NOM : FROT Prénom : Robin Jury : B. Winkler

Algèbre ← Entourez l'épreuve → Analyse

Sujet choisi : 125 Extensions de corps. Exemples et Applications

Autre sujet :

I Extension de corps, algébricité et polynômes.

1) Définitions et premières propriétés

1] Si L et K sont des corps munis d'un morphisme $K \hookrightarrow L$, on dit que L est une extension de K et on le note L/K.

2] - Exemple : $\mathbb{C}/\mathbb{R}$, $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}(X)/\mathbb{C}$ sont des extensions de corps.

3] Remarques : (i) La caractéristique d'un corps est invariante par extension de corps.
(ii) Les morphismes de corps sont toujours injectifs.

4] Si L/K est une extension de corps et $S \subset L$, on note $K(S)$ le plus petit sous corps de L contenant S. On dit que c'est le corps obtenu par adjonction de S à K. Si $S = \{a_1 \dots a_n\}$, on note $K(S) = K(a_1, \dots a_n)$.

5] Proposition : Si L/K est une extension et $S \subset L$, $T \subset L$, on a $K(S \cup T) = K(S)(T)$

6] Exemple $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$

7] Def / Prop L est un K-espace vectoriel, on note $[L:K] = \dim_K(L)$ le degré de l'extension.
On dit que L/K est finie si $[L:K] < +\infty$

8] Théorème (base télescopique)
Soit L/K et M/L deux extensions.
On a $[L:K][M:L] = [M:K]$.

2] Extension algébriques

9] def Soit L/K une extension et $\alpha \in L$.
On pose ev_α $K[X] \to K(\alpha)$
$X \mapsto \alpha$
- Si ev_α est injectif, on dit que α est transcendant.
- Sinon, on dit que α est algébrique

10] exemple :
- π est transcendant sur $\mathbb{Q}$ (Lindemann, admis)
- i est algébrique sur $\mathbb{R}$

11] Prop : Si α est algébrique sur K, il existe un unique polynôme unitaire de degré minimal noté $\mu_{K,\alpha}$ tel que $\mu_{K,\alpha}(\alpha) = 0$

12] Théorème : Les propriétés suivantes sont équivalentes :
(i) α est algébrique sur K
(ii) $K(\alpha) = K[\alpha] = \{P(\alpha), P \in K[X]\}$
(iii) $[K(\alpha):K] < +\infty$
(iv) $K(\alpha) = K[X]/(\mu_{K,\alpha})$

13] Def : On dit que L est une extension algébrique sur K si tous ses éléments sont algébriques sur K. Sinon L/K est dite transcendante.

14 ex : $\mathbb{C}/\mathbb{R}$, ~~$\mathbb{Q}$~~ $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ sont algébriques
$\mathbb{R}/\mathbb{Q}$, $\mathbb{C}(X)/\mathbb{C}$ sont transcendantes

$(\sqrt{2}+\sqrt{3})^2 = 2+3+2\sqrt{3}\sqrt{2}$

3) Polynômes, corps de décomposition et extensions séparables.

15] Soit $P \in K[X]$. On appelle corps de décomposition de P tout corps $E \supset K$ tel que P est scindé sur E et pour tout corps E' où P est scindé si $E' \subset E$ alors $E' = E$.

16] Théorème : Tout polynôme de $K[X]$ admet un corps de décomposition E. De plus si ses racines dans E sont $(\alpha_1, \dots, \alpha_n)$ on a $E = K[\alpha_1 \dots \alpha_n]$

17] Exemple : $\mathbb{C}$ est le corps de décomposition de X^2+1 sur $\mathbb{R}$.

18] Def : (i) $P \in K[X]$ est dit séparable si il est scindé à racine simple dans un corps de décomposition.

(ii) Si L/K est une extension, $\alpha \in L$ algébrique, α est dit séparable si $\mu_{K,\alpha}$ est séparable. ← simple dans une bonne ext.

(iii) Une extension algébrique L/K est dite séparable si tout $\alpha \in L$ est séparable.

(iv) Un corps K est dit parfait si toutes ses extensions algébriques sont séparables.

19] Théorème : Un corps est parfait si et seulement si : $\mathrm{car}(K) = 0$ ou $\mathrm{car}(K) = p$ et $K = \{a^p, a \in K\}$

20] Théorème (élément primitif) Si L/K est une extension finie et séparable, alors il existe $\alpha \in L$ tel que $K[\alpha] = L$. DEV 4

II Extensions de corps remarquables.

