

Sujet choisi: 125 - Extensions de corps. Exemples d'applications

Autre sujet: 108

Soit K un corps.I. Extensions de corps1) Définition et premières propriétésDef 1: Une extension de K est un couple (L, φ) où L est un corps et $\varphi: K \hookrightarrow L$ un morphisme d'anneaux. On la note L/K .Rem 2: Un morphisme d'anneaux entre deux corps est toujours injectif donc on peut supposer qu'on a l'inclusion $K \subset L$.Ex 3: $\mathbb{C}$ est une extension de $\mathbb{R}$, elle-même extension de $\mathbb{Q}$.Def 4: On définit le morphisme caractéristique de K comme l'unique morphisme d'anneau $\varphi: \mathbb{Z} \rightarrow K$.Prop 5: Si φ n'est pas injective, alors $\exists n \in \mathbb{N}$, ker $\varphi = n\mathbb{Z}$.Def 6: On définit la caractéristique de K par: $\text{carac}(K) = 0$ si φ est injective et n si ker $\varphi = n\mathbb{Z}$.Ex 7: $\text{carac}(\mathbb{Q}) = 0$, $\text{carac}(\mathbb{Z}/p\mathbb{Z}) = p$ pour p premier.Prop 8: Si $\text{carac}(K) = n \in \mathbb{N}$, alors n est premier.Def 9: On définit le sous-corps premier de K comme le plus petit sous-corps de K .Prop 10: le sous-corps premier est entièrement déterminé par la caractéristique. Il vaut $\mathbb{Q}$ si $\text{carac}(K) = 0$ et $\mathbb{Z}/p\mathbb{Z}$ si $\text{carac}(K) = p$.Ex 11: $\mathbb{Z}/p\mathbb{Z}$ est le sous-corps premier de $\mathbb{Z}/p\mathbb{Z}(X)$.Def 12: On appelle degré d'une extension L/K la dimension de L vu comme K -ev et on le note $[L:K]$.Ex 13: $[\mathbb{C}:\mathbb{R}] = 2$, $[\mathbb{R}:\mathbb{Q}] = +\infty$.Prop 14: $[L:K] = 1 \Leftrightarrow L = K$.Thm 15: (Base télescopique)Soit $M/L/K$ une tour d'extensions.Si $(j_i)_{i \in I}$ est une L -base de M et $(e_j)_{j \in J}$ est une K -base de L , alors $(j_i e_j)_{(i,j) \in I \times J}$ est une K -base de M .Cor 16: (multiplicativité du degré)Soit $M/L/K$ une tour d'extensions. $[M:K] < +\infty \Leftrightarrow ([M:L] < +\infty \text{ et } [L:K] < +\infty)$
et dans ce cas, $[M:K] = [M:L][L:K]$.Ex 17: Soit $K_n/K_{n-1}/\dots/K_1$ une tour d'extensions.Si $[K_n:K_1]$ est fini alors $\exists i \in \{1, \dots, n-1\}$, $[K_i:K_1]$ est fini.2) Extensions finies, extensions algébriquesDef 18: Un élément $\alpha \in L$ est dit L/K est une extension et dit:

- Transcendant si le morphisme $\text{ev}_\alpha: K[X] \rightarrow K[\alpha]$
 $P(X) \mapsto P(\alpha)$ est injectif.
- Algébrique sinon.

Prop 19: Si $\alpha \in L$ est algébrique il existe un unique polynôme unitaire générateur de l'idéal ker (ev_α) .Def 20: On note ce polynôme $p_{\alpha, K}$, et l'appelle polynôme minimal de α sur K .Prop 21: Un polynôme minimal est irréductible (sur $K[X]$).Ex 22: $\deg(p_{\alpha, K}) = 1 \Leftrightarrow \alpha \in K$ et dans $p_{\alpha, K} = X - \alpha$.Thm 23: Soit $\alpha \in L$. LASSE:

- α est algébrique
- $K[\alpha] = K(\alpha)$ (plus petit corps contenant K et α)
- $[K(\alpha):K] < +\infty$

