Université Bordeaux
Mathématiques

L3, Structures algébriques 2
Année 2016 – 2017

FEUILLE D'EXERCICES n° 9

Extensions de corps

Exercice 1 – [Une extension biquadratique]

1) Que vaut $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}]$? Donner une base de $\mathbb{Q}(\sqrt{2},\sqrt{3})$ vu comme $\mathbb{Q}$-espace vectoriel.

2) Quel est le polynôme minimal de $\sqrt{2}+\sqrt{3}$ sur $\mathbb{Q}$?

3) En déduire que $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Exercice 2 – [Ses sous-extensions]

Soient K un corps de caractéristique différente de 2 et $P(X) \in K[X]$ unitaire de degré 2. Soit L/K une extension de degré 2.

1) Montrer qu'il existe $a, b \in K$ tels que $P(X) = (X-a)^2 - b$.

2) Montrer qu'il existe $x \in L \setminus \{0\}$ tel que $x^2 \in K$ et $L = K(x)$.

3) Soit $y \in L$ tel que $y^2 \in K$ et $L = K(y)$. Montrer que $y/x \in K$.

4) Soient p et q deux nombres premiers distincts. Que vaut $[\mathbb{Q}(\sqrt{p},\sqrt{q}) : \mathbb{Q}]$?

5) Soit $z \in \mathbb{Q}(\sqrt{p},\sqrt{q})$ tel que $z^2 \in \mathbb{Q}$. Montrer que l'un des quatre éléments suivants appartient à $\mathbb{Q}$: z, $z/\sqrt{p}$, $z/\sqrt{q}$, $z/\sqrt{pq}$.

6) En déduire la liste des extensions de $\mathbb{Q}$ incluses dans $\mathbb{Q}(\sqrt{p},\sqrt{q})$.

7) Quelles sont les extensions de $\mathbb{Q}$ incluses dans $\mathbb{Q}(\sqrt{2}+\sqrt{3})$?

Exercice 3 – [Un calcul d'inverse]

Soit a une racine de X^3+X+1 dans $\mathbb{C}$. Quel est le degré d de l'extension $\mathbb{Q}(a)/\mathbb{Q}$? Soit $b = a^5 + a^2 + 1$. Montrer que b est non nul et exprimer son inverse sous la forme $b^{-1} = P(a)$, où $P(X) \in \mathbb{Q}[X]$ est de degré au plus $d-1$.

Exercice 4 – Soient une extension L/K et un polynôme $P(X) \in K[X]$ de degré n, irréductible sur K. Montrer que si $[L : K]$ et n sont premiers entre eux, $P(X)$ est irréductible sur L.

Exercice 5 – Montrer que l'ensemble des nombres réels algébriques est dénombrable. En déduire que les nombres transcendants forment une partie non dénombrable de $\mathbb{R}$.

Exercice 6 – [Trisection d'angle]

Montrer que l'on ne peut pas diviser en trois un angle dans un triangle équilatéral à la règle et au compas.

Exercice 7 – [Polynômes cyclotomiques]

1) Exprimer dans $\mathbb{Z}[X]$ les polynômes cyclotomiques $\Phi_8(X)$ et $\Phi_{12}(X)$.

2) Soient $n \in \mathbb{N} \setminus \{0\}$ et p un nombre premier qui ne divise pas n. Montrer que $\Phi_{pn}(X)\Phi_n(X) = \Phi_n(X^p)$.

3) Soit $n \in \mathbb{N} \setminus \{0, 1\}$ et m le produit des facteurs premiers de n. Montrer que $\Phi_n(X) = \Phi_m(X^{\frac{n}{m}})$.

4) Exprimer dans $\mathbb{Z}[X]$ les polynômes cyclotomiques $\Phi_{15}(X)$, $\Phi_{36}(X)$ et $\Phi_{60}(X)$.

