

Leçon 125 : Extension de corps. Exemples et applications.

[Ber] : *Algèbre, le grand combat*, Grégory Berhuy

[Goz] : *Théorie de galois*, Ivan Gozard

[Sau-Ran] : *Cours de calcul formel. Corps finis, systèmes polynomiaux, applications*, Phillipe Saux Picart, Eric Rannou

[Szp] : *Mathématiques Algèbre L3*, Aviva Szpirglas

I Partie A - Les bases [Goz] [Szp]

I.1 Définitions [Goz] [Szp]

■ **Déf 1 (Extension de corps) :**

■ **Ex 2 :** $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{R}$, $K(X)/K[X]$.

Rem 3 : Tout corps est un sur-corps de son sous-corps premier.

■ **Déf 4 (Degré, extension finie) :**

■ **Ex 5 :** $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R}, \mathbb{Q}] = \infty$.

Thm 6 (Base télescopique) :

■ **Cor 7 (Multiplicativité du degré) :**

■ **Déf 8 (Sous-corps engendré par une partie) :**

■ **Ex 9 :** $\mathbb{Q}(i)$ est le sous-corps de $\mathbb{C}$ engendré par i .

■ **Ex 10 :** $K(S) = \text{Frac}(K[S])$, où S est une partie.

■ **Déf 11 :** Une extension est de type fini si $L = K(\alpha_1, \dots, \alpha_n)$

■ **Prop 12 :** Une extension finie est de type fini.

■ **Contre-Ex 13 :** $\mathbb{Q}(\pi)/\mathbb{Q}$, $K(X)/K$.

■ **Déf 14 (Extension monogène, élément primitif) :**

■ **Ex 15 :** $K(X)$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

■ **Contre-Ex 16 :** $K(X, Y)$ n'est pas monogène.

■ **Prop 17 :** Si $[L : K]$ est premier, alors L/K est monogène.

I.2 Éléments algébriques, éléments transcendants, extension algébrique [Goz] [Ber] [Szp]

■ **Déf 18 (Élément algébrique, transcendant) :**

■ **Ex 19 :** Racines de l'unité, exemples classiques (voir [Szp]).

■ **Ex 20 :** Nombres de Liouville.

■ **Ex 21 :** π , e

■ **Déf 22 (Polynôme minimal) :**

■ **Ex 23 :** $\deg(\pi_x) = 1$ ssi $x \in K$

■ **Prop 24 :** P est le polynôme minimal de x ssi P est unitaire, irréductible et $P(x) = 0$.

■ **Ex 25 :** Pour $\mathbb{R}/\mathbb{Q}$, $X^n - 2$ est le polynôme minimal de $\sqrt[n]{2}$ sur $\mathbb{Q}$.

Thm 26 (Base de $K(a)$) :

■ **Ex 27 :** Voir [Ber].

Thm 28 (Caractérisation des éléments algébriques) :

Rem 29 : $K[X]/\langle \pi_x \rangle = K[x]$.

■ **Déf 30 (Extension algébrique) :**

■ **Prop 31 :** Soit L une extension algébrique de K . Soit A une K -algèbre intermédiaire. Alors A est un corps.

■ **Prop 32 :** Toute extension de degré fini de K est algébrique sur K .

Rem 33 : Le degré $[K(x) : K]$ divise $[L : K]$.

■ **Prop 34 :** Soit $L = K(\alpha_1, \dots, \alpha_n)$ une extension de type fini. Si les α_i sont algébriques sur K , alors L est de degré fini et $L = K[\alpha_1, \dots, \alpha_n]$

Thm 35 (Transitivité de l'algébricité) :

II Partie B - Extensions de corps particulières [Goz] [Ber]

II.1 Corps de rupture

■ **Déf 36 (Corps de rupture) :**

■ **Ex 37 :** Voir [Ber]

■ **Ex 38 :** Construction de $\mathbb{F}_4$. [Annexe : Tables d'opérations].

■ **Thm 39 (Existence et unicité du corps de rupture) :**

App 40 : Si $P \in K[X]$, il existe une extension dans laquelle P possède une racine.

II.2 Corps de décompositions

■ **Déf 41 (Corps de décomposition) :**

■ **Ex 42 :** Voir [Szp].

■ **Contre-Ex 43 :** Voir [Szp].

■ **Thm 44 (Existence et unicité du corps de décomposition) :**

App 45 (Existence et unicité des corps finis) :

■ **Prop 46 (Élément primitif) :**

II.3 Clôture algébrique

■ **Déf 47 (Algébriquement clos) :**

■ **Ex 48 (D'Alembert-Gauss) :**

■ **Déf 49 (Clôture algébrique) :**

■ **Ex 50 :** Clôture de $\mathbb{Q}$, de $\mathbb{R}$.

■ **Thm 51 (Steinitz) :**

III Partie D - Extensions cyclotomiques [Goz]

III.1 Corps cyclotomiques

■ **Déf 52 (Corps cyclotomique) :**

■ **Déf 53 (Polynôme cyclotomique) :**

■ **Ex 54 :** $\Phi_{1,\mathbb{Q}}(X) = X - 1$, $\Phi_{2,\mathbb{Q}}(X) = X + 1$, $\Phi_{3,\mathbb{Q}}(X) = X^2 + X + 1$, $\Phi_{4,\mathbb{Q}}(X) = X^2 + 1$

■ **Prop 55 :** $X^m - 1 = \prod_{d|m} \Phi_{d,\mathbb{Q}}(X)$.

■ **Thm 56 :** $\forall n \in \mathbb{N}^*$, $\Phi_{n,\mathbb{Q}}(X) \in \mathbb{Z}[X]$ et est irréductible dans $\mathbb{Q}[X]$.

App 57 : Le polynôme minimal de toute racine primitive n -ième est $\Phi_{n,\mathbb{Q}}(X)$, et $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

III.2 Sommes de Gauss [Goz] [Sau-Ran]

■ **Déf 58 (Somme de Gauss) :**

■ **Dév 59 (Lemme somme de Gauss) :**

■ **Dév 60 (Kronecker-Weber) :**

■ **Déf 61 (Symbole de Legendre, résidu quadratique) :**

■ **Ex 62 :** Résidus quadratiques dans $\mathbb{F}_5$.

■ **Prop 63 :** On a $\left(\frac{x}{p}\right) = x^{(p-1)/2}$ dans $\mathbb{F}_p$.

App 64 (Réciprocité quadratique) :

■ **Dév 65 (Nombres de Mersennes) :**

IV Partie E - De la géométrie [Goz] [Ber]

■ **Déf 66 (Points constructibles à partir d'un ensemble) :**

■ **Ex 67 :** Constructions géométriques ([Goz]).

■ **Déf 68 (Nombres constructibles) :**

■ **Thm 69 :** L'ensemble des nombres constructibles forme un corps, stable par racine carrée.

App 70 : Quelques exemples de nombres constructibles.

■ **Thm 71 (Wantzel) :**

App 72 : $\sqrt[3]{2}$ n'est pas constructible + duplication du cube.

| Déf 73 (Polygone constructible) :

| Thm 74 (Gauss-Wantzel) :

| Ex 75 : Le pentagone est constructible.