Université Paris Sud **Année 2004-2005**

M1 **Arithmétique**

Examen partiel du 5 avril 2005

Durée trois heures

La qualité de la rédaction entrera pour une grande part dans la notation. Les calculatrices, téléphones mobiles et documents ne sont pas autorisés.

Exercice A

Dans tout cet exercice, K **est un corps et** K^s **une clôture séparable de** K. **On note** p **un nombre premier. Lorsque le corps** K **est de caractéristique** p **(et donc contient** $\mathbb{F}_p$**), on note** $\rho_K : K \to K$ **l'application définie par** $\rho_K(x) := x^p - x$.

On suppose, jusqu'à la question 8 que K **est de caractéristique** p.

1 .a) Montrer que ρ_K est un endomorphisme du groupe additif de K et déterminer son noyau.
b) Montrer que ρ_{K^s} est surjectif.

2) Soit a **un élément de** K **qui n'est pas dans l'image de** ρ_K. **Soit** α **une racine du polynôme** $P := X^p - X - a$ **dans** K^s.
a) Déterminer l'ensemble des racines de P dans K^s.

b) Montrer que le corps $L_a = K(\alpha)$ est une extension cyclique de degré p de K.

c) Si $b \in \operatorname{Im}\rho_K$, montrer que $L_{a+b} = L_a$.

3) Soit L une extension cyclique de degré p de K contenue dans K^s. Montrer qu'il existe $a \notin \operatorname{Im}\rho_K$ tel que $L = L_a$. **Indication** *Si* $\theta \in L$ *est tel que* $\operatorname{Tr}_{L/K}(\theta) = 1$, *et si* σ *est un générateur de Gal*(L/K), *considérer l'élément* $\alpha = -\sum_{n=1}^{p-1} n.\sigma^n(\theta)$.

Dans la suite de l'exercice K **est un corps complet pour une valuation discrète,** π **est une uniformisante de** K, v **est la valuation de** K^s **qui prolonge la valuation de** K **telle que** $v(\pi) = 1$. **On suppose le corps résiduel** k **de** K **parfait.**
4) Soit a un élément de K vérifiant $v(a) > 0$. Montrer que $a \in \operatorname{Im}\rho_K$.

5) Soit a un élément de K vérifiant $v(a) = 0$. Montrer que $a \in \operatorname{Im}\rho_K$ si et seulement si l'image de a dans k appartient à l'image de ρ_k. Dans le cas contraire, montrer que L_a/K est non ramifiée.

6) Soit $a \in K$ **avec** $v(a) < 0$ **divisible par** p.
a) Montrer que l'on peut trouver $b \in K$ tel que $v(a + \rho_K(b)) > v(a)$.

b) En déduire que, si a n'est pas dans l'image de ρ_K, on peut trouver c tel que $v(a+\rho_K(c)) = -i$ avec $i \in \mathbb{N}$, premier à p s'il est non nul.

7) On suppose $v(a) = -i$, **avec** $i \in \mathbb{N}$, **premier à** p. **Soit** α **une racine de** $X^p - X - a$ **dans** K^s.
a) Calculer $v(\alpha)$.

b) Montrer que l'extension L_a/K est totalement ramifiée.

c) Montrer qu'il existe $r, s \in \mathbb{Z}$ tels que $\pi^r \alpha^s$ est une uniformisante de L_a.

8) On suppose maintenant que K **est de caractéristique** 0 **et on pose** $e_K = v(p)$. **Soient** $i \in \mathbb{N}$ **un entier premier à** p, $a \in K$ **vérifiant** $v(a) = -i$, $P = X^p - X - a$, α **une racine de** P **dans** K^s **et** $L = K(\alpha)$.
a) Calculer $v(\alpha)$.

b) Montrer que l'extension L/K est totalement ramifiée et calculer son degré.

On suppose $i < e_K/(p-1)$.
c) Montrer qu'il existe une racine β de P dans L vérifiant $v(\beta - \alpha - 1) > 0$.

d) En déduire que l'extension L/K est galoisienne.

Exercice B

Soit

$$T \ := \ X^3 - 13X + 20 \ \in \mathbb{Z}[X] \text{ et } K \ := \ \mathbb{Q}[X]/(T) \ .$$

1) Montrer que K est un corps de nombres.

2) Montrer que T est un produit de trois facteurs linéaires distincts dans $\mathbb{Q}_2[X]$.

3) En déduire que 2 est totalement décomposé dans K, c'est-à-dire qu'il est produit de trois idéaux maximaux distincts, de degré résiduel 1.

4) En déduire que l'anneau des entiers $\mathcal{O}_K$ de K n'est pas monogène. Plus précisément montrer que 2 divise l'indice $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ de $\mathbb{Z}[\alpha]$ dans $\mathcal{O}_K$ pour tout entier α de K.

5) Si α désigne une racine de T, montrer que

$$\delta_{K/\mathbb{Q}}(\alpha) \ = \ -2012 = -2^2 \cdot 503 \ .$$

En déduire le discriminant de $\mathcal{O}_K$.

6) Vérifier que $\frac{\alpha^2+\alpha}{2}$ est un entier algébrique. En déduire une $\mathbb{Z}$-base de $\mathcal{O}_K$.

Exercice C

Soit L/K une extension finie de corps de nombres. On veut montrer qu'il existe une infinité d'idéaux maximaux $\mathfrak{p}$ de $\mathcal{O}_K$ totalement décomposés dans L, c'est-à-dire tels que $\mathfrak{p}\mathcal{O}_L$ est un produit fini d'idéaux maximaux distincts de $\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L \ = \ \prod_{i=1}^{g} \mathfrak{p}_i,$$

où $\mathcal{O}_L/\mathfrak{p}_i \ \cong \ \mathcal{O}_K/\mathfrak{p}$ pour tout i.

1) Montrer qu'il suffit de traiter le cas $K = \mathbb{Q}$, L un corps de nombres galoisien. On se place dorénavant dans ce cadre.

2) Pour tout polynôme $P \in \mathbb{Z}[X]$, montrer qu'il existe une infinité de nombres premiers $p \in \mathbb{Z}$ tels que P a une racine dans $\mathbb{F}_p$.

3) On écrit $L = \mathbb{Q}(\alpha)$, où α est entier de polynôme minimal P. Montrer que si p est tel que P ait une racine dans $\mathbb{F}_p$ et soit sans facteur carré modulo p, alors P est un produit de facteurs linéaires dans $\mathbb{F}_p[X]$.

4) Conclure.