Université Claude Bernard - Lyon 1 Semestre de printemps 2019-2020

MG1 - Algèbre commutative

Fiche de TD no 1

Exercice 1. 1. Soit $\mathbb{K}$ et $\mathbb{L}$ deux corps tels que $\mathbb{K} \subset \mathbb{L}$. Soit $P_1, P_2 \in \mathbb{K}[X]$.
Montrer que le pgcd de P_1 et P_2 dans $\mathbb{L}[X]$ est le même que leur pgcd dans $\mathbb{K}[X]$.
En déduire que les polynômes P_1 et $P_2 \in \mathbb{K}[X]$ sont premiers entre eux si et seulement si il n'ont aucune racine commune dans toute extension de $\mathbb{K}$.

2. Soit $P \in \mathbb{K}[X]$ et $\mathbb{L} \supset \mathbb{K}$ une extension qui contient toutes les racines de P. Montrer que toutes les racines de P sont simples si et seulement si P est premier avec sa dérivée P'.

3. Soit $\mathbb{K}$ un corps de caractéristique nulle ou un corps fini.
Montrer qu'un polynôme irréductible de $\mathbb{K}[X]$ n'a pas de racine multiple (dans n'importe quelle extension de $\mathbb{K}$).

Exercice 2. Soit $P \in \mathbb{K}[X]$ de degré 3. Montrer que P est irréductible si et seulement si P n'a pas de racine dans $\mathbb{K}$.

Exercice 3. Soit $P(X) = a_0X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$. Soit $\alpha = p/q \in \mathbb{Q}$ une racine rationnelle de P, avec $\mathrm{pgcd}(p, q) = 1$.
Montrer que p divise a_n et q divise a_0. (En particulier, si $a_0 = 1$, toute racine rationnelle est entière.)

Exercice 4. 1. Montrer que $X^4 + 1$ est irréductible sur $\mathbb{Q}$.

2. Montrer que $X^4 + 1$ est réductible dans $\mathbb{Z}/p\mathbb{Z}$ quelque soit p premier.
Indication : Ecrire $X^4 + 1 = (X^2 + 1)^2 - 2X^2 = (X^2 - 1)^2 + 2X^2$ et montrer que -1 ou 2 ou -2 est un carré dans $\mathbb{Z}/p\mathbb{Z}$.

Exercice 5. 1. Soit p premier. Montrer que $X^{p-1} + X^{p-2} + ... + X + 1$ est irréductible sur $\mathbb{Q}$.

2. Soit p premier. Montrer que $X^n + pX + p^2$ est irréductible.
(Utiliser la réduction mod p.)

3. Soit $a \in \mathbb{Z}$ et p un premier qui ne divise pas a. Montrer que $X^p - X + a$ est irréductible sur $\mathbb{Z}/p\mathbb{Z}$.
(Raisonner par absurde et considérer le corps de décomposition de ce polynôme sur $\mathbb{Z}/p\mathbb{Z}$.)

4. Soit p premier, $\mathbb{K}$ un corps. Montrer que $P(X) = X^p - a \in \mathbb{K}[X]$ est irréductible si et seulement si P n'a pas de racine dans $\mathbb{K}$.
Indication : considérer la factorisation de P dans le corps de décomposition de P.
En particulier, si $\mathbb{K} \subset \mathbb{R}$, P est irréductible sur $\mathbb{K}$ si et seulement si $a^{1/p}$ n'est pas dans $\mathbb{K}$.

Exercice 6. Algorithme pour déterminer les diviseurs d'un polynôme $P(X) \in \mathbb{Z}[X]$.

1. Soit $g(X) \in \mathbb{Z}[X]$ divise $P(X)$, $\deg(g) = d$.
   Alors $g(j)$ divise $P(j)$ pour $j = 0, \ldots, d$.
2. Etant donnés $a_0, ..., a_d \in \mathbb{Z}$ il existe un seul polynôme $g \in \mathbb{Q}[X]$ tels que $g(j) = a_j$, $j = 0, \ldots, d$.
3. Donner une méthode pour déterminer les diviseurs du polynôme $P(X)$.

Exercice 7. 1. Déterminer toutes les extensions algébriques de $\mathbb{C}$.

2. Montrer que toute extension algébrique de $\mathbb{R}$ est isomorphe à $\mathbb{C}$.

Exercice 8. Soit $\mathbb{K}$ un corps et $f : \mathbb{Q} \to \mathbb{K}$ un morphisme de corps. Montrer que $\mathbb{K}$ est de caractéristique nulle et que f est l'identité (sous-entendu $\mathbb{Q}$ est contenu dans tout corps de caractéristique nulle).

1. Déterminer tous les automorphismes de $\mathbb{R}$.
2. Déterminer tous les automorphismes continus de $\mathbb{C}$.

Exercice 9. Soit $\mathbb{K} \subset \mathbb{L}$ une extension de degré n.
Montrer que le degré sur $\mathbb{K}$ de tout élément de $\mathbb{L}$ divise n.