TD2.2 : Extensions de corps

26/09/2023

Exercice 1 :

Soit $K \hookrightarrow L$ une extension algébrique de corps et $Q \in L[X]$ un polynôme irréductible. Montrer qu'il existe un poynôme irréductible $P \in K[X]$ tel que Q divise P dans $L[X]$.

Correction :

Soit L' un corps de rupture de Q sur L, et α une racine de Q dans L'. Alors α est algébrique sur K car α algébrique sur L et L/K algébrique. Alors le polynôme minimal de α sur K convient (car il annule α en tant que polynôme sur L donc est divisible par Q polynôme minimal de α sur L).

Exercice 2 : Extensions de degré 2

Soit L une extension d'un corps K de degré 2, de caractéristique différente de 2.

1. Montrer qu'il existe $a \in K$ tel que $L \simeq K[X]/(X^2 - a)$ (que l'on note par definition $K(\sqrt{a})$).

2. A quelle condition deux extensions de cette forme sont K-isomorphes ?

3. Décrire les K automorphismes de $K(\sqrt{a})$.

Correction :

1. Soit $x \in L\backslash K$. La famille $1, x$ est libre sur K donc $x^2 = bx + c$. En caractéristique différente de 2 , on obtient $(x + b/2)^2 = c + b^2/4$. En posant $a = c + b^2/4$ et en envoyant X sur $x + b/2$, on obtient un morphisme $K[X]/\left(X^2 - a\right) \to L$, qui est un isomorphisme car $1, x + b/2$ forment une base de L sur K.

2. Si $b \in K$ est un carré dans $K[X]/\left(X^2 - a\right)$, alors $b = (c + d\sqrt{a})^2$, et donc $2cd = 0$ et $b = c^2 + ad^2$. Donc soit b soit b/a est un carré dans k. Or si b est un carré $K[X]/\left(X^2 - b\right)$ n'est pas un corps. Donc $K[X]/\left(X^2 - a\right)$ et $K[X]/\left(X^2 - b\right)$ sont isomorphes si et seulement si b/a est un carré.

3. Notons y une racine de a dans L. Si σ est un automorphisme de L fixant K. On a $\sigma(y)^2 = \sigma\left(y^2\right) = \sigma(a) = a$ donc $\sigma(y)$ est y ou $-y$. Comme y engendre L, on obtient au plus deux automorphismes possibles. On vérifie facilement que $\sigma(e + fy) = e - fy$ définit bien un automorphisme

Exercice 3 : Une extension purement transcendante

Montrer que $k(x, \sqrt{1 - x^2})$ est purement transcendante.

Correction :

Si la caractéristique de k est 2, on a directement que $k(x, \sqrt{1 - x^2}) = k(x)$ car $(1+x)^2 = 1+x^2 = 1-x^2$.

Si maintenant la caractéristique de k n'est pas 2, on considère l'extension $k\left(\frac{\sqrt{1-x^2}}{1+x}\right)$. Cette extension contient alors

$$\frac{1 - \left(\frac{\sqrt{1-x^2}}{1+x}\right)^2}{1 + \left(\frac{\sqrt{1-x^2}}{1+x}\right)^2} = \frac{(1 + x)^2 - (1 - x^2)}{(1 + x)^2 + (1 - x^2)} = x$$

Et donc elle contient aussi $\sqrt{1 - x^2}$, et finalement $k(x, \sqrt{1 - x^2}) = k\left(\frac{\sqrt{1-x^2}}{1+x}\right)$ (et en regardant le degré de transcendance on voit que $\frac{\sqrt{1-x^2}}{1+x}$ est bien un élément transcendant, même si on aurait pu le montrer a la main.)

Exercice 4 :

On veut montrer dans cet exercice que si $F \subset K \subset L$ est une tour d'extensions de corps, alors il est équivalent que :

(i) K/F et L/K sont de type fini

(ii) L/F est de type fini.

1. Traiter les cas faciles et identifier la partie difficile.

2. On va avoir ensuite besoin de quelques résultats sur les extensions transcendantes :

a. Soit E/F et S une partie de E algébriquement indépendante sur F. Soit $\alpha \in E \backslash S$, alors $S \cup \{\alpha\}$ est algébriquement indépendante si et seulement si α est transcendant sur $F(S)$.

b. Une extension purement transcendante est totalement transcendante (c'est à dire que tout élément de $E \backslash F$ est transcendant).

