Rdp : [Goz] Gozard - Théorie de Galois

Dévt : Polynômes cyclotomiques 44 Perr
Polynôme minimal d'un élément de $\mathbb{F}_q$ 46 Tau.

125 Extensions de corps. Exemples et applications.

Cadre : Sauf indication contraire, k, K et L désignent des corps.

I. Corps et extensions de corps.

1) Définitions et premières propriétés.

[Goz] 2,7.

Def 1 : On dit qu'un anneau commutatif unitaire k est un corps si : Tout élément non nul de k est inversible dans k.

Ex 2 : $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{R}(X)$ sont des corps, $\mathbb{R}[X]$ n'est pas un corps.

Prop 3 : Tout morphisme d'anneaux unitaires ayant un corps pour domaine est injectif.

Prop-def 4 : Soit k un corps. Il existe un unique morphisme d'anneaux unitaires non trivial de $\mathbb{Z}$ dans k. Le générateur positif du noyau de ce morphisme est noté $\mathrm{car}\, k$ et appelé la caractéristique de k.

Ex 5 : $\mathrm{Car}(\mathbb{F}_p) = p$. $\mathrm{Car}\, \mathbb{Q} = 0$.

Prop 6 : La caractéristique d'un corps fini est non nulle mais la réciproque est fausse ! $\mathbb{F}_p(X)$ est de caractéristique p.

Prop-def 7 : Soit k un corps. On appelle sous-corps premier de k l'intersection de tous les sous-corps de k. Si $\mathrm{car}\, k = 0$, il est isomorphe à $\mathbb{Q}$. Si $\mathrm{car}\, k = p > 0$, il est isomorphe à $\mathbb{F}_p$.

[Goz] 21 22

Def 8 : Soit k un corps. On appelle extension de k tout morphisme de corps $k \to K$. On notera K/k pour "K est une extension de k".

Ex 9 : On a la tour d'extensions $\mathbb{C} - \mathbb{R} - \mathbb{Q}$.

Rq 10 : Comme tout morphisme de corps est injectif. On a équivalence entre K/k et $k \subseteq K$ (k est un sous-corps de K).

Prop 11 : Tout corps est extension de son sous-corps premier. Donc tout corps de caractéristique $p > 0$ (resp 0) est extension de $\mathbb{F}_p$ (resp de $\mathbb{Q}$).

Prop 12 : Soit K/k une extension. $(K, +, \cdot)$ muni de la multiplication par les scalaires de k est une k-algèbre, on note $[K : k]$ sa dimension, appelée le degré de K sur k.

Ex 13 : Le degré peut être fini : $[\mathbb{C} : \mathbb{R}] = 2$, ou infini $[\mathbb{R} : \mathbb{Q}] = +\infty$.

Thm 14 (Base télescopique) : Soient $L/K/k$ une tour d'extensions, $(x_j)_{j \in J}$ une K-base de L et $(\beta_i)_{i \in I}$ une k-base de K. Alors $(x_j \beta_i)_{i,j \in I \times J}$ forme une k-base de L.

En particulier, si les degrés manipulés sont finis, on a $[L : k] = [L : K][K : k]$. (formule de multiplicativité des degrés).

[Goz] 23

Rq 15 : On a $[K : k] = 1 \iff k = K$.

Def 16 : Soient L/k une extension, et $P \subset L$. Il existe un plus petit sous-corps de L contenant k et P, on le note $k(P)$ et il est appelé extension intermédiaire de L/k engendrée par P.

Prop 17 : Si L/k une extension, K_1 et K_2 deux extensions intermédiaires, $[k(K_1 \cup K_2) : k] \mid [K_1 : k][K_2 : k]$ et $\mathrm{ppcm}([K_1 : k], [K_2 : k]) \mid [L : k]$

2) Extensions algébriques.

[Goz] 30 33

Def 18 : Soit K/k une extension, on dit que K/k est de type fini s'il existe $\alpha_1, \dots, \alpha_n \subseteq K$ telle que $k(\alpha_1 \dots \alpha_n) = K$.

Prop 19 : Une extension de degré fini est de type fini, mais $k(X)$ donne un contre exemple à la réciproque.

