TD2 : Extensions de corps

25/09/2023

Exercice 1 : Corps de décomposition

Déterminer les corps de décompositon des polynôme suivants de $\mathbb{Q}[X]$, ainsi que leur dimension sur $\mathbb{Q}$:

— $X^2 - 3$.
— $X^3 - 2$
— $(X^3 - 2)(X^2 - 2)$
— $X^5 - 7$
— $X^4 + 4$.
— $X^6 + 3$.
— $X^8 + 16$.

Correction :

— Le corps de décomposition de $X^2 - 3$ est $\mathbb{Q}(\sqrt{3})$. Comme $\sqrt{3} \notin \mathbb{Q}$, $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$.
— Le corps de décomposition de $X^3 - 2$ est $\mathbb{Q}(\sqrt[3]{2}, \rho)$. Comme $X^3 - 2$ est irréductible sur $\mathbb{Q}$, on a $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. De plus, $\rho^2 + \rho + 1 = 0$, donc $[\mathbb{Q}(\sqrt[3]{2}, \rho) : \mathbb{Q}(\sqrt[3]{2})] \leqslant 2$. Mais $\rho \notin \mathbb{Q}(\sqrt[3]{2})$. Donc $[\mathbb{Q}(\sqrt[3]{2}, \rho) : \mathbb{Q}(\sqrt[3]{2})] = 2$ et $[\mathbb{Q}(\sqrt[3]{2}, \rho) : \mathbb{Q}] = 6$.
— Le corps de décomposition de $\left(X^3 - 2\right)\left(X^2 - 2\right)$ est $\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}, \rho) = \mathbb{Q}(\sqrt[6]{2}, \rho)$. En procéd ant comme dans le point précédent, on a $[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6$ et $[\mathbb{Q}(\sqrt[6]{2}, \rho) : \mathbb{Q}(\sqrt[6]{2})] = 2$. Donc $[\mathbb{Q}(\sqrt[6]{2}, \rho) : \mathbb{Q}] = 12$.
— Le corps de décomposition de $X^5 - 7$ est $\mathbb{Q}\left(\sqrt[5]{7}, \zeta_5\right)$ où ζ_5 est une racine primitive 5 -ième de l'unité. Le polynôme $X^5 - 7$ est irréductible par le critère d'Eisenstein. Donc $[\mathbb{Q}(\sqrt[5]{7}) : \mathbb{Q}] = 5$. Le polynôme $\phi_5 = X^4 + X^3 + X^2 + X + 1 \in \mathbb{Q}[X]$, qui annule ζ_5, est aussi irréductible (appliquer le critère d'Eisenstein à $\phi_5(X + 1)$). Donc $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$. On en déduit que $20 \mid \left[\mathbb{Q}\left(\sqrt[5]{7}, \zeta_5\right) : \mathbb{Q}\right]$. Mais $\left[\mathbb{Q}\left(\sqrt[5]{7}, \zeta_5\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt[5]{7}, \zeta_5\right) : \mathbb{Q}(\sqrt[5]{7})\right][\mathbb{Q}(\sqrt[5]{7}) : \mathbb{Q}] \leqslant 20$. Donc $\left[\mathbb{Q}\left(\sqrt[5]{7}, \zeta_5\right) : \mathbb{Q}\right] = 20$.
— Le corps de décomposition de $X^4 + 4$ est $\mathbb{Q}\left(\sqrt{2}\zeta_8, i\right) = \mathbb{Q}(i)$ où $\zeta_8 = e^{\frac{i\pi}{4}} = \sqrt{2}(1 + i)$. On a $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.
— Le corps de décomposition de $X^6 + 3$ est $\mathbb{Q}\left(i\sqrt[6]{3}, \zeta_6\right) = \mathbb{Q}(i\sqrt[6]{3})$ avec $\zeta_6 = e^{\frac{i\pi}{3}} = \frac{1+i\sqrt{3}}{2}$. Comme le polynôme $X^6 - 3$ est irréductible d'après le critère d'Eisenstein, $[\mathbb{Q}(i\sqrt[6]{3}) : \mathbb{Q}] = 6$.
— Le corps de décomposition de $X^8 + 16$ est $\mathbb{Q}\left(\zeta_{16}\sqrt{2}, \zeta_8\right) = \mathbb{Q}\left(\zeta_{16}\right)$ où $\zeta_8 = e^{\frac{i\pi}{4}} = \sqrt{2}(1 + i)$ et $\zeta_{16} = e^{\frac{i\pi}{8}}$. Le polynôme $\phi_8 = X^8 + 1$ annule ζ_{16} et est irréductible (appliquer le critère d'Eisenstein à $\phi_8(X + 1)$). Donc $[\mathbb{Q}\left(\zeta_{16}\right) : \mathbb{Q}] = 8$.

