Université Paris 7 - Denis Diderot
UFR de Mathématiques

Premier semestre 2006/07
M1 Maths-info - Algèbre

Feuille d'exercices n° 4

Corps

Exercice 1. Soit L/K une extension de corps et $a \in L$ tel que l'extension $K(a)/K$ est de degré 5. Que peut-on dire du corps $K(a^2)$?

Exercice 2. Calculer les degrés des extensions de corps suivantes :

1) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$
2) $\mathbb{Q}(i, \sqrt[3]{2})/\mathbb{Q}$
3) $\mathbb{Q}(j)/\mathbb{Q}(j^2)$ où j désigne $\frac{-1+\mathrm{i}\sqrt{3}}{2}$
4) $\mathbb{Q}(\sqrt{3}+\sqrt{5})/\mathbb{Q}$
5) $\mathbb{Q}(\sqrt{p}+\frac{1}{\sqrt{p}})/\mathbb{Q}$ où p est un nombre premier
6) $\mathbb{Q}(\sqrt[p]{ap})/\mathbb{Q}$ où p est un nombre premier et $a \geq 1$ un entier premier à p
7) $\mathbb{F}_p(t^{1/n})/\mathbb{F}_p(t)$ où p est un nombre premier et $n \geq 2$ un entier

Exercice 3. Les polynômes suivants sont-ils irréductibles dans $\mathbb{Q}[X]$?

1) $X^3 + 6X^2 + 5X + 25$
2) $X^4 + X^2 + 1$
3) $X^3 + 6X^2 + 11X + 8$
4) $X^5 + 5X^4 + 3X - 1$
5) $X^{2006} - 101$
6) $X^4 + 1$

Exercice 4. Soit p un nombre premier. En posant $Y = X - 1$ et à l'aide du critère d'Eisenstein, montrer que le polynôme $X^{p-1} + X^{p-2} + \ldots + X + 1$ est irréductible sur $\mathbb{Q}$. De quels nombres complexes est-ce le polynôme minimal ?

Exercice 5. Déterminer un corps de rupture et le corps de décomposition de chacun des polynômes suivants de $\mathbb{Q}[X]$, ainsi que le degré de ces corps sur $\mathbb{Q}$:

1) $X^4 - 1$
2) $X^4 + 1$
3) $X^7 - 1$
4) $X^4 - 4$
5) $X^5 - 2$

Exercice 6.

1) Soit K un corps et $P \in K[X]$. À quelle condition sur le polynôme P l'anneau quotient $K[X]/(P)$ est-il un corps ? Donner alors le degré de ce corps sur K.

2) Soit T le polynôme $X^3 + 24X^2 - X + 5$. Les anneaux $\mathbb{F}_5[X]/(T)$ et $\mathbb{F}_2[X]/(T)$ sont-ils des corps ? Si c'est le cas, donner leur cardinal.

3) Montrer que toute racine de T dans $\mathbb{Q}$ est entière. En déduire que $\mathbb{Q}[X]/(T)$ est un corps.

Exercice 7. Le **contenu** $c(P)$ d'un polynôme non nul $P \in \mathbb{Z}[X]$ à coefficients entiers est le pgcd de ses coefficients.

1) Soient $P, Q \in \mathbb{Z}[X]$ et p un diviseur premier de $c(PQ)$. En utilisant l'anneau intègre $\mathbb{F}_p[X]$, montrer que p divise $c(P)$ ou $c(Q)$.

2) En déduire la formule $c(PQ) = c(P)c(Q)$.

3) Soit $T \in \mathbb{Z}[X]$ un polynôme à coefficients entiers. On suppose que T se factorise sous la forme $T = PQ$ avec $P, Q \in \mathbb{Q}[X]$. Montrer qu'il existe deux polynômes à coefficients entiers $\tilde{P}, \tilde{Q} \in \mathbb{Z}[X]$ respectivement proportionnels à P et Q et tels que $T = \tilde{P}\tilde{Q}$.

Ce résultat vaut non seulement pour l'anneau $\mathbb{Z}$ mais pout tout anneau principal (et même tout anneau factoriel).

Exercice 8. Critère d'Eisenstein. Soit p un nombre premier et $P = a_n X^n + \cdots + a_0 \in \mathbb{Z}[X]$ un polynôme à coefficients entiers tels que p divise $a_0, a_1, \cdots, a_{n-1}$ mais p ne divise pas a_n et p^2 ne divise pas a_0.

Montrer, à l'aide de l'exercice précédent et de la réduction modulo p, que le polynôme P est irréductible dans $\mathbb{Q}[X]$.

Ce résultat aussi vaut non seulement pour l'anneau $\mathbb{Z}$ mais pout tout anneau principal (et même tout anneau factoriel).

Exercice 9.

1) Soit K un corps et $P \in K[X]$ un polynôme de degré n. Montrer que P est irréductible dans $K[X]$ si et seulement s'il n'a pas de racines dans les extensions L de K de degré $[L : K] \leq \frac{n}{2}$.

2) Le polynôme $X^4 + X + 1$ est-il irréductible dans $\mathbb{F}_2[X]$?

3) Le polynôme $X^4 + X^2 + 1$ est-il irréductible dans $\mathbb{F}_5[X]$?

Exercice 10. Soit p un nombre premier > 2 et $q = p^n$ pour un entier $n \in \mathbb{N}^*$.

1) Montrer qu'il y a exactement $\frac{q-1}{2}$ carrés non nuls dans $\mathbb{F}_q$.

2) Montrer que -1 est un carré dans $\mathbb{F}_q$ si et seulement si $q \equiv 1 \bmod 4$.

3) En déduire qu'il existe une infinité de nombres premiers de la forme $4m + 1$.

Ce dernier résultat est un cas particulier du théorème de la progression arithmétique de Dirichlet (1835) : pour tous entiers naturels non nuls a et b premiers entre eux, il existe une infinité de nombres premiers de la forme $a + mb$, où $m > 0$.