Université Paris Sud — Année 2005-2006

M1 — Arithmétique

Examen partiel du 3 avril 2006

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 exercices sont indépendants.

Exercice A

1) Soient A un anneau.
a) Rappeler la propriété universelle de l'anneaux $A[X]$ des polynômes à une indéterminée sur A.

Soit B une A-algèbre.
b) Construire des morphismes de B-algèbres

$$\phi \ : \ B[X] \ \rightarrow \ B \otimes_A A[X] \text{ et } \psi \ : \ B \otimes_A A[X] \ \rightarrow \ B[X]$$

inverse l'un de l'autre.

2) Soient E un corps, $P_1, P_2 \in E[X]$ des polynômes à coefficients dans E, d_1 le degré de P_1, d_2 celui de P_2 et r celui de leur pgcd.
Montrer que les anneaux $A_1 = E[X]/(P_1)$, $A_2 = E[X]/P_2$ et $A_3 = A_1 \otimes_{E[X]} A_2$ sont des E-espaces vectoriels de dimension finie et calculer leurs dimensions.

Exercice B

Soit p un nombre premier.
1) Soit X un $\mathbb{Z}_p$-module sans p-torsion (c'est-à-dire tel que si $x \in X$ est non nul, alors $px \neq 0$.) On suppose que X/pX est un groupe fini d'ordre p^r et que l'application naturelle $X \rightarrow \varprojlim_{n \in \mathbb{N}} X/p^n X$ est un isomorphisme. Montrer que X est un $\mathbb{Z}_p$-module libre de rang r.

2) Soit Y un $\mathbb{Z}_p$-module contenant un sous-$\mathbb{Z}_p$-module X qui est libre de rang r et tel que Y/X est un groupe fini. Montrer que Y est un $\mathbb{Z}_p$-module de type fini qui peut s'écrire comme le produit direct d'un p-groupe fini par un $\mathbb{Z}_p$-module libre de rang r.

Dans la suite du problème, L est une extension finie de $\mathbb{Q}_p$. On note $\mathcal{O}_L$ l'anneau des entiers de L, $\mathfrak{m}_L$ son idéal maximal, k son corps résiduel. On pose $d = [L : \mathbb{Q}_p]$, $f = [k : \mathbb{F}_p]$ et on note e l'indice de ramification de l'extension $L/\mathbb{Q}_p$. On note $\mathcal{O}_L^*$ le groupe multiplicatif des éléments inversibles de $\mathcal{O}_L$ et, pour tout entier $n \geq 1$, on pose

$$U^{(n)} \ := \ \{u \in \mathcal{O}_L \mid u - 1 \in \mathfrak{m}_L^n\} \ .$$

3 .a) Montrer que, pour tout entier $n \geq 1$, $U^{(n)}$ est un sous-groupe de $\mathcal{O}_L^*$.
b) Montrer que $U^{(n)}/U^{(n+1)}$ est un groupe fini d'ordre p^f.

c) Montrer que, pour tout $m \in \mathbb{N}$, $U^{(n)}/U^{(n+m)}$ est un p-groupe fini dont on déterminera l'ordre.

4) Montrer que $\mathcal{O}_L^*/U^{(1)}$ est un groupe cyclique d'ordre $p^f - 1$.

5) Montrer que les applications naturelles

$$\mathcal{O}_L^* \ \to \ \varprojlim_{n \geq 1} \mathcal{O}_L^*/U^{(n)} \ \text{ et, pour } n \geq 1, \ U^{(n)} \ \to \ \varprojlim_{m \in \mathbb{N}} U^{(n)}/U^{(n+m)}$$

sont des isomorphismes.

Ceci nous permet de considérer les $U^{(n)}$ comme des $\mathbb{Z}_p$-modules (un groupe abélien annulé par une puissance p^m de p peut être considéré comme un $\mathbb{Z}/p^m\mathbb{Z}$-module, donc aussi comme un $\mathbb{Z}_p$-module puisque

$$\mathbb{Z}/p^m\mathbb{Z} \ = \ \mathbb{Z}_p/p^m\mathbb{Z}_p \ .)$$

6) Soit π une uniformisante de L, soit n un entier vérifiant $n > e/(p-1)$ et $x \in \mathcal{O}_L$.
a) Montrez que

$$(1 + \pi^n x)^p - (1 + p\pi^n x) \ \in \ \mathfrak{m}_L^{n+e+1} \ .$$

b) En déduire que $U^{(n)}$ est un sous-$\mathbb{Z}_p$-module sans p-torsion et d'indice fini de $U^{(1)}$ et que, si $u \in U^{(n)}$, alors $u^p \in U^{(n+e)}$.

c) Montrer que, pour tout $m \in \mathbb{N}$, l'application de $U^{(n)}$ dans $U^{(n+e)}/U^{(n+e+m)}$, qui à u associe l'image de u^p est surjective. **Indication** *On pourra procéder par récurrence sur m.*

d) En déduire que

$$U^{(n)}/(U^{(n)})^p \ \cong \ U^{(n)}/U^{(n+e)}$$

et que $U^{(n)}$ est un $\mathbb{Z}_p$-module libre de rang d.

e) Montrer que $U^{(1)}$ est le produit direct d'un groupe cyclique d'ordre une puissance de p par un $\mathbb{Z}_p$-module libre de rang p et que $\mathcal{O}_L^*$ est le produit direct d'un groupe cyclique fini par un $\mathbb{Z}_p$-module libre de rang d.

Exercice C

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 D

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.