Exercice 2 :

Soit L/K une extension de corps et F_1, F_2 deux sous-extensions. On suppose que $[F_1 : K] \wedge [F_2 : K] = 1$. Montrer que $F_1 \cap F_2 = K$.

Correction :

Par multiplicité des degrés, $[F_1 \cap F_2 : K]$ divise $[F_1 : K]$ et $[F_2 : K]$, donc divise leur pgcd, c'est à dire 1, d'où $F_1 \cap F_2 = K$.

✉clement.chivet@ens.fr

Exercice 3 : Polynômes minimaux

Soient K un corps et L une extension finie de K. Soient x, y deux éléments de L, et P_x, P_y leurs polynômes minimaux respectifs sur K. Montrer que P_x est irréductible sur $K(y)$ si et seulement si P_y est irréductible sur $K(x)$.

Correction :

P_x est irréductibe sur $K(y)$ ssi $K(y)[X]/(P_x(X))$ est un corps ssi $K[X,Y]/(P_x(X), P_y(Y))$ est un corps, ssi $K(x)[Y]/(P_y(Y))$ est un corps, ssi P_y irréductible sur $K(x)$.

Exercice 4 :

Soit k un corps et $K = k(X)$ le corps des fractions rationnelles.

1. Soit $F \in K \backslash k$.

a. Montrer que X est algébrique sur $k(F)$.

b. En déduire que F est transcendant sur k.

c. Montrer que $[K : k(F)] = \max(\deg P, \deg Q)$ où $F = \frac{P}{Q}$ avec $P, Q \in k[X], P \wedge Q = 1$.

On pourra d'abord montrer le lemme suivant :

Lemme 0.1.

Soient $f, g \in K[t]$ premiers entre eux, et $m = \max(\deg f, \deg g)$, et $P_n \in K[t]$ des polynômes de degré strictement inférieur à m. Si il existe N tel que

$$\sum_{n=0}^{N} P_n f^n g^{N-n} = 0$$

Alors $P_n = 0$ pour tout $n \leqslant N$.

2. Soit $\phi : \mathrm{GL}_2(k) \to \mathrm{Aut}_k(K)$ le morphisme de groupe défini par

$$\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} : R \mapsto R\left(\frac{aX+b}{cX+d}\right)$$

Montrer que ϕ est surjectif et déterminer $\ker(\phi)$.

Correction :

1.

a. Notons $F = \frac{P}{Q}$ avec $P \wedge Q = 1$. Alors X est racine du polynôme $P(T) - FQ(T) \in k(F)[X]$. Ce polynôme est bien non nul, en effet c'est le polynôme $\sum_i (p_i - Fq_i)T^i$ et comme $F \notin k$, et que P et Q ne sont pas nuls, on trouve bien au moins un coefficient non nul.

b. Si F était algébrique sur k, alors $[k(F) : k] < \infty$. Puis par multiplicité des degrés ont aurait alors $[k(X) : k] = [k(X) : k(F)][k(F) : k] < \infty$, ce qui est absurde. D'où F est transcendant.

c. Prouvons le lemme : on peut supposer $\deg(g) = m$. Alors g divise $\sum_{n=0}^{N-1} P_n f^n g^{N-n}$, et donc divise aussi $P_N f^N$. Comme $f \wedge g = 1$, g divise P_N qui est de degré $< m = \deg g$, donc est nul. Alors $\sum_{n=0}^{N-1} P_n f^n g^{(N-1)-n} = 0$ et une récurrence finie termine la preuve du lemme.

Soit $F = \frac{P(X)}{Q(X)}$ comme dans la question. On veut montrer que le polynôme minimal de X sur $K(F)$ est de degré $m = \max(\deg P, \deg Q)$. Soit $R(T) \in k(F)[T]$, tel que $R(X) = 0$. On écrit $R(T) = \sum_{k=0}^{r} a_k T^k$, avec $a_k \in K(F)$ et on suppose par l'absurde que $r < m$. On peut écrire chaque $a_k = \frac{P_k(F)}{Q_k(F)}$, avec $P_k, Q_k \in k[Y]$. L'égalité $R(X) = 0$ s'écrit alors

$$\sum_{k=0}^{r} \frac{P_k(F)}{Q_k(F)} X^k = 0.$$

Soit en mettant au même dénominateur :

$$\sum_{k=0}^{r} \underbrace{P_k(F) \prod_{k' \neq k} Q_{k'}(F)}_{=:\widetilde{P_k(F)}} X^k = 0$$

qui devient alors

$$\sum_{k=0}^{r} \widetilde{P_k(F)} X^k = 0,$$

avec $\widetilde{P_k}(T) =: \sum_l a_{kl} T^l \in k[T]$.

