

Rapport du jury

Les extensions de degré fini, le théorème de la base télescopique et ses applications à l'irréductibilité de certains polynômes, ainsi que les corps finis, sont incontournables. Il est souhaitable d'introduire la notion d'élément algébrique et d'extension algébrique en en donnant des exemples. Il faut savoir calculer le polynôme minimal d'un élément algébrique dans des cas simples, notamment pour quelques racines de l'unité. La leçon peut être illustrée par des exemples d'extensions quadratiques et leurs applications en arithmétique, ainsi que par des extensions cyclotomiques. Pour aller plus loin, les candidates et candidats peuvent montrer que l'ensemble des nombres algébriques forme un corps algébriquement clos, par exemple en expliquant comment l'utilisation du résultant permet de calculer des polynômes annulateurs de sommes et de produits de nombres algébriques. Il est possible de 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](#)
- [Théorie de Galois - Escofier](#)
- [Corps commutatifs et théorie de Galois - Tauvel](#)

Développements

- [Cyclotomie](#) (sur F_q)
- [Norme d'une extension](#) (entiers algébriques)

Méta-plan

1. Extensions de corps
 1. Définitions et premières propriétés
 2. Elements algébriques
2. Extensions particulières
 1. Extensions de rupture et de décomposition
 2. Extensions cyclotomiques

3. Clôture algébrique
3. Outils d'étude des extensions
 1. K -morphisms et racines
 2. Théorème de l'élément primitif
 3. Norme

Plan détaillé

I - Extensions de corps [Berhuy]

1 - Définitions et premières propriétés

1. Définition : extension de corps (vue comme morphisme), morphisme d'extension.
2. Remarque : un morphisme de corps est nécessairement injectif. Si L/K est une extension, K s'identifie donc à un sous-corps de L .
3. Exemples :
 1. $\mathbb{C}$ est une extension de $\mathbb{R}$ et de $\mathbb{Q}$ par l'injection canonique.
 2. Soit p un nombre premier. $\mathbb{F}_p(X) \ni F \mapsto F^p \in \mathbb{F}_p(X)$ permet de voir $\mathbb{F}_p$ comme une extension non-triviale de $\mathbb{F}_p$. D'où l'importance de spécifier les morphismes !
4. Exemple de morphismes : $\mathbb{F}_p(X)$ et $\mathbb{F}_p(X^p)$ sont isomorphes en tant que corps mais pas en tant qu'extensions de $\mathbb{F}_p(X)$.
5. Définition (degré) : soit L/K une extension. L est naturellement muni d'une structure de K -algèbre. C'est en particulier un K -espace vectoriel dont on note $[L : K] \in \mathbb{N}^* \cup \{\infty\}$ la dimension. Si $[L : K] < +\infty$, on dit que l'extension est *finie*.
6. Exemple : $\mathbb{C}/\mathbb{R}$ est une extension de degré 2. $\mathbb{C}/\mathbb{Q}$ est une extension de degré infini.
7. Théorème : base télescopique.
8. Application : il n'existe aucun corps strictement compris entre $\mathbb{R}$ et $\mathbb{C}$.
9. Définition : extension engendrée par une partie

2 - Éléments algébriques

1. Définition : élément algébrique, élément transcendant. Extension algébrique.
2. Définition : polynôme minimal.

3. Théorème : on a une équivalence entre α algébrique sur K et $K[\alpha] = K(\alpha)$ et $K(\alpha)/K$ est une extension finie.
4. Corollaire : toute extension finie est algébrique.
5. Contre-exemple : L'ensemble des complexes algébriques sur $\mathbb{Q}$ est une extension algébrique infinie de $\mathbb{Q}$.
6. Théorème : l'ensemble des éléments de L algébriques sur K est un corps qui contient K .
7. Exemples : $\sqrt{3}$ et $\frac{1+\sqrt{19}}{2}$ sont algébriques sur $\mathbb{Q}$. Le nombre de Liouville est transcendant. π est transcendant sur $\mathbb{Q}$ (admis)

II - Extensions particulières

1 - Extension de rupture, de décomposition [Berhuy]

1. Définition : extension de rupture.
2. Définition : extension de décomposition
3. Exemple : $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ est une extension de rupture de $X^3 - 2$ mais pas de décomposition. $\mathbb{Q}(\sqrt[3]{2}, j)/\mathbb{Q}$ est une extension de décomposition de ce polynôme, mais pas de rupture.
4. Théorème : existence et unicité de l'extension de décomposition / de rupture
5. Application : pour tout q une puissance d'un nombre premier, il existe un corps $\mathbb{F}_q$ de cardinal q . L'extension $\mathbb{F}_q/\mathbb{F}_p$ est unique à isomorphisme d'extension près.