Dans ce cas, on a alors $\deg(p_{\alpha, K}) = [K(\alpha):K]$.Ex 24:

- i est algébrique sur $\mathbb{R}$ et $p_i: \mathbb{R} = X^2 + 1$
- $\sqrt{2}$ est algébrique sur $\mathbb{Q}$ et $p_{\sqrt{2}, \mathbb{Q}} = X^2 - 2$
- e est transcendant sur $\mathbb{Q}$ (Thm de Lindemann, voir)

Def 25: Une extension L/K est dite :

- Algébrique si tout élément de L est algébrique sur K .
- Finie si $[L:K] < +\infty$.

Rem 26: Par le thm 23, ces notions sont équivalentes pour les extensions monogènes (càd tq $\exists \alpha \in L, L = K(\alpha)$).

Prop 27: Toute extension finie est algébrique.

Ex 28: Un racine carrée est finie en général. En effet, $\mathbb{Q}(\{\sqrt{2}\}_{n \in \mathbb{N}})$ est une extension de $\mathbb{Q}$ algébrique mais pas finie.

Ex 29: $\mathbb{C}/\mathbb{R}$ et $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ sont algébriques.

Prop 30: Si L/K est finie, alors $\forall \alpha \in L, \deg(\alpha, K) \mid [L:K]$.

3) Automorphismes de corps

Def 31: Soit L/K une extension. On note $\text{Aut}_K(L)$ l'ensemble des $\varphi: L \rightarrow L$ morphismes de corps laissant K fixe, tels que $\varphi|_K = \text{id}_K$.

Ex 32: $\text{Aut}_{\mathbb{Q}}(\mathbb{R}) = \{\text{id}_{\mathbb{R}}\}$, $\text{Aut}_{\mathbb{R}}(\mathbb{C}) = \{\text{id}_{\mathbb{C}}, \bar{\cdot}\}$.

Prop 33: $\text{Aut}_K(L)$ est un groupe pour la composition $\circ$.

Prop 34: Soient $\varphi \in \text{Aut}_K(L)$ et $P \in K[X]$. φ permute les racines de P car si $\forall z \in \text{Rac}(P), \varphi(z) \in \text{Rac}(P)$.

Thm 35: Si L/K est finie, alors $|\text{Aut}_K(L)| \leq [L:K]$.

II. Extensions particulières

1) Corps de rupture, corps de décomposition

Def 36: Soit $P \in K[X]$ irréductible. L/K est un corps de rupture de P si il est de la forme $L = K(\alpha)$ avec $\alpha \in L$ tel que $P(\alpha) = 0$.

Thm 37: Soit $P \in K[X]$ irréductible.

- Il existe un corps de rupture de P .
- Si $L = K(\alpha)$ et $L' = K(\beta)$ sont deux corps de rupture de P , alors il existe un unique morphisme $\varphi: L \rightarrow L'$ tq $\varphi(\alpha) = \beta$ et $\varphi|_K = \text{id}_K$.

Rem 38: Soit $P \in K[X]$ irréductible et L/K un corps de rupture de P . Alors $[L:K] = \deg(P)$, $L \cong K[X]/(P)$ et si $\alpha \in L$ est une racine de P , alors $\{1, \alpha, \dots, \alpha^{n-1}\}$ est une K -base de L .

App 39: On peut construire $\mathbb{C}$ comme le corps de rupture de X^2+1 sur $\mathbb{R}$.

App 40: Soit $P \in K[X]$ de degré $n \in \mathbb{N}$. Alors P est irréductible dans $K[X]$ si P n'a aucune racine dans les extensions L/K telles que $[L:K] \leq \frac{n}{2}$.

Def 41: Soit $P \in K[X]$. L/K est un corps de décomposition de P si il est de la forme $L = K(\alpha_1, \dots, \alpha_n)$ où $n = \deg(P)$ et les $\alpha_i \in L$ sont racines de P .

Prop 42: Un corps de décomposition est une extension finie.

Thm 43: Soit $P \in K[X]$ de degré $n \geq 1$.

