

TD6 : EXTENSIONS DE CORPS ; CORPS FINIS

Diego Izquierdo

Les exercices 3, 7, 9 et 11 sont à préparer avant le TD. Pendant la séance de TD, les exercices seront traités dans l'ordre suivant : 3, 7, 9, 11, 13, 25.

Exercice 1 : Partiel 2012

Soit K un corps. Soit L une extension algébrique de K contenue dans $K(X)$. Montrer que $L = K$.

Exercice 2 : Fractions rationnelles telles que $F(x) = F\left(\frac{1}{x}\right)$

Soit K un corps. Soit $L = \{F \in K(x) \mid F(x) = F\left(\frac{1}{x}\right)\}$. Montrer que $K(y) \rightarrow L, F(y) \mapsto F\left(x + \frac{1}{x}\right)$ est un K -isomorphisme de corps. C'est ce résultat qui explique par exemple pourquoi, pour résoudre les équations de la forme $\sum_{k=0}^6 a_k x^k = 0$ avec $a_k = a_{6-k}$ pour chaque k , il suffit de savoir résoudre les équations de degré 3.

Exercice 3 (à préparer) : 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 $K(x)$.

Exercice 4 : Partiel 2012

Soit L/K une extension de corps algébrique de corps. Soit $P \in L[X]$. Montrer qu'il existe $Q \in K[X]$ divisible par P dans $L[X]$.

Exercice 5 : Irréductibilité de polynômes et extension de scalaires

Soient K un corps et P un polynôme irréductible de degré n sur K . Soit L une extension finie de K de degré premier à n . Montrer que P est irréductible sur L .

Exercice 6 : Un contre-exemple

Soient $K = \mathbb{Q}(T)$ et ses 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 7 (à préparer) : Corps de décomposition

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

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

Exercice 8 : Sous-corps de $K = \mathbb{Q}(2^{1/3}, \rho)$

Soient $\rho = e^{2i\pi/3} \in \mathbb{C}$ et $K = \mathbb{Q}(2^{1/3}, \rho)$.

1. Déterminer le degré de K sur \mathbb{Q} , et exprimer K comme le corps de décomposition d'un polynôme bien choisi.
2. Déterminer tous les sous-corps de K ainsi que leur degré.

Exercice 9 (à préparer) : Partiel 2011

Soit K un corps de caractéristique $p > 0$. Soit $a \in K$. Considérons le polynôme $P = X^p - X - a$. Soit L un corps de décomposition.

1. Soit $x \in L$ une racine de P . Montrer que les racines de P sont $x, x + 1, \dots, x + p - 1$.
2. Montrer que P est soit scindé soit irréductible.
3. Montrer que, si P n'a pas de racines dans K , alors $[L : K] = p$.

Exercice 10 : Degré du corps de décomposition d'un polynôme de degré 3

Soit K un corps. Considérons P un polynôme de degré 3 sur K et L son corps de décomposition.

1. Montrer que $[L : K] \in \{1, 2, 3, 6\}$.
2. Montrer que P est irréductible si, et seulement si, $[L : K] \in \{3, 6\}$.
3. Supposons P irréductible. Soit Δ son discriminant. Montrer que $[L : K] = 3$ si, et seulement si, Δ est un carré dans K .
4. Calculer $[L : K]$ dans les cas suivants :
 - (a) $K = \mathbb{Q}$, $P = X^3 - 3X^2 - 6X - 20$;
 - (b) $K = \mathbb{Q}$, $P = X^3 + 3X^2 - 3X - 4$;
 - (c) $K = \mathbb{Q}(i)$, $P = X^3 - 6iX^2 - 9X + 3i$;
 - (d) $K = \mathbb{R}(T)$, $P = X^3 + (T^2 - 1)X + T^3 - 1$.

Exercice 11 (à préparer) : Extensions de degré 2

Soient K un corps et L/K une extension de degré 2. On suppose la caractéristique de K différente de 2.

1. Montrer qu'il existe $x \in L \setminus K$ tel que l'on ait $L = K(x)$ et $x^2 \in K$.
2. Montrer alors l'égalité $L^{\times 2} \cap K^{\times} = K^{\times 2} \sqcup x^2 K^{\times 2}$.
3. Soient $y, z \in K^{\times}$. Montrer que $K(\sqrt{y})$ et $K(\sqrt{z})$ sont isomorphes en tant que K -algèbres si et seulement si zy^{-1} est un carré dans K .

Exercice 12 : Extensions de degré 2 en caractéristique 2

Soient K un corps et L/K une extension de degré 2. On suppose que caractéristique de K est égale à 2.

1. Supposons que L n'est pas de la forme $K(x)$ avec $x^2 \in K$. Montrer

qu'il existe $z \in L$ tel que l'on ait $L = K(z)$ et $z^2 - z \in K$.

2. En déduire une classification des extensions de degré 2 de K à isomorphisme de K -algèbres près.

Exercice 13 : Extensions engendrées par deux racines carrées

Soient K un corps de caractéristique différente de 2. Soient $x, y \in K^\times$.

