Université Pierre et Marie Curie **2004-2005**

MF12 Algèbre et théorie de Galois

Examen 2ème session du 6 septembre 2005 (durée 4h)

Tous les anneaux considérés sont commutatifs et unitaires. Le barême indiqué (sur **100**) peut éventuellement être modifié légèrement.

Questions et exercices de cours (30 pts)

Q1) Donner la définition des notions suivantes : a) anneau noethérien, b) anneau principal, c) élément irréductible d'un anneau, d) anneau factoriel.

Q2) Montrer qu'un anneau principal est factoriel.

Q3) Soit K un corps. Montrer que l'anneau de polynômes $K[X]$ est principal.

Q4) Soient K un corps et $P \in K[X]$ un polynôme non constant. Donner la définition du corps de décomposition de P sur K.

Exercice 1 (15 pts) Soit $\mathbb{Z}[i\sqrt{5}\,] = \{a + i\sqrt{5}\,b \mid a, b \in \mathbb{Z}\}$. C'est un sous-anneau de $\mathbb{C}$, stable par la conjugaison complexe $z \mapsto \overline{z}$. Pour tout $\xi = a + i\sqrt{5}\,b$ dans $\mathbb{Z}[i\sqrt{5}\,]$, on définit sa norme $N(\xi)$ par :

$$N(\xi) = \xi\overline{\xi} = a^2 + 5b^2.$$

On observera que $N(\xi)$ est un entier ≥ 0.

1) Soient $\xi, \xi' \in \mathbb{Z}[i\sqrt{5}\,]$. Montrer, en utilisant la conjugaison complexe, que $N(\xi\xi') = N(\xi)N(\xi')$. En déduire que ξ est inversible si et seulement si $N(\xi) = 1$, c.-à-d., si et seulement si $\xi = \pm 1$.

2) Déduire de 1) que tout élément de norme 4, 6 ou 9 est irréductible.

3) En considérant deux factorisations de 6 distinctes, montrer que $\mathbb{Z}[i\sqrt{5}\,]$ n'est pas factoriel.

Exercice 2 (15 pts) Pour tout corps K et tout polynôme $Q = \sum_{i=0}^{d} a_i X^i$ dans $K[X]$, le polynôme dérivé Q' est défini par $Q' = \sum_{i=1}^{d} i a_i X^{i-1}$. On rappelle la formule suivante (qu'on ne demande pas de démontrer) :

$$(*) \qquad (Q_1 Q_2)' = Q_1' Q_2 + Q_1 Q_2'.$$

Soient k un corps, $P \in k[X]$, non constant, et soit K un corps de décomposition de P sur k. On suppose que le PGCD de P et P' est 1.

Montrer que les racines de P dans K sont deux à deux distinctes.

Problème (40 pts) Soit p un nombre premier > 0 et soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps à p éléments.

1) Soit L un surcorps de $\mathbb{F}_p$. Montrer que l'application $F : x \mapsto x^p$ est un endomorphisme de L. Pour tout $n \geq 1$, soit

$$L^{F^n} = \{x \in L \mid x^{p^n} = x\}.$$

Montrer que L^{F^n} est un sous-corps de L.

2) Soit $n \geq 1$ et soit K un corps de décomposition sur $\mathbb{F}_p$ du polynôme $X^{p^n} - X$. En utilisant la question 1) et l'exercice 2, montrer que K a exactement p^n éléments. On le notera $\mathbb{F}_{p^n}$.

3) Montrer que l'extension $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$ est galoisienne.

4) Soit $\mathbb{F}_p \subseteq L$ une extension de corps de degré fini m. Montrer que L est de cardinal p^m et que tout élément $x \neq 0$ de L vérifie $x^{p^m-1} = 1$. En déduire que l'extension $L/\mathbb{F}_p$ est galoisienne.

5) Montrer que si $\mathbb{F}_{p^n}$ contient un sous-corps L tel que $[L : \mathbb{F}_p] = d$, alors d divise n.

Soit $x \in \mathbb{F}_{p^n}$ et soit $P = \mathrm{Irr}_{\mathbb{F}_p}(x)$ son polynôme minimal sur $\mathbb{F}_p$. Montrer que P est un polynôme irréductible de degré d divisant n.

6) Pour tout $d \geq 1$, soit $I(p, d)$ l'ensemble des $P \in \mathbb{F}_p[X]$ irréductibles unitaires de degré d et soit $i(p, d)$ son cardinal.

Soient d un diviseur de n et $P \in I(p, d)$. Montrer qu'il existe exactement d éléments $\alpha \in \mathbb{F}_{p^n}$ tels que $\mathrm{Irr}_{\mathbb{F}_p}(\alpha) = P$.

Indication : Soit α une racine de P dans L, un corps de décomposition de P sur $\mathbb{F}_{p^n}$; en utilisant la question 4), montrer que $\alpha \in \mathbb{F}_{p^n}$ et que P a d racines distinctes dans $\mathbb{F}_{p^n}$.

7) En considérant sur $\mathbb{F}_{p^n}$ la relation d'équivalence $\sim$ définie par : $x \sim y$ si x et y ont le même polynôme minimal sur $\mathbb{F}_p$, montrer que

$$p^n = \sum_{d|n} i(p, d)d.$$

Soit T une indéterminée. On considère la série formelle

$$\sigma(T) = \sum_{d \geq 1} i(p, d) \sum_{k \geq 1} \frac{T^{dk}}{k}.$$

Montrer que

$$\sigma(T) = \sum_{n \geq 1} \frac{(pT)^n}{n}.$$