- Il existe un corps de décomposition $D_K(P)$ tq $[D_K(P):K] \leq n!$.
- Deux corps de décomposition de P sont K -isomorphes.

Ex 44: $\mathbb{Q}(\sqrt[3]{2})$ est un corps de rupture de $X^3 - 2$ qui n'est pas un corps de décomposition. $\mathbb{Q}(j, \sqrt[3]{2})$ est un corps de décomposition.

App 45: (Springer)

Soit L/K une extension de degré impair. Soit q une forme quadratique sur K^n et $q|_L$ la forme quadratique sur L^n définie par extension des scalaires de q . Alors

$$\exists v \in L^n - \{0_{L^n}\}, q|_L(v) = 0 \Rightarrow \exists w \in K^n - \{0_{K^n}\}, q(w) \neq 0.$$

Ex 46: L'hypothèse d'impairité du degré est importante. En effet, $q(x, y) = x^2 + y^2$ est unilatère sur $\mathbb{R}$ mais pas sur $\mathbb{C}$.

2) Corps finis

Prop 47: Un corps fini est de caractéristique non-nulle.

Def 48: Soit $\text{car}(K) = p$ on définit par $F: K \rightarrow K, x \mapsto x^p$ le Frobenius.

Prop 49: Le Frobenius est un morphisme de corps injectif.

DEVI

Rem 50: Dans le cas d'un corps fini de Frobenius est bijectif.

Prop 51: Si K est un corps fini de cardinal q . Alors $\exists n \in \mathbb{N}$ tel que $q = p^n$ où $p = \text{carac}(K)$.

Lemme 52: Si $|K| = q$ alors $\forall x \in K, x^q = x$.

Lemme 53: $\{x \in \mathbb{D}_{\mathbb{Z}/p\mathbb{Z}}(X^q - X) \mid x^q = x\}$ est un corps de cardinal q .

Thm 54: Soit $q = p^n$ avec p premier et $n \in \mathbb{N}$. Il existe un corps de cardinal q unique à isomorphisme de corps près.

Rem 55: $\mathbb{F}_q = \mathbb{D}_{\mathbb{F}_p}(X^q - X)$.

Rem 56: $\forall p$ premier, $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$.

Rem 57: on peut construire explicitement un corps de cardinal p^n comme corps de rupture d'un polynôme irréductible sur $\mathbb{F}_p$ de cardinal n .

Ex 58: $\mathbb{F}_p \cong \mathbb{F}_2[x]/(x^2 + x + 1) \cong \mathbb{F}_2[\alpha]$ où $\alpha^2 + \alpha + 1 = 0$.

Thm 59: Soit $I_n(p)$ le cardinal de $U_n(p)$ ensemble des polynômes unitaires irréductibles de degré n de $\mathbb{F}_p[x]$.
Alors $X^{p^n} - X = \prod_{d \mid n} \prod_{p \in U_d(p)} P$.

Cor 60: $I_n(p) = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) p^d$.

Rem 61: En particulier $I_n(p) \geq 1$ pour la construction décrite dans la remarque 57 est toujours réalisable (à condition de trouver le polynôme irréductible du bon degré).

3) Corps cyclotomiques

Def 62: Une extension cyclotomique de $\mathbb{Q}$ est une extension de la forme $\mathbb{Q}(\zeta)/\mathbb{Q}$ où $\zeta \in U_n$ est une racine de l'unité.

Def 63: Soit $U_n^\times = \{\zeta \in U_n \mid \langle \zeta \rangle = U_n\}$ l'ensemble des racines n -ièmes primitives de l'unité. Alors on définit le n -ième polynôme cyclotomique par: $\Phi_n = \prod_{\zeta \in U_n^\times} (X - \zeta)$. Par exemple pour p premier, $\Phi_p = X^{p-1} + \dots + X + 1$.

Prop 64: $\forall n \geq 1, X^n - 1 = \prod_{d \mid n} \Phi_d$.

Cor 65: $\forall n \geq 1, \Phi_n \in \mathbb{Z}[X]$.