1. Montrer que l'extension $K(\sqrt{x}, \sqrt{y})$ de K est de degré 4 si et seulement si on a $x, y, xy \in K^\times \setminus K^{\times 2}$.
2. Dans ce cas, montrer que les seuls corps intermédiaires entre K et $K(\sqrt{x}, \sqrt{y})$ sont $K, K(\sqrt{x}), K(\sqrt{y}), K(\sqrt{xy})$ et $K(\sqrt{x}, \sqrt{y})$.

Exercice 14 : Partiel 2014

Soit K un corps de caractéristique différente de 2. Soient $a, b \in K^\times$, avec $b \notin K^{\times 2}$. Soient $K_1 = K(\sqrt{b})$ et $L = K(\alpha)$ avec $\alpha^2 = a + \sqrt{b}$. On rappelle (exercice 11) que $K^\times \cap K_1^{\times 2} = K^{\times 2} \sqcup bK^{\times 2}$.

1. Montrer que $L = K_1$ si, et seulement si, il existe $d \in K^\times$ tel que $a^2 - b = d^2$ et $2(a + d) \in K^{\times 2}$.
2. Montrer qu'il existe $\beta \in L^\times$ tel que $\beta^2 = a - \sqrt{b}$ si, et seulement si, $a^2 - b \in K^{\times 2} \sqcup bK^{\times 2}$.
3. Calculer $K^\times \cap L^{\times 2}$.
4. Montrer qu'il existe $c \in K^\times$ tel que $L = K(\sqrt{b}, \sqrt{c})$ si, et seulement si, $a^2 - b \in K^{\times 2}$.

Exercice 15 : Sommes de carrés

Soit $\alpha \in \mathbb{C}$ tel que $\alpha^2 = 1 + \rho\sqrt[3]{2}$.

1. Montrer que le corps $\mathbb{Q}(\alpha)$ est une extension de degré 6 de \mathbb{Q} .
2. Dans $\mathbb{Q}(\alpha)$, le nombre -1 est-il une somme de carrés ?

Exercice 16 : Penser à utiliser la trace !

Le nombre $\sqrt[3]{2}$ est-il dans $\mathbb{Q}(\sqrt[3]{3})$?

Exercice 17 : Est-il un carré ?

Le nombre $1 + \sqrt[3]{2}$ est-il un carré dans $\mathbb{Q}(\sqrt[3]{2})$?

Exercice 18 : Groupe additif d'un corps fini

Soient $n \in \mathbb{N}^*$ et p un nombre premier. Quel est le groupe additif $(\mathbb{F}_{p^n}, +)$?

Exercice 19 : Intersections de corps finis

Soient p un nombre premier et n, s, t trois entiers avec $s|n$ et $t|n$. Soient K et L les sous-corps de \mathbb{F}_{p^n} de cardinaux respectifs p^s et p^t . Quel est le cardinal de $K \cap L$?

Exercice 20 : Un isomorphisme

Montrer que les anneaux $\mathbb{F}_3[X]/(X^2 + X + 2)$ et $\mathbb{F}_3[X]/(X^2 + 2X + 2)$ sont isomorphes. Exhiber un isomorphisme explicite.

Exercice 21 : Rattrapage 2014

Pour tout entier $n > 0$, on note P_n l'ensemble des polynômes irréductibles de degré n à coefficients dans \mathbb{F}_2 .

1. Montrer que $\prod_{f \in P_4} f = \frac{X^{16} - X}{X^4 - X} \in \mathbb{F}_2[X]$.
2. Expliciter tous les éléments de P_4 .
3. Déterminer $|P_6|$.

Exercice 22 : Dénombrement de polynômes irréductibles

On définit la fonction $\mu : \mathbb{N}^* \rightarrow \{-1, 0, 1\}$ par $\mu(1) = 1$, $\mu(p_1 \dots p_r) = (-1)^r$ si p_1, \dots, p_r sont des nombres premiers distincts et $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier.

1. Soient f et g deux fonctions de \mathbb{N}^* vers \mathbb{C} telles que :

$$\forall n \in \mathbb{N}^*, g(n) = \sum_{d|n} f(d).$$

Montrer la formule d'inversion de Möbius :

$$\forall n \in \mathbb{N}^*, f(n) = \sum_{d|n} g(d) \mu\left(\frac{n}{d}\right).$$

2. Soient $m \in \mathbb{N}^*$ et $q \in \mathbb{N}^*$ une puissance d'un nombre premier. Déduire de la question précédente une formule explicite pour le nombre de polynômes irréductibles de degré m à coefficients dans \mathbb{F}_q .

Exercice 23 : Partiel 2013

Soient p et q deux nombres premiers distincts, avec p impair. Soit K un corps de décomposition du polynôme séparable $X^p - 1 \in \mathbb{F}_q[X]$ et soit ω une racine primitive p -ième de l'unité dans K . Pour toute partie Z de $\mathbb{Z}/p\mathbb{Z}$, on pose $P_Z(X) = \prod_{i \in Z} (X - \omega^i) \in K[X]$. Pour tout entier r premier à p , on note aussi $rZ \subseteq \mathbb{Z}/p\mathbb{Z}$ l'image de Z par la bijection $z \mapsto rz$ de $\mathbb{Z}/p\mathbb{Z}$.