Ex 20 : $\mathbb{C} = \mathbb{R}(i)$.

Def 21 : Si K/k une extension, et $\exists \alpha \in K$ telle que $k(\alpha) = K$, on dit que K/k est monogène et α est un élément primitif de K. (un tel élément n'est pas unique).

Dans la suite, on considère K/k une extension, $\alpha \in K$ on a un morphisme $k[X] \to K$ d'évaluation en α.

Prop-def 22 : Soit $\alpha \in K$ on a un morphisme $k[X] \to K$ d'évaluation en α. L'un des deux cas suivants est réalisé :
- Ce morphisme est injectif, on dit alors que α est transcendant sur k
- Ce morphisme admet un noyau I_α, engendré par un polynôme unitaire non trivial P_α, dit polynôme minimal de α.

Ex 23 : Tout nombre complexe strict λ est algébrique sur $\mathbb{R}$, de polynôme minimal $X^2 + |\lambda|^2$.

Rq 24 : Le polynôme minimal P de α algébrique sur k est caractérisé par les propriétés suivantes : $P \in k[X]$ est unitaire et $\forall R \in k[X]^*$, $R(\alpha) = 0 \Rightarrow d^\circ P \leq d^\circ R$.

Prop 25 : Soit $P \in k[X]$, P est le polynôme minimal de α si et seulement si : $P(\alpha) = 0$, P est unitaire et irréductible dans $k[X]$.

Ex 26 : Dans l'extension $\mathbb{R} - \mathbb{Q}$, pour $n \in \mathbb{N}$, le polynôme minimal de $2^{\frac{1}{n}}$ sur $\mathbb{Q}$ est $X^n - 2$.

Théo 27 : (Structure des extensions monogènes) Soient K/k une extension et $\alpha \in K$.
- Si α est transcendant, l'évaluation en α donne un isomorphisme entre $k(\alpha)$ et $k(X)$.
- Si α est algébrique, alors $k(\alpha) = k[\alpha]$, on a un isomorphisme $k(\alpha) \simeq k[X]/(P_\alpha)$, $[k(\alpha) : k] = d^\circ P_\alpha$ et $1, \alpha, \dots, \alpha^{d-1}$ où $d = d^\circ P_\alpha$ est une k-base de $k(\alpha)$, l'entier d est le degré de α sur k.

Théo 28 : Si k-h est une extension, en posant $M = \{x \in K \mid x \text{ est algébrique sur } k\}$ alors M est une extension intermédiaire de K et k

Prop 29 Toute extension finie est algébrique, mais la réciproque est fausse : $\mathbb{R}-\mathbb{Q}$, prendre l'ensemble des éléments algébriques sur $\mathbb{Q}$.

II Adjonction de racines

1) Corps de rupture.

On cherche ici à construire des extensions.

Def 30 Soit $P \in k[X]$ irréductible. On dit que le corps K est un corps de rupture pour P si : K est une extension monogène de k, dont un élément primitif est racine de P :

$$\exists \alpha \in K \mid K = k(\alpha) \text{ et } P(\alpha) = 0.$$

Ex 31 : Si $d^\circ P = 1$, k est corps de rupture pour P. Certains corps de rupture pour X^2+1 sont $\mathbb{R}$, mais pas sur $\mathbb{Q}$.

Théo 32 : Si $P \in k[X]$ est irréductible, alors il existe un corps de rupture pour P. De plus, deux corps de rupture sont k-isomorphes (isomorphes comme k-algèbre).

Ex 33 : On peut construire le corps à 4 éléments comme corps de rupture de X^2+X+1 sur $\mathbb{F}_2$.

Cor 34 : $\forall P \in k[X]$, $d^\circ P \geq 1$, $\exists K$-h extension algébrique monogène dans laquelle P a une racine (au moins).

Prop 35 : Un polynôme $P \in k[X]$ de degré n est irréductible dans $k[X]$ si et seulement si il n'admet pas de racine dans toute extension de k de degré $\leq \frac{n}{2}$.

Ex 36 : Un polynôme de degré 2 ou 3 est irréductible si et seulement si il n'admet pas de racines dans k.