Thm 66: $\forall n \geq 1, \Phi_n$ est irréductible dans $\mathbb{Z}[X]$ et $\mathbb{Q}[X]$.

App 67: (progression arithmétique de Dirichlet, version faible)
 $\forall n \geq 1$, il existe une infinité de premiers congrus à 1 modulo n .

Cor 68: $\Phi_n = \prod_{\zeta \in U_n^\times} (X - \zeta)$ où $\zeta \in U_n^\times$.

Thm 69: $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_p)) \cong (\mathbb{Z}/(p-1)\mathbb{Z}, +)$ pour p premier.
C'est-à-dire, $\text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta_p))$ est cyclique d'ordre $p-1$.

III. Constructions à la règle et au compas

Def 70: On dit qu'un point $Z \in \mathbb{C}$ est constructible en une étape à partir d'une partie $P \subset \mathbb{C}$ si Z est l'intersection de deux droites, deux cercles ou d'une droite et d'un cercle dont les données (centres, points par lesquels la droite passe) sont dans P .

Def 71: On définit $\mathbb{E}$ comme l'ensemble des points constructibles en un nombre fini d'étapes à partir de $\{0, 1\}$. Un élément de $\mathbb{E}$ est dit constructible.

Prop 72: $\mathbb{E}$ est un corps stable par racines carrées contenant $\mathbb{Q}$.

Thm 73: (Wantzel) Soit $\alpha \in \mathbb{E}$.

$\alpha \in \mathbb{E} \Leftrightarrow \exists K_0, \dots, K_n / K_0 = \mathbb{Q}$ tour d'extensions telle que $\forall i \in [0, n-1], [K_{i+1} : K_i] = 2$ et $\alpha \in K_n$.

Cor 74: Si $\alpha \in \mathbb{C}$ est constructible alors $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ est une puissance de 2.

Ex 75: la racine cube est impossible. Au moins une des deux racines réelles de $X^3 - 2 = 0$ n'est pas constructible.

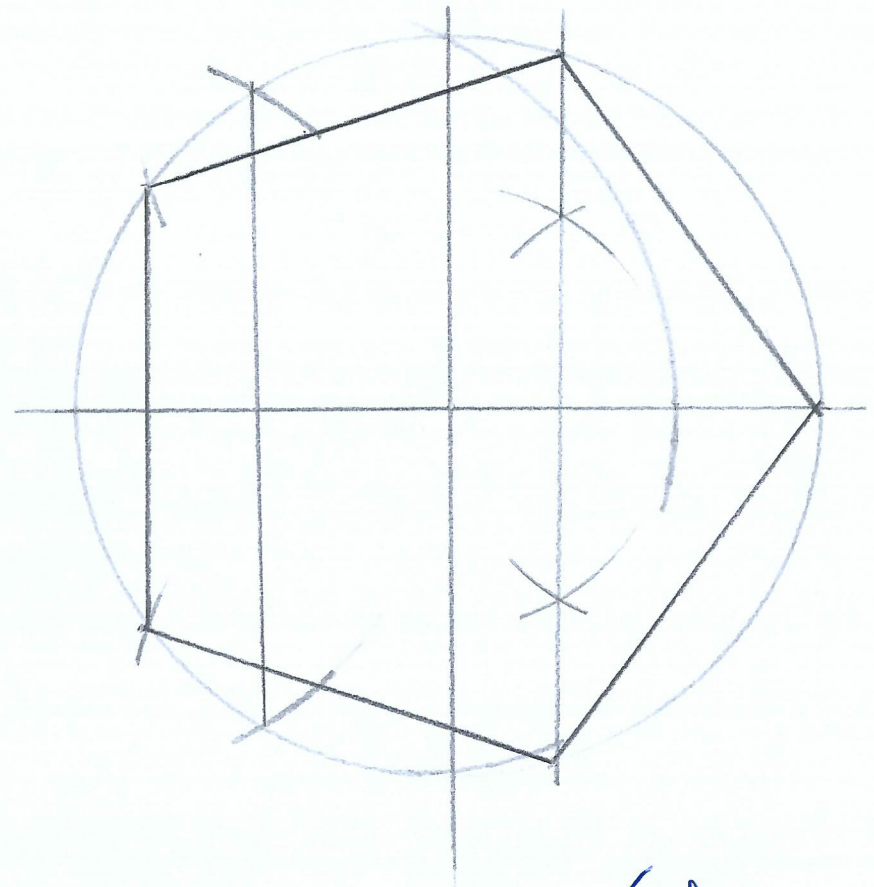
App 76: la duplication du cube est impossible puisque $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$.

