

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 télescopique, 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 $\mathbb{Q}$ 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.

Références

- [Algèbre - le Grand combat - Berhuy](#)
- [Cours d'Algèbre - Daniel Perrin](#)
- [Théorie de Galois - Escofier](#)
- [Mathématiques pour l'Agrégation \(Algèbre\) - J.E. Rombaldi](#)
- [Objectif agrégation](#)

Développements

- [Cyclotomie](#) (dans $\mathbb{F}_q$)
- [Algorithme de Berlekamp](#)

Méta-plan

1. Irréductibilité
 1. Polynômes irréductibles

- 2. Contenu d'un polynôme. Irréductibilité sur un anneau.
- 3. Cyclotomie : prélude
- 2. Extensions algébriques
 - 1. Algébricité, polynôme minimal
 - 2. Corps de rupture, corps de décomposition
- 3. Corps finis
 - 1. Construction des corps finis
 - 2. Irréductibilité sur les corps finis

Plan détaillé

Tous les anneaux considérés seront implicitement commutatifs et unitaires.

I - Irréductibilité

1 - Polynômes irréductibles [Berhuy]

1. Définition : soit A un anneau (commutatif unitaire). Un polynôme $P \in A[X]$ est dit irréductible si pour tous polynômes $f, g \in A[X]$ tels que $P = fg$, f ou g est inversible dans $A[X]$.
2. Remarque : si A est intègre, les inversibles de $A[X]$ sont exactement les éléments de $A^\times$. En particulier, si A est un corps, $(A[X])^\times = A \setminus \{0\}$.
3. Exemples :
 1. Si A est intègre, $X - a$ est irréductible quelque soit a . Lorsque A est un corps algébriquement clos, tous les polynômes irréductibles sont de cette forme.
 2. $X^2 + 1$ est irréductible dans $\mathbb{Q}[X]$, $\mathbb{R}[X]$ mais pas dans $\mathbb{C}[X]$.
 3. $2X$ est irréductible dans $\mathbb{Q}[X]$ mais pas dans $\mathbb{Z}[X]$.
4. Proposition : soit A un anneau intègre et P un polynôme irréductible. P n'a pas de racine dans A . Si de plus P est de degré au plus 3 et non constant, la réciproque est vraie.
5. Contre-exemple : $(X^2 + 1)^2$ est réductible sur $\mathbb{R}[X]$ bien que sans racine réelle.
6. Théorème (Eisenstein) : soit A un anneau intègre et $p \in A$ un élément premier de A . Soit $P \in A[X]$. On suppose que p ne divise pas le coefficient dominant de P mais divise tous les autres coefficients de P . On suppose de plus que p^2 ne divise pas le coefficient constant de P . Alors P est irréductible dans $\text{Frac}(A)[X]$.

7. Exemple : On considère p un nombre premier et $\Phi_p := \sum_{k=0}^{p-1} X^k$. Le polynôme $\Phi_p(X+1)$ satisfait le critère d'Eisenstein et Φ_p est irréductible dans $\mathbb{Q}[X]$.

2 - Contenu d'un polynôme [Perrin]

On fixe dans cette partie A un anneau factoriel.

1. Définition (contenu) : Soit A un anneau factoriel. On appelle contenu d'un polynôme $P \in A[X]$ tout pgcd des coefficients de P dans A . On le note $c(P)$. Lorsque $c(P)$ est inversible dans A , on dit que P est primitif.
2. Exemples :
 1. Tout polynôme unitaire est primitif.
 2. 2 et -2 sont des contenus de $2X + 4$.
3. Lemme (Gauss) : le contenu est multiplicatif, c'est-à-dire que $c(PQ) = c(P)c(Q)$. En particulier, un polynôme est primitif si, et seulement si, tous ses diviseurs sont primitifs.
4. Théorème : notons K le corps des fractions de A . Soit $P \in A[X]$. P est irréductible sur A si, et seulement si, il est irréductible sur K et primitif.
5. Exemple : les polynômes Φ_p sont tous irréductibles dans $\mathbb{Q}[X]$.

3 - Cyclotomie : prélude [Escofier]

On fixe K un corps de caractéristique $\text{Car}(K)$.