Prop 37 : Si $P \in k[X]$ de degré n irréductible. Et L-k de degré m premier à n, alors P est irréductible dans $L[X]$.

Ex 38 X^3+X+1 est irréductible sur $\mathbb{Q}(i)$, tout polynôme irréductible sur $\mathbb{R}$ est de degré au plus 2.

2) Corps de décomposition.

Def 39 : Soit K-h une extension, $P \in k[X]$ de degré $n \geq 1$. On dit que K est un corps de décomposition de P sur k si : P est scindé dans $K[X]$ et si K est engendré par les racines de P.

Rq 40 : Un corps de décomposition est une extension finie. ~~~

Un corps de décomposition est une extension minimale de k contenant toutes les racines (avec multiplicité) de P.

Théo 41 : Soit $P \in k[X]$ de degré ≥ 1. Il existe un corps de décomposition de P sur k, de degré au plus $n!$. De plus, deux corps de décomposition de P sont k-isomorphes.

Ex 42 : Si $d^\circ P = 2$, les notions de corps de rupture et de corps de décomposition sont confondues. $\mathbb{Q}(\sqrt[3]{2})$ n'est pas corps de décomposition de X^3-2, il manque j.

Théo 43 : Pour p premier et $q = p^n$, il existe un unique (à isomorphisme près) corps de cardinal q, noté $\mathbb{F}_q$, et défini comme corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$.

Appl 44 : Pour $n \geq 1$, le polynôme cyclotomique $\Phi_n \in \mathbb{Z}[X]$ est irréductible et à coefficients entiers. De plus, pour p et $n \in \mathbb{N}$, $p \wedge n = q$. Les facteurs irréductibles de Φ_n dans $\mathbb{F}_p$ sont de degré ordre de q dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Perr

DVP

Def 45 : Pour $n \geq 1$, on définit la fonction de Möbius par : $\mu(n) = 0$ si n est divisible par un carré parfait, sinon $\mu(n) = (-1)^d$ où $d = \#\{p \in \mathbb{P} \mid p \mid n\}$.

Théo 46 : Pour $n \in \mathbb{N}^*$, $q = p^k$, il y a $\sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$ polynômes de degré n irréductibles dans $\mathbb{F}_p$, cette formule équivaut à $\frac{q^n}{n}$ pour $n \to \infty$ Tou

DVP

Cor 47 : En particulier, il existe des polynômes irréductibles de tout degré.

3) Clôture algébrique.

Prop-def 48 : Soit k un corps, équivalents sont : - Tout polynôme non constant est scindé sur k.
- Tout polynôme non constant admet une racine dans k.
- Ses seuls polynômes irréductibles sur k sont de degré 1.
- Toute extension algébrique de k lui est égale.

On dira alors que k est algébriquement clos.

Ex 49 : $\mathbb{R}$ n'est pas, algébriquement clos, un corps fini n'est pas algébriquement clos.

Théo 50 (D'Alembert Gauss) : $\mathbb{C}$ est algébriquement clos.

Cor 51 : Les polynômes irréductibles de $\mathbb{R}$ sont les polynômes de degré 1 et ceux de deg 2 de discriminant négatif strictement

Def 52 : Une extension K-k est dite clôture algébrique de k si : elle est algébrique et K est algébriquement clos

Ex 53 : $\mathbb{C}$ est une clôture algébrique de $\mathbb{R}$, mais pas de $\mathbb{Q}$.

Prop 54 : Si K-k est une extension tel K est algébriquement clos, l'ensemble des éléments de K algébriques sur k est une clôture algébrique de k.

[603]

Théo 55 (Steinitz) Tout corps admet une clôture algébrique. De plus, deux clôtures algébriques d'un corps k sont k-isomorphes.

Ex 56 : L'ensemble $\overline{\mathbb{Q}}$ des complexes algébriques sur $\mathbb{Q}$ en forme une clôture algébrique.

$\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$ est une clôture algébrique de $\mathbb{F}_p$.

III. Extensions normales, séparables, galoisiennes.

1) Extension séparable.