App 77: la quadrature du cercle est impossible puisque π est transcendant.

App 78: Soient $m \in \mathbb{N}$ tel que $m = p^d$ avec p premier. Alors $\zeta_m = e^{\frac{2\pi i}{m}} \in \mathbb{E} \Leftrightarrow d = 1$ et $p = 1 + 2^m$ avec $m \in \mathbb{N}$.

Cor 79: (Gauss-Wantzel) Soit $n \in \mathbb{N}$. Le n -gon régulier est constructible si $n = 2^\alpha p_1 \dots p_r$ avec $\alpha \in \mathbb{N}$ et les p_i premiers tels que $p_i = 1 + 2^{m_i}$.

DEV 2



Construction du pentagone régulier

125 - Extensions de corps. Exemples et applications.

1 Commentaires généraux

Comme tout ce qui se trouve sur Agreg-Maths, ne prenez rien pour argent comptant. Des erreurs sèment sans doute le document. Aucun choix pris pour écrire un plan n'est intrinsèquement bon ou mauvais. Le plus important est d'être convaincu et convaincant quant à la pertinence de chacune de vos décisions.

Le plan a été écrit en conditions d'examen, en trois heures, puis présenté devant un jury. C'est une leçon sur laquelle j'étais à l'aise donc je me suis permis un plan très long.

Les items 4 à 11 servent à proprement introduire la notion de caractéristique d'un corps. Ils servent à proprement introduire la construction des corps finis dans ma partie II.2. Cependant, je pense que ce n'est pas la peine de détailler autant cette notion dans cette leçon. (Ca serait par contre tout à fait pertinent dans la leçon sur les corps finis justement.) Donc si j'avais voulu raccourcir le plan, j'aurais condensé ces items en un ou deux.

J'ai oublié d'ajouter un item pour énoncer que l'ensemble des nombres algébriques d'une extension a une structure de corps. C'est un point important.

2 Défense de plan

J'ai proposé une accroche sur les constructions à la règle et au compas. Je donne l'exemple de la quadrature du cercle et de la construction des polygones réguliers. Ce sont des problèmes importants de l'histoire des mathématiques car faciles à énoncer mais dont la résolution n'a été fournie que bien plus tard grâce à aux outils abstraits issus de la théorie des corps. (Evidemment cette accroche n'est pertinente que si vous abordez les constructions à la règle et au compas dans votre plan. Cette leçon fait partie de ces sujets d'algèbre abstraits dont la motivation n'est pas évidente. Une introduction théorique du style « En théorie des anneaux on aime bien manipuler des éléments inversibles... » me paraît vraiment scabreuse...)

Ensuite j'ai suivi mon plan de façon assez linéaire en mentionnant mon premier développement.

Finalement, je reboucle sur les constructions à la règle et au compas en apportant une réponse au problème initiale via mon deuxième développement. Pour insister sur le fait que je boucle la boucle, j'ai commencé mon accroche en écrivant tout à droite du tableau de sorte que je retombe dessus en poursuivant de gauche à droite.