1) Corps finis

20] théorème : Soit K un corps fini de caractéristique p alors $|K| = p^n$ avec $n \in \mathbb{N}$

21] Si K est fini, le groupe multiplicatif K^* est

22] Soit $n \in \mathbb{N}^*$. Soit K un corps fini de caractéristique p. $|K| = p^n$ si et seulement si K est corps de décomposition sur $\mathbb{F}_p$ de $X^{p^n} - X$

23] Cor. Pour tout $n \in \mathbb{N}$, p premier il existe un corps de cardinal p^n noté $\mathbb{F}_{p^n}$ unique à $\mathbb{F}_p$-isomorphisme près.

24) Théorème Soient s et n dans $\mathbb{N}$ et p premier.

$\mathbb{F}_{p^s} \subset \mathbb{F}_{p^n} \iff s \mid n$

25] ~~Toute~~ Thm toute extension finie d'un corps K fini est simple et séparable.

2) Extensions cyclotomiques sur $\mathbb{Q}$

26] Def : Soit K un corps. On appelle racine n-ème de l'unité de K les racines de $X^n - 1 \in K[X]$ dans le corps de décomposition.

On note U_n le groupe des racines n-ème de l'unité.

On note Ω_n l'ensemble des générateurs de ce groupe appelés racines primitives n-ème de l'unité.

27] Def : Si $\omega \in \Omega_n^{K=\mathbb{Q}}$ on dit que $\mu_{K\omega}$ est le n-ème polynôme cyclotomique sur K et on le note ϕ_n

28] Prop : On a $\deg \phi_n = \varphi(n) = \mathrm{card}(\Omega_n)$ et ϕ_n est indépendant du choix de ω

~~29] Def~~ On a $\phi_n = \prod_{\omega \in \Omega_n} (X - \omega)$

29] Def Si $\omega \in \Omega_n$ on dit que $K[\omega]$ est la n-ème extension cyclotomique de K.

30] Exemples : $K = \mathbb{Q}$ $\phi_1 = X - 1$, $\phi_2 = X + 1$, $\phi_3 = X^2 + X + 1$

$\phi_4 = X^2 + 1 \dots$

31] Si $K=\mathbb{Q}$, on a pour tout n

(i) $X^n - 1 = \prod_{d|n} \Phi_d(X)$

(ii) $\Phi_n(X)$ est unitaire dans $\mathbb{Z}[X]$

32] Application : Théorème de Wedderburn.
Tout anneau fini à division est commutatif. } DEV2

III Construction à la règle et au compas

On identifie ici le plan $\mathbb{R}^2$ à $\mathbb{C}$ et on fixe $\mathcal{P}_0$ un ensemble de points de $\mathbb{R}^2$.

33] Def (i) Une droite est constructible à partir de $\mathcal{P}_0$ si c'est une droite reliant deux points de $\mathcal{P}_0$.

(ii) Un cercle de centre z_0 de rayon r est constructible à partir de $\mathcal{P}_0$ si $z_0 \in \mathcal{P}_0$ et il existe z_1 et z_2 dans $\mathcal{P}_0$ tels que $|z_1 - z_2| = r$

(iii) Un point est dit constructible à partir de $\mathcal{P}_0$ si c'est l'intersection de deux cercles ou droites constructible à partir de $\mathcal{P}_0$.

34] Def : Un point z est constructible à la règle et au compas si il existe $z_1, \dots, z_n = z$ tels que $\forall i$, z_i soit constructible à partir de $\{0,1\} \cup \{z_1, \dots z_{i-1}\}$.

35] Exemples :

(i) le milieu d'un segment est constructible à la règle et au compas

(ii) la bissectrice d'un angle est constructible

(iii) si z et z' sont constructibles alors : $z+z'$, $z \times z'$, ~~aussi~~ $\bar{z}$ aussi ~~si~~ si $z' \neq 0$, $\frac{z}{z'}$ aussi.

36] Corollaire L'ensemble des nombres constructibles à la règle et au compas forme un sous corps de $\mathbb{C}$ qui contient $\mathbb{Q}$.

37] Théorème (Wantzel)
Soit $z \in \mathbb{C}$. z est constructible à la règle et au compas si et seulement si on a $\mathbb{Q} = K_0 \subsetneq K_1 \dots \subsetneq K_n = \mathbb{Q}[z]$ avec $\forall i \leq n-1$ $[K_{i+1} : K_i] = 2$

38] Exemples

(i) On ne peut pas, de manière générale, trisecter un angle à la règle et au compas (Sauf si $\theta = \pi$)

(ii) On ne peut pas doubler le volume d'un cube de coté donné

(iii) La quadrature du cercle est impossible.

