Université Paris Sud — Année 2008-2009

M1 — Arithmétique

Examen partiel du 27 mars 2009

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.

Les quatre problèmes sont indépendants.
Notes de cours autorisées.

Exercice A

1) Déterminer tous les polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_3$. Montrez que le polynôme $X^4 + X - 1$ est irréductible sur $\mathbb{F}_3$.

2) Soit $P = X^5 + 4X^2 - X + 3 \in \mathbb{Z}[X]$. **On note** P_2 **l'image de** P **dans** $\mathbb{F}_2[X]$ **et** P_3 **son image dans** $\mathbb{F}_3[X]$.
a) Déterminer la décomposition de P_3 en produit de polynômes irréductibles unitaires sur $\mathbb{F}_3$.

b) Montrer que P_2 a une racine dans $\mathbb{F}_4$. En déduire la décomposition de P_2 en produit de polynômes irréductibles sur $\mathbb{F}_2$.

3) Soit $Q \in \mathbb{Z}[X]$ un polynôme de degré ≤ 5. Montrer que le polynôme $P + 6Q$ est irréductible sur $\mathbb{Q}[X]$.

Exercice B

Soit K **un corps.**

1) Soient N **un entier** ≥ 1 **et** L **une extension cyclique de degré** N **de** K. **On choisit un générateur** σ **de** $\mathrm{Gal}(L/K)$ **et on note** $T : L \to K$ **la trace. Si** $\alpha, \theta \in L$, **on pose**

$$\begin{aligned}\rho_\theta(\alpha) = \theta\alpha + \sigma\theta(\alpha + \sigma\alpha) + \ldots + \sigma^i\theta(\alpha + \sigma\alpha + \ldots + \sigma^i\alpha)\\ + \ldots + \sigma^{N-2}\theta(\alpha + \sigma\alpha + \ldots + \sigma^{N-2}\alpha)\,.\end{aligned}$$

On suppose que $T(\alpha) = 0$.

a) Calculer $\rho_\theta(\alpha)$.

b) En déduire qu'il existe $\beta \in L$ tel que $\alpha = \sigma(\beta) - \beta$.

Dans la suite du problème, on suppose que le corps K est de caractéristique $p > 0$.

2) Soit L une extension cyclique de degré p de K.

a) Montrer qu'il existe $\beta \in L$ tel que $\sigma(\beta) = \beta + 1$.

b) Montrer que $L = K[\beta]$ et déterminer tous les conjugués de β dans l'extension L/K.

c) Montrer qu'il existe $b \in K$ tel que le polynôme minimal de β sur K est $X^p - X - b$.

3) Réciproquement, montrer que si $b \in K$ est tel que le polynôme $P = X^p - X - b$ n'a pas de racine dans K, alors P est irréductible sur K et si β est une racine de P dans un corps contenant K, le corps $K[\beta]$ est une extension cyclique de degré p de K.

4) On suppose maintenant que K (toujours de caractéristique p) est complet pour une valuation discrète, son corps résiduel k étant parfait. On note v la valuation de K telle que $v(K^*) = \mathbb{Z}$. Soit $b \in K$.

Montrer que, pour que le polynôme $X^p - X - b$ soit irréductible sur K, il faut et il suffit qu'il existe un entier $i > 0$, premier à p et $c \in K$ tel que $v(b - c^p + c) = -i$.

Exercice C

1) Pour tout anneau commutatif R, on note $R[[X]]$ l'anneau des séries formelles à coefficients dans R, c'est-à-dire le séparé complété de $R[X]$ pour la topologie (X)-adique. On pose aussi $R((X)) = S^{-1}R[[X]]$ où S est le système multplicatif $(X^n)_{n\in\mathbb{N}}$.

a) Soit $(a_n)_{n\in\mathbb{N}}$ une suite d'éléments de R. Montrer que la série $\sum_{n=0}^{+\infty} a_n X^n$ converge dans $R[[X]]$ et que tout élément de $R[[X]]$ s'écrit d'une manière et d'une seule comme la somme d'une telle série.

b) Donner une description analogue des éléments de $R((X))$ (utilisant les familles $(a_n)_{n\in\mathbb{Z}}$ d'élments de R tels que l'ensemble des $n < 0$ tels que $a_n \neq 0$ est fini).