3 Développements

Mon premier développement est le théorème de Springer. J'aime bien ce développement et il est d'un bon niveau. D'ailleurs faites très attention aux versions de ce développement qu'on trouve sur Agreg-Maths. Beaucoup de versions font de grosses omissions qui nécessitent plusieurs lignes de détails. (Par exemple, soyez au clair sur où est utilisée l'hypothèse d'impairité. C'est plus subtile que ça en a l'air.) Et le pire c'est que le développement n'est

pas très pertinent. En effet, je n'ai jamais trouvé d'application concrète. Je n'ai aucun exemple de forme quadratique qui admettrait un vecteur isotrope sur une extension de degré impair explicite sans en admettre un explicite sur le corps de base. En fait les extensions de degré impair c'est pas très naturel. Donc à part en le présentant comme une curiosité ou une illustration de notions abstraites (ce qui est déjà pas mal), il est dur à défendre. Je ne le conseillerais qu'aux fans inconditionnés des formes quadratiques dont vous devriez faire partie.

Mon deuxième développement est le théorème de Gauss-Wantzel. Il se motive parfaitement via la construction de la défense. Il est également d'un bon niveau et nécessite de faire des choix sur quels points on détaille et quels points on omet. Personnellement je justifiais le calcul du groupe de Galois à l'oral. (Ca n'a jamais vraiment plu aux différents jury auxquels j'ai pu montrer ça. Donc faut être béton sur la justification.) Evidemment il faut savoir faire la construction du pentagone. Elle est à apprendre par coeur et fait toujours joli en annexe.

4 Détails de quelques items

Exemple 17

En le relisant je me rends compte que j'aurais dû mettre une équivalence. Le but de cet item et de teaser l'argument de dévissage au cas monogène dans mon premier développement sur le théorème de Springer.

Théorème 35

Se déduit de la structure des extensions finies pour se ramener au cas monogène et de la proposition 34. C'est une amélioration de la borne naïve $n!$ où n est le degré de l'extension.

Exemple 40

Critère d'irréductibilité original dont la preuve se déduit de l'existence des corps de rupture. A connaître et à caser partout.

Items 47 à 55

Cette présentation permet de montrer qu'on a bien compris comment sont construits les corps finis. Point sur lequel on a vite fait de faire un raisonnement circulaire et qui est central dans la leçon des corps finis.

Exemple 58

Sous réserve de temps, il est bienvenu d'accompagner cet item des tables d'opérations de $\mathbb{F}_4$ en annexe. Elle est dans le Gozard (ou le Ulmer ?)

Théorème 59 et corollaire 60

Peut faire un beau développement.

Théorème 66

Résultat non-trivial qui fait aussi un beau développement pour cette leçon. Attention, on en a besoin si on fait Gauss-Wantzel ! En effet, on a besoin de connaître le polynôme minimal des extensions cyclotomiques... Donc il faut avoir conscience qu'on l'utilise et avoir en tête une idée de la preuve. (Gauss-Wantzel nous force donc à parler de cyclotomie dans toutes les leçons où on le recase...)

Application 67

C'est un résultat connu et ça fait donc une belle application de l'irréductibilité des polynômes cyclotomiques. Par contre ce n'est pas immédiat. Mais ça vaut le coup d'y passer un peu de temps. (Ca serait trop court pour un développement par contre.) C'est très bien fait dans le Berhuy.

Théorème 69

Je l'écris proprement là pour pouvoir m'y référer pendant mon développement sur Gauss-Wantzel. (Attention, je donne quand même l'idée de la preuve à l'oral parce que c'est quand même central dans le développement.)

Définitions 70 & 71

C'est la façon la plus économique que j'ai trouvé pour introduire l'ensemble des nombres constructibles. Je faisais toute cette section III. de tête car je n'ai jamais trouvé de bouquin qui faisait correctement les constructions à la règle et au compas. (C'est-à-dire dans le plan complexe. Pourquoi tout le monde fait ça dans $\mathbb{R}^2$?? Quelle horreur...) Le moins pire est le Berhuy parce qu'il y a pas mal de dessins.

Exemple 75

Contre-exemple au théorème de Wantzel indispensable. Il y a des vidéos de Caldero dessus pour les détails.

5 Références

Majoritairement le Gozard, complété par le Ulmer. J'utilise le Rombaldi pour l'item 59 et le Berhuy pour l'item 67 et pour les constructions à la règle et au compas. (Il faut en mettre 2/3 en annexe idéalement.)