1. Définition (racine primitive de l'unité) : pour $n \in \mathbb{N}^*$, on appelle racine primitive n -ième tout élément d'ordre n dans $K^\times$. On note $\mu_n^*(K)$ leur ensemble.
2. Définition (polynôme cyclotomique) : on appelle n -ième polynôme cyclotomique à coefficients dans K le polynôme

$$\Phi_{n,K} := \prod_{\omega \in \mu_n^*(K)} (X - \omega)$$

3. Exemples :
 1. $\Phi_{1,K} = X - 1$ quelque soit le corps K .
 2. $\Phi_{p,\mathbb{C}}$ est le polynôme Φ_p précédemment défini lorsque p est un nombre premier.
4. Lemme : Supposons $\neg(\text{Car}(K) \mid n)$. On a la relation de récurrence forte dans $K[X]$:

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

5. Corollaire : si $\text{Car}(K) = 0$, $\Phi_{n,K} \in \mathbb{Z}[X]$. Si $\text{Car}(K) = p$, $\Phi_{n,K} \in \mathbb{F}_p[X]$.
6. Théorème : les polynômes cyclotomiques à coefficients dans $\mathbb{C}$ sont irréductible sur $\mathbb{Q}$ et $\mathbb{Z}$.

II - Extensions algébriques [Escofier]

1 - Algébricité

On fixe une extension de corps L/K

1. Définition (élément algébrique) : un élément $x \in L$ est dit algébrique sur K s'il est annulé par un polynôme non nul à coefficients dans K . Dans le cas contraire, il est dit transcendant.
2. Définition (polynôme minimal) : on appelle polynôme minimal d'un élément algébrique x l'unique générateur unitaire de l'idéal $\{P \in K[X] \mid P(x) = 0\}$.
3. Exemples :
 1. le nombre complexe $e^{\frac{2i\pi}{n}}$ est algébrique sur $\mathbb{Q}$. Son polynôme minimal est $\Phi_{n,\mathbb{C}}$.
 2. Dans l'extension $\mathbb{C}(X)/\mathbb{C}$, l'indéterminée X est transcendante sur $\mathbb{C}$.
4. Proposition : soit $P \in K[X]$ unitaire et $x \in L$. Alors P est le polynôme minimal de x si, et seulement si, $P(x) = 0$ et P est irréductible dans $K[X]$.
5. Théorème : Soit $x \in L$. x est algébrique sur K si, et seulement si, $K[x] = K(x)$. Dans ce cas, $K(x)$ est un corps isomorphe à $K[X]/\langle \pi_x \rangle$, et sa dimension en tant que K -espace vectoriel est $\deg(\pi_x)$. Une base en est donnée par $(1, x, \dots, x^{\deg(\pi_x)-1})$.
6. Théorème (base télescopique)
7. Exemple : Le corps $\mathbb{Q}(i, \sqrt{2})$ est de dimension 4 sur $\mathbb{Q}$. De plus, $\sqrt{2} + i$ est de degré 4 sur $\mathbb{Q}$, donc $\mathbb{Q}(i, \sqrt{2}) = \mathbb{Q}(\sqrt{2} + i)$.
8. Application : L'ensemble $\bar{\mathbb{Q}}$ des nombres complexes algébriques (sur $\mathbb{Q}$) est une clôture algébrique de $\mathbb{Q}$.

2 - Corps de rupture, corps de décomposition.

1. Définition (corps de rupture) : soit $P \in K[X]$ un polynôme irréductible. Une extension de rupture de P est une extension de corps L/K telle qu'il existe $\alpha \in L$

tel que $L = K[\alpha]$ et $P(\alpha) = 0$.