1. Montrer que $P_Z \in \mathbb{F}_q[X]$ si, et seulement si, $qZ = Z$.
2. Quels sont les degrés des facteurs irréductibles de $X^7 - 1$ dans $\mathbb{F}_2[X]$? Dans $\mathbb{F}_3[X]$? De $X^{17} - 1$ dans $\mathbb{F}_2[X]$?

On pose $Z_p^+ = \{x \in (\mathbb{Z}/p\mathbb{Z})^\times \mid \exists y \in (\mathbb{Z}/p\mathbb{Z})^\times, x = y^2\}$ et $Z_p^- = (\mathbb{Z}/p\mathbb{Z})^\times \setminus Z_p^+$ et on suppose à partir de maintenant que la classe de q modulo p est dans Z_p^+ .

3. Quels sont les cardinaux de Z_p^+ et Z_p^- ?
 4. Montrer que $P_{Z_p^\pm} \in \mathbb{F}_q[X]$. En déduire que le polynôme cyclotomique $\phi_p = \frac{X^p-1}{X-1}$ n'est pas irréductible dans $\mathbb{F}_q[X]$.
- On suppose à partir de maintenant $q = 2$ et p tel que $2 \in Z_p^+$.
5. On pose $Q^\pm = \sum_{i \in Z_p^\pm} X^i \in \mathbb{F}_2[X]$. Calculer $Q^+(X)^2$ et en déduire $\{Q^+(\omega), Q^-(\omega)\} = \{0, 1\}$.
- On suppose à partir de maintenant $Q^+(\omega) = 0$ et $Q^-(\omega) = 1$, ce qu'on peut toujours faire quitte à changer de racine primitive ω .
6. Montrer que $P_{Z_p^\pm} = \phi_p \wedge Q^\pm$.
 7. Décomposer le polynôme $X^7 - 1$ en produit de facteurs irréductibles dans $\mathbb{F}_2[X]$. Même question avec le polynôme $X^{17} - 1$.

Exercice 24 : Quand 5 est un carré modulo p ?

Soit p un nombre premier différent de 5. Soit L un corps de décomposition du polynôme $\phi_5 = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_p[X]$.

1. Montrer que L est engendré par une racine de ϕ_5 .
2. Montrer que $[L : \mathbb{F}_p]$ est égal à 1 si $p \equiv 1 \pmod{5}$, 2 si $p \equiv -1 \pmod{5}$, 4 si $p \equiv \pm 2 \pmod{5}$.
3. Soient $\zeta \in L$ une racine de ϕ_5 et $\beta = \zeta + \zeta^{-1}$. Montrer que $(2\beta + 1)^2 = 5$.
4. Déduire des questions précédentes que 5 est un carré dans \mathbb{F}_p si, et seulement si, $p \equiv \pm 1 \pmod{5}$.

Exercice 25 : Polynômes de la forme $X^{p^k} - X - a$

Soient F un corps de caractéristique $p > 0$ et $k \geq 1$ un entier. On rappelle que, pour tout $a \in F$, le polynôme $X^p - X - a$ est soit irréductible, soit scindé sur F (exercice 9).

1. Soit $x \in F$ tel que $x^{p^k} - x \in \mathbb{F}_p$. Montrer que F contient un sous-corps contenant x isomorphe à un sous-corps de $\mathbb{F}_{p^{kp}}$.
2. Soient $a \in \mathbb{F}_p$ et $P = X^{p^k} - X - a$. Montrer que, si P est irréductible, alors $p^k | pk$. En déduire pour quelles valeurs de p , k et a le polynôme P est irréductible.
3. Supposons que $k > 1$ et soit $a \in \mathbb{F}_{p^k}$. Montrer que le polynôme $X^{p^k} - X - a \in \mathbb{F}_{p^k}[X]$ n'est pas irréductible.

Exercice 26 : Théorème de Chevalley-Warning

Soit $P \in \mathbb{F}_q[X_1, \dots, X_n]$ homogène de degré d avec $0 < d < n$. Soit $V = \{(x_1, \dots, x_n) \in \mathbb{F}_q^n | P(x_1, \dots, x_n) = 0\}$.

1. Soient $Q = 1 - P^{q-1} \in \mathbb{F}_q$ et $S = \sum_{x \in \mathbb{F}_q^n} Q(x)$. Montrer que $S = |V|$ dans \mathbb{F}_q .
2. Montrer que $S = 0$.

3. Dédurre de ce qui précède que P admet un zéro non trivial dans \mathbb{F}_q^n .
4. Par contre, il existe un polynôme $P \in \mathbb{F}_q[X_1, \dots, X_n]$ homogène de degré n dont l'unique zéro dans \mathbb{F}_q^n est $(0, \dots, 0)$. Pouvez-vous exhiber un tel polynôme ? Vous pourrez vous aider de la fonction norme $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}$.

Exercice 27 : Clôture algébrique d'un corps fini

Soit p un nombre premier. Montrer que $\bigcup_{n=0}^{\infty} \mathbb{F}_{p^{n!}}$ est une clôture algébrique de \mathbb{F}_p .