit* F *un sous espace u-stable non réduit* $\{0\}$. *Alors, on considère* u_F *l'endomorphisme de* F *induit par* u. *Par le théorème de Cayley-Hamilton,*χ_u *annule* u *donc annule* u_F. *Ainsi* $\pi_{u_F} \mid \chi_u$, *par irréductibilité de* χ_u, $\pi_{u_F} = \chi_u$,*donc* $n \geq \dim(F) =$[3]$\dim(\chi_{u_F}) \geq \deg(\pi_{u_F}) = \deg(\chi_u) = n$. *En clair* $\dim(F) = n$ *donc* $F = E$.

Réciproquement supposons que seuls E *et* $\{0\}$ *sont des sous-espaces u-stables. Si* $\chi_u = PQ$ (δ). *avec* P *et* Q *non constants et premiers entre eux. Si* $F, G = \{0\}$, *alors*

2. car $P(0) \neq 0$.
3. Le polynôme caractéristique d'un endomorphisme est toujours égal à la dimension de l'espace quand celui ci n'est pas l'espace nul et on a bien dit $F \neq \{0\}$

le lemme des noyaux donne $E = F \bigoplus G = \{0\}$*, impossible. Sans perte de généralité* $F \neq \{0\}$ *donc* $F = E$ *et il existe* $x \in F = E \backslash \{0\}$*. En notant* $d = \deg(P) \notin \{0, n\}$*, comme* F *u-stable, et* $x \in F$ *on a que* $\forall i \in \{0, 1, ..., d-1\}, u^i(x) \in F$ *et, l'espace engendrée par cette famille,* $\Delta = vect(u^i(x)/i \in \{0, 1, ..., d-1\})$ *est au au plus de dimension* d *et au moins de dimension* 1 *car* x *non nul. Mais* Δ *est u-stable car* $u^d(x) \in \Delta$ *puisque* $P(u) = 0$*. Donc par hypothèse de départ* $\Delta = \{0\}$ *ou* E*, mais cela contredit sa dimension !* χ_u *est irréductible*

4. *Pour la cas rationnel (*$A \in M_n(\mathbb{Q})$*), ça reste vrai mais c'est un peu plus délicat. Je pense qu'il y a deux façons de voir les choses.*

   La première façon est de se demander, en pratique, c'est-à-dire concrètement dans la vraie vie, comment fait-on pour obtenir la décomposition de Dunford d'une matrice ? Dans les cas simples où la matrice est diagonalisables ou nilpotente, c'est immédiat la matrice $+0$ *constitue sa décomposition de Dunford. Sinon c'est pas immédiat.*
   Il existe en fait une méthode constructive pour récupérer la décomposition de Dunford d'une matrice : méthode de Newton en algèbre. Ainsi on voit alors que les éléments de la décomposition de Dunford de A *vont rester à coefficients dans* $\mathbb{Q}$ *par construction.*

   Le deuxième point de vue, est un point de vue complètement opposé à cette descente sur la terre ferme, au contraire elle va encore plus dans l'abstraction en allant chercher la théorie de Galois ! En effet on note $\chi_A \in \mathbb{Q}[X]$ *le polynôme caractéristique de* A *et* $\mathbb{L}$ *son corps de décomposition.* $\chi_A \in \mathbb{Q}[X]$ *est scindé sur* $\mathbb{L}$*,* A *admet donc une décomposition de Dunford sur* $\mathbb{L}$*, disons* $A = N + D$ *où* $N \in M_n(\mathbb{L})$ *et* $D \in M_n(\mathbb{L})$*.*

   $\mathbb{L}/\mathbb{Q}$ *est galoisienne (finie) puisqu'elle est normale (c'est un corps de décomposition) et aussi séparable car* $\mathbb{Q}$ *est un corps parfait (il est de caractéristique* 0*).*

   Donc $\mathbb{L}^{Gal(\mathbb{L}/\mathbb{Q})} = \mathbb{Q}$*.*

   Donc on veut prouver $D, N \in M_n(\mathbb{L}^{Gal(\mathbb{L}/\mathbb{Q})}) = M_n(\mathbb{Q})$*.*

   Pour $\sigma \in Gal(\mathbb{L}/\mathbb{Q})$*. On note* $A^\sigma = (\sigma(a_{i,j}))_{i,j}$*. Alors* $D+N = A = A^\sigma = D^\sigma + N^\sigma$*. Par unicité, de la décomposition de Dunford sur* $\mathbb{L}$*,* $D^\sigma = D$ *et* $N^\sigma = N$*. Ce qui veut dire que l'on obtient ce que nous voulions.*

5. *Soit* $P \in \mathbb{F}_q[X]$ *irréductible et on note* $d = \deg(P)$*. Montrons que son corps de rupture est son corps de décomposition.*
   Soit $\mathbb{F}_q(a)$ *son corps de rupture. Alors on remarque que* $(h^k(a))_{0 \leq k \leq d-1}$ *où* h *est l'application*
   $$\begin{array}{rccc} h & : & \mathbb{F}_q(a) & \to & \mathbb{F}_q(a) \\ & & x & \mapsto & x^q \end{array}$$
   sont des racines de P *tous dans le corps de rupture de* P*. Si elles sont toutes différentes alors le corps de rupture contient toutes les racines de* P*, ce qui montre*

que c'est le corps de décomposition.

Supposons $\exists 0 \leq j < i \leq d-1$ *tel que* $h^i(a) = h^j(a)$*, alors* $a^{q^i} = a^{q^j}$ *, donc en composant par* h^{d-i}*, on a (avec Fermat notamment) :* $a = a^{q^{d+j-i}}$*. Donc* P *qui est le polynôme minimal de* a*, divise* $X^{q^{d+j-i}} - X$*. Or par le développement* 3*,* P *étant irréductible sur* $\mathbb{F}_q$*, on a que* $d \mid d+j-i = d-(i-j) < d$*... ABSURDE donc les racines sont toutes distinctes, ce qui conclut.*

6. *Oui ceci découle du théorème de l'élément primitif pour les corps finis*[4]*. En effet, plus précisément, pour tout* $m \in \mathbb{N}^*$*, en prenant un élément* b *générateur du groupe cyclique* $F^*_{q^m}$*, on a que* $F_q(b) = \mathbb{F}_{q^m}$*. Le polynôme minimal de* b *est alors un polynôme irréductible sur* $\mathbb{F}_q$ *de degré* m*.*

4. Ce théorème reste vrai pour les corps infinis tant que l'extension de corps est séparable et finie.

Références

[GOU] Xavier Gourdon, *Les maths en tête. Algèbre et probabilités*, ELLIPSES 3e édition, 2021.

[OBJ] Vincent Beck, *Objectif Agrégation*, H K Eds, 2005.

[calA] Josette Calais, *Eléments de la théorie des anneaux : Anneaux commutatifs, Niveau L3*, ellipses, 2006.

[GOZ] Yvan Gozard, *Théorie de Galois : Niveau L3-M1*, ellipses 2e édition, 2009.

[Per] Daniel Perrin, *Cours d'algèbre*, ellipses, 1998.

https://kconrad.math.uconn.edu/blurbs/ringtheory/irredselmerpoly.pdf, de Keith Conrad, *irreductibility of* $x^n - x - 1$

https://www.agreg-maths.fr/uploads/versions/5425/dirichlet%20faible%20et%20application.pdf, de Thibault Monneret *Polynômes cyclotomiques + Dirichlet faible +Application aux GAF + Bonus : Galois inverse*