Alors en replacant par la définition de F :

$$\sum_{k=0}^{r} \sum_{l} a_{kl} \frac{P(X)^l}{Q(X)^l} X^k = 0.$$

et en multipliant par $Q(X)^L$ avec L assez grand (les sommes sont des sommes finies) on obtient :

$$\sum_{k=0}^{r} \sum_{l} a_{kl} P(X)^l Q(X)^{L-l} X^k = 0,$$

Ce qui donne en inversant la sommation

$$\sum_{l} (\sum_{k=0}^{r} a_{kl} X^k) P(X)^l Q(X)^{L-l} = 0.$$

> Par le Lemme, on déduit que tous les a_{kl} sont nuls, donc $\widetilde{P_k}$ aussi et finalement les a_k sont nuls (car les Q_k sont non nuls). Finalement, $R = 0$, ce qui conclut.

Remarque 2. En utilisant le Lemme de Gauss (dernier exercice de la feuille), on peut aller plus vite : le polynome $R(T) = P(T) - F(X)Q(T) \in k(F)[T]$ peut être vu comme un polynôme de $k[F][T]$. De plus $k[F]$ et $k[T]$ sont principaux, le premier car F est transcendant donc isomorphe au deuxième, et le deuxième par le cours (futur ?). Or comme polynôme en F à coefficient dans $k[T]$, il est irréductible dans $k(T)[F]$ car de degré 1, et est primitif car $P \wedge Q = 1$, donc est irréductible sur $k[T][F] = k[F][T]$, et donc est irréductible sur $k(F)[T]$.

2. Soit $\phi \in \mathrm{Aut}_k(K)$, et $F = \phi(X)$. Alors pour tout $R \in k(X)$, on remarque que $\phi(R) = R(F)$. L'image de ϕ est donc $k(F)$, ce qui force F à être de la forme $\frac{P}{Q}$ avec $\max\{\deg P, \deg Q\} = 1$ par la question précédente, et comme $P = aX + b$ et $Q = bX + d$ doivent être premiers entre eux, on voit que (a, b) et (c, d) ne sont pas colinéaires, ce qui montre la surjectivité. ϕ sera dans le noyau ssi elle envoie X sur X c'est à dire encore ssi elle correspond à λId.

Exercice 5 :

1. Est-ce que l'extension $\mathbb{Q}(\sqrt{2}, \pi)/\mathbb{Q}$ est purement transcendante ?
2. Est-ce que l'extension $\mathbb{R}(X, Y)/\mathbb{R}(X + Y)$ est purement transcendante ?

Correction :

1. le degré de transcendance de cette extension est 1, car $\mathbb{Q}(\sqrt{2}, \pi)/\mathbb{Q}(\pi)$ est algébrique (et on suppose que l'on sait que π est transcendant). Si par l'absurde cette extension était purement transcendante,

alors on aurait $\mathbb{Q}(\sqrt{2},\pi) \simeq \mathbb{Q}(Y)$. Or l'extension de droite n'a pas de racine de 2, en effet si un tel $\mathbb{Q}$-isomorphisme existait, l'image $\frac{P(Y)}{Q(Y)}$ de $\sqrt{2}$ vérifierai

$$\left(\frac{P(Y)}{Q(Y)}\right)^2 = 2$$

soit encore

$$P(Y)^2 = 2Q(Y)^2$$

ce qui par exemple en prenant le coefficient dominant q_n de Q donne $p_n^2 = 2q_n^2$, absurde.

2. Par additivité du degré de transcendance, on a que le degré de cette extension est 1. Or $\mathbb{R}(X,Y) = \mathbb{R}(X+Y)(Y)$, donc Y ne peut pas être algébrique par définition du degré de transcendance (le fait que ce soit le cardinal de n'importe quelle base de transcendance, si Y était algébrique $\varnothing$ serait une base de transcendance de $\mathbb{R}(X,Y)/\mathbb{R}(X+Y)\ldots$). On a donc bien une extension purement transcendante.

