Leçon n°125 : Extensions de corps. Exemples et applications.

Dans toute la suite on considérera $\mathbb{K}$, $\mathbb{L}$ et $\mathbb{M}$ trois corps.

I/ Extensions de corps.

A/ Définitions générales. [PER]

Définition 1 : Extension.

Exemple 2 : Exemples d'extensions.

Remarque 3 : Si $\mathbb{L}/\mathbb{K}$ est une extension alors $\mathbb{L}$ est un $\mathbb{K}$-espace vectoriel.

Définition 4 : Degré d'une extension.

Remarque 5 : Pour des corps finis, $|\mathbb{L}| = |\mathbb{K}|^n$.

Théorème 6 : Multiplicativité des degrés.

Définition 7 : $\mathbb{K}[\alpha]$ et $\mathbb{K}[\alpha_1, \dots, \alpha_n]$.

B/ Éléments algébriques et transcendants. [PER]

Définition 8 : Élément algébrique, transcendant et polynôme minimal.

Exemple 9 : $T \in \mathbb{K}(T)$ est transcendant sur $\mathbb{K}$, $\sqrt{2}$, i sont algébriques.

Proposition 10 : Si α est transcendant, alors $\mathbb{K}[\alpha] \simeq \mathbb{K}[T]$ et $\mathbb{K}(\alpha) \simeq \mathbb{K}(T)$.

Théorème 11 : Équivalence pour les éléments algébriques.

Proposition 12 : Le polynôme minimal est irréductible et définit le degré d'un élément algébrique.

Exemple 13 : $\mathbb{Q}(\sqrt{2})$ et $\mathbb{Q}(i)$ sont des extensions de degré 2 sur $\mathbb{Q}$. Les racines primitives n-èmes de l'unité sont algébriques de degré $\varphi(n)$.

Définition 14 : Extensions finies et algébriques.

Proposition 15 : Une extension finie est algébrique.

Théorème 16 : Si $\mathbb{L}/\mathbb{K}$ est une extension, alors $\mathbb{M} = \{x \in \mathbb{L} \mid x \text{ est algébrique sur } \mathbb{K}\}$ est un sous-corps de $\mathbb{L}$.

Remarque 17 : On peut utiliser le résultant pour calculer des polynômes annulateurs de sommes ou produits de nombres algébriques.

Définition 18 : Corps algébriquement clos.

Exemple 19 : $\mathbb{C}$.

Théorème 20 : Critère d'Eisenstein.

Remarque 21 : $X^n - 2$ est irréductible sur $\mathbb{Q}$ pour tout $n \in \mathbb{N}^*$, donc $\overline{\mathbb{Q}}$ est de dimension infinie en tant que $\mathbb{Q}$-ev.

II/ Extensions et polynômes.

A/ Corps de rupture. [PER]

Définition 22 : Corps de rupture.

Théorème 23 : Existence et unicité.

Exemple 24 : Exemples de corps de rupture.

Théorème 25 : $P \in \mathbb{K}[X]$ de degré n est irréductible $\iff$ P n'a pas de racine dans les extensions de degré au plus $\frac{n}{2}$ de $\mathbb{K}$.

Corollaire 26 : $X^4 + 1$ réductible mod tout p mais est irréductible sur $\mathbb{Q}$ (c'est le 8ème polynôme cyclotomique).

B/ Corps de décomposition. [PER]

Définition 27 : Corps de décomposition.

Théorème 28 : Existence et unicité.

Exemple 29 : Exemples de corps de décomposition.

Théorème 30 : Théorème de l'élément primitif.

Remarque 31 : Le théorème de l'élément primitif est faux en général, considérer un corps infini de caractéristique non nulle.

C/ Corps finis. [PER] [ROM] [OBJ]

Définition 32 : Caractéristique et inclusion selon la caractéristique.

Remarque 33 : Un corps fini est de cardinal une puissance d'un nombre premier.

Proposition 34 : Morphismes de Frobenius.

Théorème 35 : Existence et unicité des corps finis.

Proposition 36 : $\mathbb{F}_q^\times$ est cyclique.

Remarque 37 : Ce résultat permet de démontrer le théorème de l'élément primitif dans le cas fini.

Développement 1

Notation 38 : Notation $U_n(p)$ et $I(n,p)$.

Théorème 39 : $X^{p^n} - X = \prod_{d|n} \prod_{P \in U_d(p)} P$, équivalent et $I(n,p) \geq 1$.

Corollaire 40 : Il existe des polynômes irréductibles de tout degré, donc construction explicite de $\mathbb{F}_q = \mathbb{F}_p[X]/(P)$ où P irréductible de $\mathbb{F}_p[X]$ de degré n, plus facile à manipuler informatiquement.

Exemple 41 : Construction de $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$ et $\mathbb{F}_9 = \mathbb{F}_3[X]/(X^2+1)$.

Algorithme 42 : Algorithme de Berlekamp.

III/ Nombres constructibles.

A/ Définitions et propriétés. [CAR]

Définition 43 : Points constructibles.

Proposition 44 : Construction des parallèles, médiatrices, bissectrices.

Théorème 45 : L'ensemble $\mathcal{C}$ des nombres constructibles est un sous-corps de $\mathbb{R}$ stable par racine carrée.

B/ Lien avec la théorie des corps. [CAR]

Lemme 46 : Équations pour droites et cercles.

Développement 2.a)

Théorème 47 : Théorème de Wantzel.

Corollaire 48 : Résultat de Wantzel.

C/ Réponse aux trois problèmes historiques. [CAR]

Développement 2.b)

Corollaire 49 : La duplication du cube est impossible.

Corollaire 50 : La quadrature du cercle est impossible.

Corollaire 51 : La trissection de l'angle est impossible en général.

Références :

- [PER] Perrin p. 65-80
- [ROM] Rombaldi Algèbre 2nd éd. p. 415
- [CAR] Carréga Théorie des corps p. 13-37
- [OBJ] Beck, Malick Peyré Objectif Agrégation p. 244