Leçon 125 : Extensions de corps. Exemples et applications.

Développements :

Polynômes irréductibles sur F_q, Théorème de l'élément primitif.

Bibliographie :

Tauvel (corps commutatifs et théorie de Galois), Rombaldi, Gozard, Perrin, Escofier, Berhuy, Gourdon, Papini.

Rapport du jury :

Le théorème de la base téléscopique et ses applications à l'irréductibilité de certains polynômes, ainsi que les corps finis sont incontournables. De même 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. S'ils le désirent, les candidats peuvent s'aventurer en théorie de Galois ou expliquer comment l'utilisation du résultant permet de calculer des polynômes annulateurs de sommes et de produits de nombres algébriques.

Intro

Evoquer le résultant pour le calcul de polynômes minimaux ? cf Rombaldi.

1 Corps et extensions de corps

1.1 Premières définitions

Définition 1 (Tauvel Corps comm p77). *[Gozard p21] Extension de corps.*

Remarque 2 (Tauvel p77). *[Gozard p21] Identification avec les sous-corps.*

Exemple 3 (Gozard p21). $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$.

Définition 4 (Romb p415). *Caractéristique d'un corps.*

Proposition 5 (Romb p415). *La caractéristique d'un corps fini est un nombre premier.*

Exemple 6. $\mathbb{R}$ *est de caractéristique nulle,* $\mathbb{Z}/p\mathbb{Z}$ *est de caractéristique* p.

Définition 7 (Perrin p72). *[Romb p416] Sous-corps premier.*

Remarque 8. *On identifiera le sous-corps premier avec* F_p.

Remarque 9. *Un corps de caractéristique nulle est infini mais la réciproque est fausse* ($F_p(X)$).

Proposition 10 (Gozard p21). *Tout corps est une extension de son sous-corps premier.*

1.2 Extensions et degré

Proposition 11 (Gozard p22). K *peut être muni d'une structure de* k *algèbre.*

Définition 12 (Tauvel CM p77). *[Gozard p22] Degré d'une extension. Extension finie, infinie.*

Exemple 13 (Gozard p22). $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = +\infty$.

Définition 14 (Tauvel CM p78). *Sous-extension.*

Théorème 15 (Gozard p22). *[Tauvel CM p78] Théorème de la base télescopique.*

Proposition 16 (Tauvel CM p78). *[Romb p247] Multiplicativité des degrés.*

Application 17 (Tauvel CM p79). *Si* $[L : k]$ *est un nombre premier, il n'existe aucun corps* K *vérifiant* $k \subset K \subset L$.

1.3 Extensions de type fini

Définition 18 (Gozard p23). *Sous extension engendrée par une partie.*

Définition 19. *Quand la partie est finie, on note* $k(\alpha_1, .., \alpha_n)$ *et on dit que l'extension est de type finie et monogène si* $n = 1$.

Exemple 20. $Q(\sqrt{2})$ *est monogène.*

Proposition 21. *Description de* $K(\alpha)$ *avec les polynômes.*

Exemple 22 (Berhuy p774). $Q(i, \sqrt{2})$, $K(a + b\alpha) = K(\alpha)$, $Q(\sqrt{d})$.

Proposition 23. *Une extension de degré fini est de type fini.*

Contre exemple 24. $k(X)/k$ *est monogène mais de degré infini.*

Application 25 (Gozard p24). *Si* $[L : k]$ *est un nombre premier, alors* L *est une extension simple de* k.

1.4 Eléments algébriques et transcendants

Définition 26 (Berhuy, Gozard). *Morphisme d'évaluation et noyau.*

Définition 27 (Romb p245). *[Perrin p66] Elément algébrique. Elément transcendant.*

Exemple 28. *e et π sont transcendants. (Admis).*

Exemple 29 (Romb). *Nombres de Liouville sont transcendants sur Q, $\sqrt{13}$ est algébrique sur Q, T est transcendant sur $K(T)$ (sinon extension finie).*

Proposition 30 (Gozard). *Si a est transcendant, $k(X) \to k(a), f(X) \mapsto f(a)$ est un isomorphisme de k-algèbre et donc $[k(a) : k] = \infty$.*

