Université Paris Sud — Année 2008-2009

M1 — Arithmétique

TD n$^\circ$ IV

Exercice A

Soient p **un nombre premier,** K **une extension finie de** $\mathbb{Q}_p$, k **son corps résiduel,** L **une extension finie galoisienne totalement ramifiée de** K, $\mathcal{O}_L$ **l'anneau des entiers de** L **et** v_L **la valuation de** L **telle que** $v_L(L^*) = \mathbb{Z}$. **On pose** $G := \mathrm{Gal}_{L/K}$ **et on choisit une uniformisante** π **de** L. **Pour tout** $\sigma \in G$, **on pose** $i_L(\sigma) = v_L(\sigma(\pi) - \pi) - 1$.

1) Montrer que $i_L(\sigma) \in \mathbb{N} \cup \{+\infty\}$ et que $i_L(\sigma) = +\infty$ si et seulement si σ est l'élément neutre de G.

2) Soit $i \in \mathbb{N}$. Montrer que $i_L(\sigma) \geq i$ si et seulement si $v_L(\sigma(a) - a) \geq i + 1$ pour tout $a \in \mathcal{O}_L$.

3) Pour tout $i \in \mathbb{N}$, **on pose**

$$G_i := \{\sigma \in G \mid i_L(\sigma) \geq i\} .$$

Montrer que G_i est un sous-groupe invariant de G.

4) Pour tout $\sigma \in G$, **on note** $\theta_0(\sigma)$ **l'image de** $\sigma(\pi)/\pi$ **dans** k.

a) Montrer que θ_0 est un homomorphisme de G dans le groupe multiplicatif k^* de k.

b) Déterminer le noyau de θ_0 et montrer que G/G_1 est un groupe cyclique d'ordre premier à p.

5) Soit i **un entier** ≥ 1. **Pour tout** $\sigma \in G_i$, **on note** $\theta_i(\sigma)$ **l'image de** $\frac{\sigma(\pi)-\pi}{\pi^{i+1}}$ **dans** k.

a) Montrer que θ_i est un homomorphisme de G_i dans k et déterminer son noyau.

b) Montrer que G_i/G_{i+1} est un groupe abélien d'ordre une puissance de p.

6) Montrer que G_1 est un groupe d'ordre une puissance de p.

Exercice B

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 Trace$_{L/K}(\theta) = 1$, 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 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 $v(b+\rho_K(c)) = -i$ 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 C

On choisit une clôture algébrique $\overline{\mathbb{Q}}$ de $\mathbb{Q}$ et, pour tout nombre premier p, une clôture algébrique $\overline{\mathbb{Q}_p}$ de $\mathbb{Q}_p$ contenant $\overline{\mathbb{Q}}$. On choisit une racine α du polynôme $X^{12} - 7$ dans $\overline{\mathbb{Q}}$

et on pose $L := \mathbb{Q}(\alpha)$. **On note** B **la fermeture intégrale de** $\mathbb{Z}$ **dans** L. **Pour tout nombre premier** p, **on pose** $L_p := \mathbb{Q}_p \otimes_{\mathbb{Q}} L$.

1 .a) Montrer que $X^{12} - 7$ est irréductible sur $\mathbb{Q}_7$ et sur $\mathbb{Q}$. Calculer le degré de l'extension $L/\mathbb{Q}$.
b) Montrer que L_7 est un corps et calculer l'indice de ramification et le degré résiduel de l'extension $L_7/\mathbb{Q}_7$.

c) Combien y-a-t'il d'ideaux maximaux de B au-dessus de 7 ? Pour chacun d'eux, déterminer l'indice de ramification et le degré résiduel.

2 .a) Montrer que, si $p \notin \{2, 3, 7\}$, alors L_p est un produit d'extensions finies non ramifiées de $\mathbb{Q}_p$.
b) Montrer que l'anneau $\mathbb{Z}[\alpha]$ est p-clos.

3 .a) Montrer que le polynôme $X^3 - 7$ a une racine b et une seule dans $\mathbb{Q}_2$.
b) Montrer que le polynôme $(1 + X)^4 - b$ est un polynôme d'Eisenstein sur $\mathbb{Q}_2$.

Soit $\beta \in \overline{\mathbb{Q}}_2$ **une racine du polynôme** $X^4 - b$, **soit** $E = \mathbb{Q}_2(\beta)$ **et soit** $\mathcal{O}_E$ **l'anneau de ses entiers.**

c) Calculer l'indice de ramification et le degré résiduel de l'extension $E/\mathbb{Q}_2$. A-t'on $\mathcal{O}_E = \mathbb{Z}_2[\beta]$?

Soit ε **une racine primitive troisième de l'unité dans** $\overline{\mathbb{Q}_2}$, **soit** $E' := \mathbb{Q}_2(\varepsilon\beta)$ **et soit** $\mathcal{O}_{E'}$ **l'anneau de ses entiers.**

d) Calculer l'indice de ramification et le degré résiduel de l'extension $E'/\mathbb{Q}_2$. A-t'on $\mathcal{O}_{E'} = \mathbb{Z}_2[\varepsilon\beta]$?

e) Montrer que L_2 est isomorphe à $E \times E'$. Combien y-a-t'il d'ideaux maximaux de B au-dessus de 2 ? Pour chacun d'eux, donner l'indice de ramification et le degré résiduel.

4) En s'inspirant de la question précédente, écrire L_3 comme un produit de corps. Dire combien il y a d'ideaux maximaux de B au-dessus de 3. Pour chacun d'eux, déterminer l'indice de ramification et le degré résiduel.

5) Décrire l'anneau $\mathcal{O}_L$ des entiers du corps L.

Exercice D

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 $\mathcal{O}_K$.