39] Corollaire (Gauss) Un polygône régulier est constructible à la règle ~~et~~ au compas si $e^{\frac{2i\pi}{n}}$ l'est.
C'est le cas si et seulement si $n = 2^k p_1 \cdots p_r$ où $k \in \mathbb{N}$ et $p_1 \dots p_r$ sont premiers de Fermat (i.e. $\exists k_i$, $p_i = 2^{k_i} + 1$)

Leçon 125* : Extensions de corps. Exemples et applications

I) Rqs diverses

Q dev1 — Dev1 : pquoi les hyp séparable ?

commentaires plan
- Motiver + la partie III, intui°, heuristique ps thm de Wantzel
- Mentionner l'intérêt des nbres alg. (eg. solu° des éq° poly.)
- Applica° de la base télescopique

rapport jury — Théorie de Galois "dégradée"

Dès qu'on parle de séparabilité, il y a des questions chiantes sr l'inséparabilité

- C-ex du thm de l'élt prim ?

$\to \begin{cases} L = \mathbb{F}_p(T_1, T_2) & \text{Corps des frac° à 2 indét. sr } \mathbb{F}_p \\ K = \mathbb{F}_p(T_1^p, T_2^p) \end{cases}$

Supposons qu'il existe $\Theta \in L$, $L = K[\Theta]$

$\begin{cases} x = T_1 + T_2 \in L \\ \mu_{K,x} = X^p - T_1^p + T_2^p = (X - T_1 + T_2)^p \end{cases}$

$\hookrightarrow$ extension non sep.

$\Theta = \dfrac{P(T_1, T_2)}{Q(T_1, T_2)} \to \Theta^p = \dfrac{P(T_1, T_2)^p}{Q(T_1, T_2)^p} = \dfrac{P(T_1^p, T_2^p)}{Q(T_1^p, T_2^p)} \in K$

Idée de la leçon — Intérêt d'une exten° de corps (en dehors d'un cxte particulier) : pouvoir manipuler + de nbres pr simplifier un pb en le compl.

ex : 2 mat. sont semblables s/ K si elles le sont sur L

justifie de se servir de la décomp. de Jordan

des poss.
- Loi de réciprocité quadr. av résultant ← original (H_2G_2, T2 !)
- Somme de Gauss (Jean-Pierre Serre, Cours d'arithmétique)

exple d'appli à l'arithm.
- $x^2 + y^2 = z^2$, premiers entre eux

$\mathbb{Z}[i]$: $(x+iy)(x-iy) = z^2$ or $(x+iy) \wedge (x-iy) = 1$

$\Rightarrow x + iy = (u+iv)^2 = u^2 - v^2 + 2iuv$

(Mary Lendrix)

⚠ Anneau et pas corps
un peu HS.

Props de plans

- I. Généralités
  II. Corps finis
  III. Nbres algébriques
  ↳ construc° à la règle et au compas
- I. Généralités
  II. Théorie de Galois
  III. Applica° + transverses
  ↳ exten° pr autoriser + de solu°
  ↳ matrices semblables
  ↳ Σ de Gauss
  ↳ critère de factorisa° (cf exo 1)

(II). Exercices

$\boxed{1}$ $m, n \geq 2$, $m \wedge n = 1$. $a \in \mathbb{Q}$

Mq $X^{mn} - a$ irr sr $\mathbb{Q}$ ssi $\begin{cases} X^m - a & \text{irr sr } \mathbb{Q} \\ X^n - a & \text{irr sr } \mathbb{Q} \end{cases}$

($\Rightarrow$) Soit z une $\sqrt{\ }$ de $X^{mn} - a$.

$[\mathbb{Q}[z] : \mathbb{Q}] = mn$ ← deg d'ext = deg du poly min de z = mn car $X^{mn} - a$ irr.

$[\mathbb{Q}[z^n] : \mathbb{Q}] \leq m$ ← z^n $\sqrt{\ }$ de $X^m - a$

$[\mathbb{Q}[z] : \mathbb{Q}[z^n]] \leq n$ ← z $\sqrt{\ }$ de $X^n - z^n$

Thm de la base télescopique ⇒ les 2 $\leq$ sont des $=$.