Exemple 31. *$[Q(L) : Q] = \infty$ avec L=nombre de Liouville.*

Définition 32 (Romb p245). *Polynôme minimal. Il est irréductible.*

Proposition 33 (Gozard). *P est le polynome minimal de a si et seulement si P unitaire, annule a et irréductible.*

Exemple 34 (Perrin p66). *[Berhuy p782] $\sqrt{2}$ i sont algébriques sur Q de polynômes minimaux $X^2 - 2, X^2 + 1$. $\sqrt[p]{n}$ est algébrique sur $\mathbb{Q}$, $exp(2ik\pi/n)$ est algébrique sur $\mathbb{Q}$. $\in K(X)$ est transcendant sur K [Perrin p66].*

Proposition 35 (Romb p246). *[Tauvel p81][Gozard p31] α est algébrique sur K si et seulement si $K[\alpha] = K(\alpha)$ si et seulement si $[K[\alpha] : K] = deg(\Pi_\alpha) < +\infty$. On a alors $[K(\alpha) : K]$ est égal au degré du polynôme minimal et une base est $(1, \alpha, ..., \alpha^{deg(P)-1})$.*

Exemple 36 (Beruy p782). *$[Q(i) : Q] = 2$, $[Q(\sqrt[4]{3}) : Q] = 4$ et $[Q(\sqrt{2}+\sqrt{3}) : Q] = 4$, $[Q(\sqrt{d}) : Q] = 2$, $[Q(i, \sqrt{2}) : \mathbb{Q}(i)] = 2$ donc $[\mathbb{Q}(i, \sqrt{2}) : \mathbb{Q}] = 4$.*

Théorème 37 (Romb p248). *L'ensemble des éléments de L algébriques sur K est un sous-corps de L qui contient K.*

1.5 Extensions algébriques

Définition 38 (Perrin p67). *Extension algébrique.*

Proposition 39 (Gozard p37). *[Romb p252][Tauvel CM p80] Une extension finie est algébrique. En outre, $deg_k(x)$ divise $[K : k]$.*

Proposition 40 (Beruy p783). *Si α_1, ...,α_k sont algébriques sur K, $K(\alpha_1, ..., \alpha_k)$ est de degré fini et est donc algébrique. Donc $K(\alpha_1, ..., \alpha_k) = K[\alpha_1, ..., \alpha_k]$.*

Proposition 41 (Beruy p784). *$K(S)$ est algébrique sur K si et seulement si tout élément de S est algébrique.*

Proposition 42. *Pour $M/L/K$, et $x \in M$ algébrique sur K, on a $Irr(x, L)|Irr(x, K)$ dans L[X].*

Exemple 43. *$\mathbb{C}$ est une extension algébrique de $\mathbb{R}$. $\mathbb{R}$ n'est pas une extension algébrique de $\mathbb{C}$ car e et π sont transcendants. $K(T)$ n'est pas une extension algébrique de K car T est transcendant sur K.*

Théorème 44. *Si $x_1, .., x_n$ sont algébriques sur K, alors $K(x_1, .., x_n)$ est une extension algébrique finie de K, avec $[K(x_1, .., x_n) : K] \leq \prod [K(x_i) : K]$.*

Corollaire 45. *L/K est finie si et seulement si l'extension est algébrique et engendrée par K et par un nombre fini d'éléments.*

Exemple 46 (Perrin p67). *$\sqrt{2} + \sqrt[3]{5}$ est algébrique sur $\mathbb{Q}$.*

Exemple 47 (Perrin p67). *L'ensemble des éléments de $\mathbb{C}$ algébriques sur $\mathbb{Q}$ est un sous-corps de $\mathbb{C}$. $A/\mathbb{Q}$ est algébrique mais n'est pas finie.*

Proposition 48. *Transitivité de l'algébricité.*

2 Exemple de construction de corps ; lien avec les polynômes.

2.1 Corps de rupture

Proposition 49. *Soit $P \in K[X]$. P est irréductible si et seulement si $K[X]/(P)$ est un corps.*

Définition 50 (Romb p418). *Corps de rupture. Un corps de rupture de P sur K est une extension de corps L sur K telle que P admet une racine λ dans L, et telle que L est engendré par K et λ.*