3. Soit E/F une extension et $S \subset E$ une partie algébriquement indépendante sur F. Soit $A \subset E$ une extension algébrique de F.

a. Montrer que S est algébriquement indépendante sur A.

b. Montrer que A est l'ensemble des éléments de $A(S)$ algébriques sur F.

c. Montrer que $[E : F(S)] < \infty \Rightarrow [A : F] < \infty$.

4. Conclure la preuve du théorème.

Correction :

1. Si L/F est de type fini, $L = F(a_1, \ldots, a_n)$, alors L/K aussi car $L = K(a_1, \ldots, a_n)$.

Si les deux sont de type fini, $L = K(a_1, \ldots, a_n)$ et $K = F(b_1, \ldots, b_m)$, alors L/F aussi car $L = F(b_1, \ldots, b_m, a_1, \ldots, a_n)$. Il reste à montrer que L/F de type fini implique K/F de type fini.

2.

a. Voir le cours.

b. On suppose $E = F(\mathcal{X})$, avec $\mathcal{X}$ un ensemble algébriquement indépendent over F. Soit $\beta \in E$ algébrique sur F. L'objectif est de montrer que $\beta \in F$. Tout d'abord β est un quotient de deux polynômes en $\mathcal{X}$ à coefficients dans F, et donc est dans $F(\mathcal{X}_0)$, où $\mathcal{X}_0 \subset \mathcal{X}$ est fini. On peut donc supposer que $\mathcal{X}$ est fini, et on montre par récurrence sur $n = |\mathcal{X}|$ que $\beta \in F$.

Si $n = 0$, alors $E = F$ et la propriété est vraie.

Supposons $n > 0$, et soit $\alpha \in \mathcal{X}$. On note $\mathcal{X}' = \mathcal{X} - \{\alpha\}$ et $K = F(\mathcal{X}')$, de sorte que $E = K(\alpha)$ et que α soit transcendant sur K par la question 2.a. (car $\mathcal{X}' \cup \{\alpha\} = \mathcal{X}$ is independent over F.)

Alors $\beta \in E = K(\alpha)$ est algébrique sur K, et donc par l'exercice 4 de la feuille précédente, $\beta \in K = F(\mathcal{X}')$. L'hypothèse de récurrence permet alors de conclure que $\beta \in F$.

3.

a. On peut supposer que $|S| = n < \infty$ (car une relation algébrique ne ferait intervenir qu'un nombre fini d'éléments de S), et soit $m = \max\{|S'|, S' \subset S, S'$ algébriquement indépendant sur $A\}$. Alors d'une part $m = \mathrm{degtr}_A(A(S))$, et $\mathrm{degtr}_F(A(S)) = \underbrace{\mathrm{degtr}_F(A)}_{=0} + \mathrm{degtr}_A(A(S)) = m$.

D'autre part,

$$\mathrm{degtr}_F(A(S)) = \underbrace{\mathrm{degtr}_F(F(S))}_{=n} + \mathrm{degtr}_{F(S)}(A(\mathcal{S}))$$

On obtient alors $m \geqslant n$, mais par définition de m, $m \leqslant n$, et finalement $S' = S$ et on obtient que S est algébriquement indépendant sur A.

b. Par 3.a, $A(S)$ est purement transcendante, donc totalement transcendante par question 2.b. Alors si $\gamma \in A(S)$ est algébrique sur F, γ est aussi algébrique sur A et donc est dans A. L'autre inclusion fient du fait que A est algébrique sur F.

c. Nous allons montrer la contraposée. Si $|A : F| = \infty$, comme A est algébrique sur F, on a $A > F(\beta_1, \beta_2, \ldots, \beta_r)$ pour toute famille finie $\beta_1, \beta_2, \ldots, \beta_r$ d'élements de A.

On peut alors construire une suite strictement croissante $F = A_0 < A_1 < \cdots$ de sous-extensions de A/F, et en notant $L_i = A_i(S)$, On a $F(S) = L_0 \subseteq L_1 \subseteq \cdots$ et tous les L_i sont dans E. Or toutes ces inclusions sont en fait strictes : en effet par 3.b appliquée à A_i, on sait que $L_i \cap A = A_i$, donc $L_i = L_j$ implique $A_i = A_j$ et donc $i = j$.

On a donc une suite infinie strictement croissante de sous-extensions de $E/F(S)$, d'où $|E : F(S)| = \infty$.