2 - Extensions cyclotomiques [Escofier]

1. Définition : racine primitive de l'unité. Polynôme cyclotomique (sur un corps quelconque).
2. Exemple : Φ_p avec p premier
3. Lemme : relation de récurrence sur les polynômes cyclotomiques
4. Corollaire : $\Phi_{n,\mathbb{Q}} \in \mathbb{Z}[X]$. De plus, si n et p premier avec p , $\Phi_{n,\mathbb{F}_p} = \overline{\Phi_{n,\mathbb{Q}}}$.
5. Théorème : les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}[X]$. Il suit que $[\mathbb{Q}(\mu_n^*) : \mathbb{Q}] = \phi(n)$.

3 - Clôture algébrique [Berhuy / Tauvel]

1. Définition : corps algébriquement clos. Clôture algébrique

2. Remarque : $\mathbb{C}$ est algébriquement clos, mais n'est pas une clôture algébrique de $\mathbb{Q}$ car pas algébrique !
3. Théorème : Soit L/K une extension avec L algébriquement clos. L'ensemble $\bar{K}$ des éléments de L algébriques sur K est une clôture algébrique de K .
4. Application : $\bar{\mathbb{Q}}$ est une clôture algébrique de $\mathbb{Q}$.
5. Théorème : Soit L/K une extension finie et Ω/K une extension telle que Ω est un corps algébriquement clos. Alors il existe un morphisme d'extension $L/K \rightarrow \Omega/K$, c'est-à-dire que L s'identifie à un sous-corps de Ω .

III - Outils d'étude des extensions

1 - Morphismes et racines [Escofier]

Soit L/K une extension. Pour $P \in K[X]$, on note $\mathcal{Z}(P, L)$ l'ensemble des racines de P dans L .

1. Soit σ un automorphisme d'extension. σ induit une permutation de $\mathcal{Z}(P, L)$.
2. Théorème : Si $L = K(\alpha)$ et $P = \pi_\alpha$, alors $Aut \rightarrow \mathfrak{S}(\mathcal{Z})$ est injectif. En particulier, $|Aut| \leq \deg(P)$.
3. Exemple : Il n'existe que deux automorphismes de l'extension $\mathbb{C}/\mathbb{R}$
4. Application (DVT 1) : soit q une puissance non triviale d'un nombre premier p et $L/\mathbb{F}_q$ une extension finie. L'automorphisme de l'extension $x \mapsto x^q$ est d'ordre $[L : \mathbb{F}_q]$ et engendre le groupe $Aut_{\mathbb{F}_q}(L)$ (qui est donc cyclique).
5. Théorème (DVT 1): soit n un entier premier avec q et Φ_n le polynôme cyclotomique à coefficients dans $\mathbb{F}_q$. Ses facteurs irréductibles ont tous pour degré l'ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$.
6. Application (DVT 1) : $\Phi_8 \in \mathbb{Z}[X]$ est irréductible mais son projeté dans tout corps fini est réductible.

2 - Norme d'un extension [Tauvel + de mémoire]

1. Définition : soit L/K une extension finie. On appelle norme de $\alpha \in L$ le déterminant de l'application K -linéaire $m_\alpha : x \mapsto \alpha x$.
2. Exemples :
 1. $N(\alpha) = 0 \iff \alpha = 0$
 2. si $\alpha \in K$, $N(\alpha) = \alpha^{[L:K]}$.

3. Si p est un nombre premier et $q = p^n$, la norme de $\alpha \in \mathbb{F}_q$ dans l'extension F_q/F_p est $\alpha^{\frac{q-1}{p-1}}$.

3. Proposition (propriétés de la norme, DVT 2) :

1. La norme est multiplicative
2. Si π_α est le polynôme minimal de α , d son degré et n le degré de l'extension, $N(\alpha) = (-1)^n [\pi_\alpha(0)]^{n/d}$.
3. Si M/L est une extension telle que π_α est scindé dans L , alors $N(\alpha)$ est le produit des racines de π_α dans M à la puissance n/d .

4. Définition (corps de nombres, anneaux d'entiers) : on appelle corps de nombres toute extension $K/\mathbb{Q}$ finie. On appelle entier de K tout élément $z \in K$ annulé par un polynôme unitaire à coefficients dans $\mathbb{Z}$. On note $\mathfrak{O}_K$ l'ensemble des entiers de K .

5. Exemples :

1. $\mathfrak{O}_{\mathbb{Q}} = \mathbb{Z}$
2. $\mathfrak{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$

6. Lemme : $\forall z \in K, z \in \mathfrak{O}_K \iff \pi_z \in \mathbb{Z}[X]$.

7. Théorème : $\mathfrak{O}_K$ est un sous-anneau de K .

8. Application : soit $z \in \mathfrak{O}_K$. Alors $z \in \mathfrak{O}_K^\times \iff N(z) = \pm 1$. (DVT 2)