Exemple 51. *$k(\alpha)$ est le corps de rupture du polynôme minimal de α.*

Exemple 52. *$Q(\sqrt[3]{2})$, $Q(\sqrt{2})$.*

Proposition 53 (Perrin p70). *[Beruy pour prop universelle] Soit $P \in K[X]$ irréductible. Il existe un corps de rupture sur K, unique à isomorphisme de K-algèbres près. [Tauvel p100] Si $K = k(a)$ et $K = k(b)$ sont des corps de rupture de P avec a et b racines de P, alors il existe un unique k-isomorphisme θ de K dans L tel que $\theta(a) = b$.*

Théorème 54 (Tauvel CM p100). *Soient k_1 et k_2 des corps et σ un isomorphisme de k_1 sur k_2, P_1 un polynôme irréductible sur k_1 et $P_2 = \sigma(P_1)$. Soit K_1 et K_2 les les corps de rupture de P_1 et P_2 et $a_i \in K_i$ une racine de P_i tel que $K_i = k_i(a_i)$. Il existe un unique isomorphisme θ de K_1 sur K_2 prolongeant σ et tel que $\theta(a_1) = a_2$.*

Corollaire 55. *Pour L/K et $x \in L$ algébrique sur K, $K(x)$ est le corps de rupture de $Irr(x, K)$ sur K.*

Exemple 56 (Gozard p58). *X^2-2 a pour corps de rupture $Q(\sqrt{2})$. X^3-2 a pour corps de rupture $Q(\sqrt[3]{2})$ mais aussi $Q(j\sqrt[3]{2})$. Ainsi, ce polynôme est n'est pas entièrement factorisé sur le corps de rupture.*

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

Proposition 57 (Perrin p78). *P est irréductible si et seulement si P n'a pas de racines dans les extensions d'indice $\leq n/2$.*

Théorème 58 (Perrin p79). *Si $P \in K[X]$ est irréductible de degré n et si L est une extension de degré m avec m et n premiers entre eux, alors P est encore irréductible sur L.*

Exemple 59 (Perrin p79). *X^3+X+1 est irréductible sur $Q(i)$ et sur Q.*

Contre exemple 60 (Perrin p79). *X^4+1 est irréductible sur Q mais pas sur $Q(i)$.*

2.2 Corps de décomposition

Définition 61 (Gozard p59). *Corps de décomposition.*

Exemple 62 (Gozard p60). *$\mathbb{C}$ est un corps de décomposition sur $\mathbb{R}$ de X^2+1. $Q(\sqrt{2})$ est un corps de décomposition sur Q de X^2-2.*

Contre exemple 63. *$Q(\sqrt[3]{2})$ n'est pas un corps de décomposition sur Q de X^3-2 mais simplement un corps de rupture. Son corps de décomposition est $Q(\sqrt[3]{2}, j\sqrt[3]{2})$ extension de degré 6.*

$\mathbb{Q}(i,\sqrt{2})$ est le corps de décomposition de X^4-1 sur $\mathbb{Q}$.

Proposition 64 (Gozard p60). *Existence et unicité du corps de décomposition. Donner l'isomorphisme ?*

Proposition 65 (Tauvel p104). *$[K:k] \leq n!$ où n est le degré du polynome p dont K est un corps de décomposition.*

Théorème 66. *Théorème de l'élément primitif.*

Corollaire 67. *Si K est de caractéristique nulle ou un corps fini et L une extension de K alors $[L:K] \leq n$ si et seulement si pour tout $x \in L$, $[K(x):K] \leq n$.*

Exemple 68 (Francinou Gianella). *Un exemple.*

Application 69 (Gourdon). *Une démonstration du théorème de Cayley-Hamilton sur un corps quelconque.*

2.3 Clôture algébrique

Définition 70 (Gozard p62). *Corps algébriquement clos.*

Exemple 71 (Gozard p62). *Q, $\mathbb{R}$, F_p ne sont pas algébriquement clos.*

Proposition 72 (Gozard p62). *Tout corps algébriquement clos est infini.*

Théorème 73. *(Gozard p62] Théorème de d'Alembert Gauss. $\mathbb{C}$ est algébriquement clos.*