Dans la suite de ce problème, k est un corps parfait, E est un corps contenant k et t un élément de E transcendant sur k. On pose $A = k[t]$. L'application de l'anneau des polynômes $k[X]$ dans A qui envoie un polynôme Q sur sa valeur $Q(t)$ en t est donc un isomorphisme de $k[X]$ sur A.

2) Soit $\mathfrak{p}$ un idéal maximal de A et $P \in k[X]$ l'unique polynôme unitaire tel que $\pi = P(t)$ est un générateur de $\mathfrak{p}$. Soit $\hat{A}$ le séparé complété de A pour la topologie $\mathfrak{p}$-adique.

a) Montrer que l'application naturelle de A dans $\hat{A}$ est injective (dans la suite, on l'utilise pour identifier A à un sous-anneau de $\hat{A}$).

b) Montrer que $\hat{A}$ est un anneau de valuation discrète complet et que π est une uniformisante de $\hat{A}$.

c) On note a l'image de t dans le corps résiduel k' de $\hat{A}$. Montrer que $k' = k[a]$. Déterminer le polynôme minimal de a sur k.

d) Montrer que ce polynôme a une racine dans $\hat{A}$ qui relève a. En déduire qu'il existe un unique k-plongement $s : k' \to \hat{A}$ qui est tel que, pour tout $b \in k'$, s(b) est un relèvement de b dans $\hat{A}$.

e) On utilise s pour identifier k' à un sous-corps de $\hat{A}$. Montrer que $\hat{A}$ s'identifie à l'anneau $k'[[\pi]]$ des séries formelles en l'indéterminée π à coefficients dans k'. Que peut-on dire du corps des fractions $\hat{K}$ de $\hat{A}$?

3) Soit $\hat{L}$ une extension finie séparable de $\hat{K}$, k' le corps résiduel de $\hat{L}$ et π une uniformisante de $\hat{L}$. Montrer que $\hat{L}$ s'identifie au corps des séries formelles $k'((\pi))$.

4) Soient $Q \in k[X]$ un polynôme unitaire et $P_1, P_2, \ldots, P_g$ les polynômes irréductibles unitaires distincts qui divisent Q. On pose $k_i = k[X]/(P_i)$. Montrer que $\hat{A} = A_1 \times A_2 \times A_g$ avec $A_i \simeq k_i[[X]]$.

Exercice D

On choisit un nombre premier p **et une clôture algébrique** $\overline{\mathbb{Q}_p}$ **de** $\mathbb{Q}_p$. **On note** v_p **l'unique valuation sur** $\overline{\mathbb{Q}_p}$ **telle que** $v_p(p) = 1$. **Pour tout sous-corps** L **de** $\overline{\mathbb{Q}_p}$ **on pose** $\mathcal{O}_L = \{x \in L \mid v_p(x) \geq 0\}$.

On se donne deux entiers r, s **strictement positifs et on pose** $P = p^3 + pX^r + pX^{r+1} + X^{r+s}$.

1) On suppose $r > 2s$ **et que** $r + s = 3m + 2$, **avec** $m \in \mathbb{N}$.

a) Montrer que P est irréductible sur $\mathbb{Q}_p$.

b) Soit α une racine de P dans $\overline{\mathbb{Q}_p}$ et soit $E = \mathbb{Q}_p[\alpha]$. Montrer que l'extension $E/\mathbb{Q}_p$ est totalement ramifiée. Montrer qu'il existe $i \in \mathbb{Z}$ tels que $\mathcal{O}_E = \mathbb{Z}_p[p^{-1}\alpha^i]$.

2) On suppose maintenant que $r = 3$ **et** $s = 5$.

a) Montrer que $P = P_1 P_2$ avec $P_1, P_2 \in \mathbb{Q}_p[X]$ irréductibles unitaires et $\deg(()P_1) < deg(P_2)$. Déterminer les degrés de P_1 et P_2.

b) Soient β une racine de P_1 et γ une racine de P_2 dans $\overline{\mathbb{Q}_p}$, $F_1 = \mathbb{Q}_p[\beta]$, $F_2 = \mathbb{Q}_p[\gamma]$ et $F_3 = \mathbb{Q}_p[\beta, \gamma]$. Pour $i = 1, 2, 3$, calculer le degré de l'extension $F_i\mathbb{Q}_p]$ et trouver un élément π_i tel que $F_i = \mathbb{Z}_p[\pi_i]$.