Exercice 8 – [$\cos \frac{2\pi}{n}$]

1) Soit $n \in \mathbb{N} \setminus \{0\}$. Montrer que $x_n = \cos \frac{2\pi}{n}$ est algébrique sur $\mathbb{Q}$ et déterminer le degré de $\mathbb{Q}(x_n)/\mathbb{Q}$.

2) Quel est le polynôme minimal de x_n si n est premier ? Quel est son polynôme minimal dans les cas où $n = 10, 12$ et 15 ?

Exercice 9 – [Deux exemples de corps de décomposition]

1) Soit α le réel $\sqrt{1 + \sqrt{7}}$. Trouver le polynôme minimal $P(X)$ de α sur $\mathbb{Q}$. Que vaut $[\mathbb{Q}(\alpha) : \mathbb{Q}]$?

2) Montrer que $K = \mathbb{Q}(\alpha, i\sqrt{6})$ est le corps de décomposition de $P(X)$ sur $\mathbb{Q}$ inclus dans $\mathbb{C}$.

3) Déterminer le degré et une base de K sur $\mathbb{Q}$.

4) Soit $\beta = \sqrt{3 + \sqrt{5}}$. Déterminer le corps de décomposition inclus dans $\mathbb{C}$ du polynôme minimal de β.

Exercice 10 – [Un corps de cardinal 16]

Soit $P(X) = X^4 + X^3 + 1 \in \mathbb{F}_2[X]$.

1) Montrer que $K = \mathbb{F}_2[X]/\langle P(X)\rangle$ est un corps commutatif à 16 éléments.

2) Soit a la classe de X modulo $P(X)$. Quel est l'ordre de a dans le groupe multiplicatif $K^\times$? Donner sans calculs les générateurs de $K^\times$ en fonction de a.

3) Trouver un élément d'ordre 3 dans $K^\times$. En déduire le sous-ensemble de K qui forme un sous-corps k à 4 éléments. Le corps K contient-il un sous-corps de cardinal 8 ou 6 ?

4) Quelles sont les autres racines de $X^4 + X^3 + 1$ dans K ? Calculer le polynôme minimal sur $\mathbb{F}_2$ de tous les éléments de K. Déterminer le polynôme minimal de a sur k (penser à utiliser l'automorphisme de Frobenius).

5) Pour chaque polynôme irréductible $Q(X) \in \mathbb{F}_2[X]$ de degré 4, trouver une racine de $Q(X)$ dans K et en déduire un isomorphisme de corps explicite entre $\mathbb{F}_2[X]/\langle Q(X)\rangle$ et K.

6) Quelle est la factorisation de $X^{16} - X$ en produit d'irréductibles dans $\mathbb{F}_2[X]$?

Exercice 11 – [Le critère de réduction pour l'irréductibilité dans $\mathbb{Q}[X]$ n'a pas de réciproque]

1) Soient K un corps commutatif et $P(X)$ un polynôme non constant de $K[X]$. Montrer que $P(X)$ est irréductible dans $K[X]$ si et seulement si $P(X)$ n'a de racine dans aucune extension de K de degré inférieur ou égal à $\dfrac{\deg P(X)}{2}$.

2) Montrer que X^4+1 est irréductible dans $\mathbb{Q}[X]$, mais réductible sur tout corps fini.

Exercice 12 – [Le symbole de Legendre en 2]

1) Soient p un nombre premier impair et K un corps de décomposition sur $\mathbb{F}_p$ de $P(X) = X^4 + \overline{1}$. Soit α une racine de $P(X)$ dans K. Montrer que $(\alpha+\alpha^{-1})^2 = \overline{2}$.

2) En déduire que 2 est un carré dans $\mathbb{F}_p$ si et seulement si $p \equiv \pm 1 \mod 8$.

3) Déterminer $\left(\dfrac{42}{59}\right)$.

4) Quels sont les nombres premiers p qui sont irréductibles dans $\mathbb{Z}[i\sqrt{2}]$?