Exercice 6 : Degré du corps de décomposition

Soient K un corps, $P \in K[X]$ un polynôme de degré $n \geqslant 1$ et L un corps de décomposition de P sur K. Montrer que $[L:K]$ divise $n!$.

Correction :

Cours

Exercice 7 : 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 $K_1 \cap K_2$.

Exercice 8 : Extensions de degré 2

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

1. On suppose que la caractéristique de K n'est pas 2. 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 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.

Exercice 9 : Une extension purement transcendante

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

Correction :

Exercice 10 : Un exemple

Soit $K = \mathbb{Q}(\sqrt[3]{2}, j)$ où $j = e^{2i\pi/3}$.

1. Déterminer $[K:\mathbb{Q}]$, et exprimer K comme corps de décomposition d'un polynôme bien choisi.

2. Déterminer tous les sous-corps de K ainsi que leur degré.

Correction :

1. Comme $[\mathbb{Q}(j):\mathbb{Q}]=2$ et $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3]$ on a $[K:\mathbb{Q}]=6$. Si $P=X^3-2$ alors K contient un corps de décomposition de P. Comme les racines de P sont $\sqrt[3]{2}, j\sqrt[3]{2}$ et $j^2\sqrt[3]{2}$ un corps de décomposition de P contient toujours $\sqrt[3]{2}$ et $j=\frac{j\sqrt[3]{2}}{\sqrt[3]{2}}$ donc K est un corps de décomposition de P.

2. Un sous corps de K est de degré $1,2,3$ ou 6. Les cas 6 et 1, sont triviaux. On montre que si L est un sous corps de K de degré 3 alors $L=\mathbb{Q}(j^i\sqrt[3]{2})$ pour un $i=0,1,2$ et que si L est de degré 2 alors $L=\mathbb{Q}(j)$.

On regarde les automorphismes de K, ils sont déterminés sur j et $\sqrt[3]{2}$ et donc il ne peut avoir qu'au plus 6. Il y en a exactement 6 et le groupe des automorphismes de K est isomorphe à S_3 le groupe de permutation de trois éléments, agissant sur $\{\sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}\}$ le 3-cycle correspond à la multiplication par j et la transposition est engendrée par $j\mapsto j^2$.

Supposons tout d'abord que $[L:\mathbb{Q}]=2$ alors comme dans l'exercice 2, on a $L=\mathbb{Q}(\alpha)$ avec $\alpha^2\in\mathbb{Q}$. Et on a donc un automorphisme $c_\alpha: L\to L, \alpha\mapsto-\alpha$, de plus on a $K=L(\sqrt[3]{2})$. La composée $L\xrightarrow{c_\alpha} L\to K$ s'étend en un morphisme $K\to K$ (cela revient à choisir une racine cubique de 2 et on en a déjà choisi une dans la définition de K). On obtient donc un automorphisme de K, celui-ci est d'ordre 2. Pour conclure il suffit de montrer que L est invariant par le 3-cycle, supposons que ce n'est pas le cas. Notons $\tau: K\to K$ le 3-cycle, si $\tau(L)\neq L$ alors $\tau(L)=\mathbb{Q}[\tau(\alpha)]$ et comme précédemment on construit un automorphisme de K qui est déterminé par $\tau(\alpha)\mapsto-\tau(\alpha)$. On obtient alors trois automorphismes et on peut prescrire que chacun d'entre eux envoie $\sqrt[3]{2}$ sur lui même. Alors ces trois automorphismes sont égaux et donc c_α commute à l'action de τ ce qui est impossible dans S_3.

Supposons dans un deuxième cas que $[L:\mathbb{Q}]=3$ alors $[K:L]=2$ et on a un automorphisme L-linéaire de K d'ordre 2 et L s'identifie au points fixes de K sous cet automorphisme. Avec la connaissances du groupe des automorphismes et de leurs points fixes on gagne.

Exercice 11 : Critères d'irréductiblité

1. (Eisenstein) Soit $P=\sum_{i=0}^n a_iX^i$ à coefficients entiers. Supposons qu'il existe un nombre premier p tel que $p|a_i$ pour $i\leqslant n-1$, p ne divise pas a_n et p^2 ne divise pas a_0. Alors P est irréductible sur $\mathbb{Q}$.

2. (Lemme de Gauss) Pour P un polynôme, on note $c(P)$ le pgcd de ses coefficients. On dit que P est primitif si $c(P)=1$.

Soit A un anneau factoriel, et K son corps des fractions. Les éléments irréductibles de $A[X]$ sont les éléments premiers de A et les polynôme primitifs irréductibles sur $K[X]$.