4. Comme L est de type fini sur F, on a $\mathrm{degtr}_F(L) < \infty$, et donc $\mathrm{degtr}_F(E) < \infty$ car $\mathrm{degtr}_F(L) = \mathrm{degtr}_F(E) + \mathrm{degtr}_E(L)$. Soit S une base de transcendance (donc S fini) de E/F, et notons $K = F(S)$. Rappelons que l'on veut montrer que E/F est de type fini, il reste donc à montrer que E/K est de type fini. Or comme E/K est algébrique, cela revient à montrer que cette extension est finie.

Pour cela, soit $\mathcal{X}$ une base de transcendance de L sur K, alors comme $L/K(\mathcal{X})$ est algébrique et de type finie, elle est finie et $[L : K(\mathcal{X})] < \infty$. Mais la question 3.c s'applique dans ce cas et on obtient $[E : K] < \infty$, ce qui conclut.

Exercice 5 : Un contre-exemple

Soit $K = \mathbb{Q}(T)$, et deux sous corps $K_1 = \mathbb{Q}(T^2)$ et $K_2 = \mathbb{Q}(T^2 - T)$. Montrer que K est algébrique sur K_1 et K_2 mais pas sur $K_1 \cap K_2$.

Correction :

Comme T est racine des polynômes $X^2 - T^2 \in K_1(X)$ et $X^2 - X - T^2 + T \in K_2(X)$, le corps K est algébrique sur K_1 et K_2. Montrons que $K_1 \cap K_2 = \mathbb{Q}$. Soient $F_1 \in \mathbb{Q}(T)$ et $F_2 \in \mathbb{Q}(T)$ telles que $F_1\left(T^2 - T\right) = F_2\left(T^2\right) =: F$. Comme $F_1\left(T - T^2\right)$ est invariante par $T \mapsto 1 - T$ et $F_2\left(T^2\right)$ est invariante par $T \mapsto -T, F$ est invariante par $T \mapsto T + 1$. Mais alors, les zéros et les pôles de F dans $\overline{\mathbb{Q}}$ sont invariants par $t \mapsto t + 1$. Comme F ne peut avoir qu'un nombre fini de zéros et de pôles, on en déduit que F n'a pas zéros ni de pôles. Par conséquent, $F \in \mathbb{Q}$ et $K_1 \cap K_2 = \mathbb{Q}$.

Exercice 6 : Théorème de Lüroth

1. On admet le résultat suivant, que l'on verra plus tard dans le cours : Soit A un anneau factoriel ($K[X_i]_i$ est factoriel) de corps des fractions F. Si $f \in A[X]\backslash\{0\}$ s'écrit $f = gh$ avec g et h dans $F[X]$, alors il existe $g_0 = \alpha g \in A[X]$ et $h_0 = \beta h \in A[X]$ tel que $f = g_0 h_0$.

a. Soient $P, Q \in F[X]$ premiers entre eux et $U, V \in F[Y]$ premiers entre eux, et on suppose que U et V ne sont pas tous deux constants. Notons $f(X,Y) = U(Y)P(X) - V(Y)Q(X)$. Supposons que $f = gh$ avec $g \in F[X,Y]$ et $h \in F[X]$. Montrer que h est constant.

b. Soient $P, Q \in F[X]$ premiers entre eux et notons $d = \max(\deg P, \deg Q)$. Soit $E = F(\beta)$ où β est transcendant, et soit $f = p - \beta q \in E[X]$. Montrer que $\deg(f) = d$ et f est irréductible si $d > 0$.

2. On veut montrer le théorème de Lüroth : Soit $L = F(\alpha)$, avec α transcendant sur F. Soit E une extension intermédiaire $L/E/F$. Alors $E = F(\beta)$ pour un certain $\beta \in E$.

a. Soit $\beta \in E\backslash F$. Montrer que $d(\beta) \overset{\text{def}}{=} [L : F(\beta)] < \infty$, puis que $n \overset{\text{def}}{=} [L : E] < \infty$, puis conclure qu'il suffit de trouver un β tel que $d(\beta) = n$.

b. Soit $g = \min_E(\alpha)$. Quel est le degré de g, et est-ce que $g \in F[X]$?

c. Soit β un coefficient de g dans $E\backslash F$. Montrer que β convient. *On pourra partir de $q(\alpha)p(X) - p(\alpha)q(X) = g(X)h(X)$ dans $L[X]$, où $\beta = \frac{p(\alpha)}{q(\alpha)}$, puis remplacer α par Y, et enfin remarquer que le degré en Y du terme à gauche est d, alors que le degré en X du terme à droite est n.*