Proposition 74 (Romb p379). *[Gozard p63] Les polynômes réels irréductibles sont les polynômes de degré 1 et de degré 2, $P = aX^2+bX+c$ tels que $b^2-4ac<0$ (polynômes qui n'ont pas de racines réelles.*

Application 75. *Toute matrice de $M_n(\mathbb{C})$ est trigonalisable.*

Remarque 76. *Q (et F_p) admettent des polynômes irréductibles de tout degré.*

Définition 77 (Gozard p63). *Clôture algébrique.*

Théorème 78 (Gozard p63). *(ADMIS) Tout corps admet une clôture algébrique, unique à isomorphisme de K-algèbres près.*

Exemple 79 (Gozard p64). *La clôture algébrique de $\mathbb{R}$ est $\mathbb{C}$.*
La clôture algébrique de Q est l'ensemble des nombres complexes algébriques sur Q.

3 Corps finis

3.1 Construction des corps finis

Proposition 80 (Tauvel CM p7). *Si K est un corps fini de caractéristique p alors sont sous-corps premier est isomorphe à F_p.*
(K est une F_p algèbre de dimension finie en tant que F_p-ev.)

Remarque 81. *On identifiera le sous-corps premier avec F_p.*

Proposition 82 (Tauvel CM p8). *Soit K un corps fini de card q. Alors il existe p premier et $n \in \mathbb{N}$ tels que $q=p^n$ et si q est premier alors K est isomorphe à F_q.*

Remarque 83. *Il n'existe pas de corps fini de cardinal 4 ou 105.*

Application 84 (Perrin p73). *Il existe un corps à $q=p^n$ éléments, c'est le corps de décomposition de X^q-X sur F_p. Il est unique à isomorphisme près, noté F_q.*

Exemple 85 (Beruy). *Construction de l'isomorphisme.*

Application 86. *Théorème de Wilson.*

3.2 Structure des corps finis

Proposition 87. *$F_{p^m} \subset F_{p^n}$ si et seulement si $m|n$.*

Proposition 88 (Perrin p74)**.** *F_q^* est un groupe cyclique de cardinal $q-1$.*

Exemple 89 (Ortiz)**.**

Définition 90 (Papini p69)**.** *Un générateur de K^* est appelé racine primitive de K.*

Corollaire 91 (Elément primitif, Papini p69)**.** *[Papini p69] Si α est un générateur de F_q^* alors $F_q = F_p(\alpha)$.*

Corollaire 92 (Papini p74)**.** *Il existe un polynôme irréductible de degré n sur F_p : le polynôme minimal de α sur F_p.*

Remarque 93. *On peut avoir $F_q = F_p(\alpha)$ sans que α soit générateur de F_q^*.*

Exemple 94 (Escofier p558)**.** *$F_2[X]/(X^4+X^3+X^2+X+1) = F_2[\overline{X}]$ et $\overline{X}$ est d'ordre 5.*

Proposition 95 (Papini p74)**.** *Tout corps fini de cardinal p^n est isomorphe à $F_p[X]/(P)$ où P est un polynôme irréductible de degré n sur F_p.*

Exemple 96 (Rombaldi p438)**.** *F_8, $F_1 6$.*

Exemple 97 (Papini)**.** *F_9.*

Exemple 98 (Berhuy p659)**.** *Exemple d'isomorphismes.*

3.3 Polynômes irréductibles sur les corps finis

Proposition 99. *Algorithme de Berlekamp.*

Exemple 100 (Escofier)**.**

Définition 101. *On note $I(n,q)$ l'ensemble des polynômes irréductibles de degré n sur F_q.*

Proposition 102. *$\forall n \geq 1$, $X^{q^n} - X = \prod_{d|n} \prod_{P \in I(d,q)} P$.*

Définition 103. *Fonction de Mobius.*

Proposition 104. *Pour tout $n \geq 1$, $n.|I(n,q)| = ...$ Puis développement asymptotique.*

Application 105 (Beruy)**.** *Test de Rabin : $P \in F_q[X]$ est irréductible sur F_q si et seulement si P divise $X^{q^n} - X$ et si $pgcd(P, X^{q^d} - X) = 1$ pour tout d diviseur strict de n.*