Prop 57 : Soit K-k une extension. P, Q ∈ k[X], on a P|Q dans k[X] ⇔ P|Q dans K[X].

Def 58 : On dit que P ∈ k[X] est séparable s'il est simplement scindé dans un corps de décomposition. Pour K-k une extension on dit que α ∈ K est séparable si P_α est séparable, et que K est séparable si tous ses éléments le sont.

Prop 59 : Si P ∈ k[X] est irréductible, P est séparable si et seulement si son polynôme dérivé est non nul.

Cor 60 : Si k est de caractéristique 0, toute extension de k est séparable.

Prop-def 61 : Équivalents sont :
- Toute extension algébrique de k est séparable sur k
- La clôture algébrique de k en est une extension algébrique.

Si ces conditions sont réalisées, on dit que k est un corps parfait.

Prop 62 : Si car k = p. Le morphisme de Frobenius $x \mapsto x^p$ est surjectif sur k si et seulement si k est parfait.

Appli 63 : Les $\mathbb{F}_q$ sont tous des corps parfaits. Un corps algébriquement clos est parfait.

Ex 64 : Soit p un nombre premier, $\mathbb{F}_p(T)$ n'est pas parfait : $X^p - T \in \mathbb{F}_p(T)[X]$ est irréductible.

Théo 65 (Élément primitif) Soit K-k une extension finie séparable. Alors K-k a un élément primitif : ∃ x ∈ K | K = k(x).

Théo 66 : Soit K-k une extension finie, elle admet un élément primitif si et seulement si il existe un nombre fini d'extensions intermédiaires.

2) Extensions normales.

Def 67 : Soit K-k une extension algébrique. On dit que l'extension est normale si tout polynôme irréductible sur k ayant une racine dans K a toutes ses racines dans K.

Ex 68 : k est normal sur lui-même. La clôture algébrique de k est normale sur k. Toute extension de degré 2 (corps de rupture) est normale.

Théo 69 : Soit K-k une extension finie. Elle est normale si et seulement si elle s'écrit comme corps de décomposition d'un polynôme sur k.

Prop 70 : Si K-k est finie, normale et séparable, alors elle s'écrit comme corps de décomposition d'un polynôme de k[X] irréductible.

Prop 71 : Si L-K-k est une tour d'extensions avec L normale sur k, alors L est normale sur K. Mais K n'a pas de raisons d'être normale sur k.

Ex 72 : $\mathbb{Q}(\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, j) = \mathbb{Q}$.

3) Groupe de Galois, extension galoisienne.

Def 73 : Soient K-k et L-k deux extensions, les k-homomorphismes de K dans L sont les morphismes de k-algèbres de K dans L. On définit Gal(K-k) le groupe de Galois de K-k comme le groupe des k-automorphismes de K.

Prop 74 : Pour f : k → k un morphisme de corps, $\{x \in k \mid f(x) = x\}$ est un sous-corps de k noté Inv(f).

Théo 75 : Si k-k est finie, on a |Gal(K-k)| ≤ [K:k]. Dans le cas d'égalité, on dit que K est galoisienne finie.

Théo 76 : Si K-k, le corps F = Inv(Gal(K-k)) est une extension intermédiaire, K-F est galoisienne, et K-k est galoisienne ssi k = F.

Théo 77 K-k finie est galoisienne si et seulement si elle est normale et séparable.

On définit donc une extension galoisienne comme une extension algébrique normale séparable.

Soit L-k une extension K une extension intermédiaire, Gal(K-k) est un sous-groupe de Gal(L-k).

De même, pour G ≤ Gal(K-k), Inv(G) est une extension intermédiaire à L-k.

Théo 78 (Correspondance de Galois) Si L-k est galoisienne finie. La correspondance entre les sous-groupes de Gal(L-k) et les corps invariants est décroissante et bijective (pour l'inclusion).

De plus, si M-k est galoisienne, Gal(M-k) ≃ Gal(L-k)/Gal(L-M).

Rq 79 : Si g ∈ Gal(K-k), et α est racine de P ∈ k[X], g(α) en est aussi une : Gal(K-k) agit sur les racines de P dans K. Cette action est transitive.

Ex 80 : Pour l'ex 72, on a