2. Exemples :

1. notons $\mathbb{U}_n$ les racines n -ièmes de l'unité de $\mathbb{C}$. L'extension $\mathbb{Q}(\mathbb{U}_n)/\mathbb{Q}$ est une extension de rupture de $\Phi_{n,\mathbb{C}}$ (ce qui ne l'empêche pas de contenir plusieurs racines de Φ_n)
2. Les extensions $\mathbb{Q}(j\sqrt[3]{2})$ et $\mathbb{Q}(\sqrt[3]{2})$ sont deux extensions de rupture de $X^3 - 2$.
3. Théorème : soit P un polynôme irréductible. L'extension $M := K[X]/\langle P \rangle$ est une extension de rupture de P engendrée par la classe x de X dans le quotient. De plus, pour toute extension de rupture L/K de P et toute racine α de P dans L , il existe un unique isomorphisme d'extension de M dans L qui envoie x sur α .
4. Application : $\mathbb{C}$ peut être défini comme le corps $\mathbb{R}[X]/\langle X^2 + 1 \rangle$. L'unité imaginaire i est alors définie comme la classe de X dans le quotient.
5. Définition (corps de décomposition) : soit P un polynôme non nul. On appelle extension de décomposition de P toute extension L/K telle que P est scindé dans L et L est engendrée par les racines de P dans L .
6. Exemple : l'extension $\mathbb{Q}(\sqrt[3]{2}, j)$ est une extension de décomposition de $X^3 - 2$ sur $\mathbb{Q}$, mais pas une extension de rupture.
7. Théorème : pour tout polynôme P non nul, il existe une unique extension de décomposition de P à isomorphisme d'extension près. Le degré d'une telle extension est majoré par $\deg(P)!$.
8. Application : soit M une matrice carrée à coefficients dans K . Il existe une extension finie L/K telle que M vue comme matrice à coefficients dans L est trigonalisable et admet une décomposition de Dunford.

III - Corps finis

1 - Construction des corps finis [Rombaldi, Perrin]

1. Théorème : soit p un nombre premier et $n \geq 1$. Il existe $\mathbb{F}_q$ une corps à $q := p^n$ éléments unique à isomorphisme de $\mathbb{F}_p$ -extension près. L'extension $\mathbb{F}_q/\mathbb{F}_p$ est une extension de décomposition de $X^q - X$.
2. Remarque : Le groupe $\mathbb{F}_q^\times$ est un sous-groupe fini de groupe multiplicatif d'un corps : il est cyclique. Tout générateur de ce groupe engendre l'extension $\mathbb{F}_q/\mathbb{F}_p$, et cette extension est donc monogène.

3. Lemme : Notons $\mathcal{I}_d$ l'ensemble des irréductibles unitaires de degré d de $\mathbb{F}_p[X]$.

On a :

$$X^q - X = \prod_{d|n} \prod_{P \in \mathcal{I}_d} P$$

4. Corollaire : soit $n, d \in \mathbb{N}^*$. Il existe une injection d'extensions $\mathbb{F}_{p^d}/\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^n}/\mathbb{F}_p$ si, et seulement si, $d \mid n$.

5. Exemple : $\mathbb{F}_4$ est isomorphe au corps $\mathbb{F}_2/\langle X^2 + X + 1 \rangle$. En particulier, $\mathbb{F}_4$ n'est pas isomorphe à $\mathbb{Z}/4\mathbb{Z}$.

2 - Polynômes irréductibles sur les corps finis [Escofier, Objectif agreg]

1. Proposition : soit $P \in \mathbb{F}_p[X]$ unitaire et de degré n . P est irréductible si, et seulement si, $P \mid X^n - X$ et pour tout $d \mid n$, $P \nmid X^d - X$.

2. Théorème (Berlekamp, DVT 1)

3. Remarque : lorsque P est à facteurs multiples, on peut commencer par calculer $R := \text{pgcd}(P', P)$. Si c'est 0, P admet une racine p -ième sur laquelle on peut appliquer récursivement l'algorithme. Sinon, on applique récursivement l'algorithme à R et P/R .

4. Théorème (cyclotomie sur $\mathbb{F}_q$) : soit $n \in \mathbb{N}$ tel que $p \wedge n = 1$ et L une extension de décomposition de $X^n - X$. Les facteurs irréductibles de $\Phi_{n,L}$ dans $\mathbb{F}_q[X]$ ont tous pour degré l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$. (DVT 2)

5. Application : le polynôme $\Phi_{8,\mathbb{C}} \in \mathbb{Z}[X]$ est irréductible sur $\mathbb{Q}$ et $\mathbb{Z}$ mais réductible sur tout corps fini. (DVT 2)