($\Leftarrow$) $[\mathbb{Q}[z] : \mathbb{Q}] = [\mathbb{Q}[z] : \mathbb{Q}[z^n]]\,[\mathbb{Q}[z^n] : \mathbb{Q}]$

$= k m$ (thm base télescopique)

$[\mathbb{Q}[z] : \mathbb{Q}] = [\mathbb{Q}[z] : \mathbb{Q}[z^m]]\,[\mathbb{Q}[z^m] : \mathbb{Q}]$

$= k' n$ (")

On a $\begin{cases} m \mid [\mathbb{Q}[\zeta_3] : \mathbb{Q}] \\ n \mid [\mathbb{Q}[\zeta_3] : \mathbb{Q}] \end{cases} \Rightarrow \text{ppcm}(m,n) = mn \mid [\mathbb{Q}[\zeta_3] : \mathbb{Q}]$

Et $[\mathbb{Q}[\zeta_3] : \mathbb{Q}] \leq mn$. Donc $=$té.

2) $[L:K] = m$. $P \in K[X]$ irr s/ K $\deg(P) = n$ $m \wedge n = d$

<u>Rq</u> il y a au plus d facteurs irr de P s/ L.
(ie $P = \prod_{i=1}^{r} P_i$ av $P_i \in L[X]$ irr et $r \leq d$).

(Cor : si $m \wedge n = 1$, P reste irréductible)

Soit α une $\sqrt{\ }$ de P_i. α est une $\sqrt{\ }$ de P. Dc :

$$\begin{tikzcd}
 & L[\alpha] \arrow[dl, dash, "\deg P_i \text{ car } P_i \text{ irr.}"'] \arrow[dr, dash] & \\
L \arrow[dr, dash, "m"'] & & K[\alpha] \arrow[dl, dash, "n \text{ car } P \text{ irr}"] \\
 & K &
\end{tikzcd}$$

Dc $n \mid m \deg(P_i) \Rightarrow \begin{cases} \frac{n}{d} \mid \frac{m}{d} \deg(P_i) \\ \frac{n}{d} \wedge \frac{m}{d} = 1 \end{cases} \underset{\text{Gauss}}{\Rightarrow} \frac{n}{d} \mid \deg P_i$

Valable pour $\forall i \rightarrow$ on somme : $\underbrace{\sum_{i=1}^{r} \frac{n}{d}}_{r \frac{n}{d}} = \sum_{i=1}^{r} \deg P_i = \deg P = n$

Donc $r \leq d$.

(<u>Rq</u> : Si l'extension est normale alors $r = d$).

3) $b, c \in \mathbb{Z}$, $\Delta = b^2 - 4c$ ne soit pas un carré mod p où p est un entier premier impair.

(g_n) : $\begin{cases} g_1 = 1 \\ g_2 = b \\ g_{n+2} = b\, g_{n+1} - c\, g_n \end{cases}$

Mq $\forall n$ tq $p+1 \mid n$ alors $p \mid g_n$.

$K = \mathbb{F}_p[\sqrt{\Delta}] = \mathbb{F}_{p^2}$ ← unicité des corps finis.

$X^2 - bX + c$ $\quad x_1 = \dfrac{b + \sqrt{\Delta}}{2}$ $\quad x_2 = \dfrac{b - \sqrt{\Delta}}{2}$

pr simplifier les calculs

$g_n = A x_1^{n-1} + B x_2^{n-1}$

$\begin{cases} g_1 = A + B = 1 \\ g_2 = A x_1 + B x_2 = b \end{cases} \Rightarrow \begin{cases} B = \dfrac{-x_2}{x_1 - x_2} \\ A = 1 + \dfrac{x_2}{x_1 - x_2} = \dfrac{x_1}{x_1 - x_2} \end{cases}$

$B(x_1 - x_2) = x_1 - b \overset{x_1 + x_2 = b}{=} -x_2$

$g_n = \dfrac{1}{x_1 - x_2} (x_1^n - x_2^n)$

On remarque que $x_1^p = x_2$. En effet $(X^2 - bX + c)^p = X^p - bX + c$ (Froebenius) et donc x_1^p $\sqrt{}$ du m poly et $x_1^p \neq x_1$ sinon on a $x_1^p \in \mathbb{F}_p$ ($\mathbb{F}_p$ est exactement $\{x, x^p = x\}$) donc $x_1^p = x_2$.

$p+1 \mid n \Rightarrow \underbrace{x_1^{p+1} - x_2^{p+1}}_{= 0} \mid x_1^n - x_2^n$ $\quad x_1^{p+1} = x_1 x_2$ $\quad x_2^{p+1} = x_1 x_2$

ie. $x_1^n - x_2^n = 0$ ds $\mathbb{F}_p$