Université Paris Sud — Année 2007-2008

M1 — Arithmétique

Examen du 10 juin 2008

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.

Pour tout nombre premier p, on choisit une clôture algébrique $\overline{\mathbb{Q}_p}$ de $\mathbb{Q}_p$ et on note v_p l'unique valuation de $\overline{\mathbb{Q}_p}$ telle que $v_p(p) = 1$. Les quatre problèmes peuvent être traités indépendamment. Mais certains des résultats de A et B sont utiles pour C. Le quatrième problème, totalement indépendant des autres, est facultatif.

Exercice A

Soient K un corps, d un entier ≥ 1 et L une extension finie séparable de K de degré d. Soient λ un élément de L tel que $L = K[\lambda]$ et soit P le polynôme minimal de λ.

1) On note $N_{L/K}$ la norme de L à K.

a) Soit $c \in K$. Montrer que $N_{L/K}(\lambda + c) = (-1)^d P(-c)$.

b) Soient $u, v \in K$, avec $u \neq 0$. Montrer que $N_{L/K}(u\lambda + v) = (-u)^d P(-v/u)$.

2) On suppose que $P = X^d + aX + b$, avec $d \geq 2$, $a, b \in K$. Calculer $N_{L/K}(\lambda P'(\lambda))$. En déduire que le discriminant du polynôme P est égal à

$$(-1)^{\frac{d(d-1)}{2}}(d^d b^{d-1} + (-1)^{d-1}(d-1)^{d-1}a^d)\ .$$

Exercice B

Soit p un nombre premier.

1) Soient F une extension finie de $\mathbb{Q}_p$ et F_0 l'extension maximale non ramifiée de $\mathbb{Q}_p$ contenue dans F. On pose $e = [F : F_0]$, $f = [F_0 : \mathbb{Q}_p]$, on choisit une uniformisante π de F et on note P_π le polynôme minimal de π sur L_0. On note $\mathcal{O}_F$ l'anneau des entiers de F, $\mathcal{D}_F$ (resp. δ_F) la différente (resp. le discriminant) de $\mathcal{O}_F/\mathbb{Z}_p$.

a) Montrer que $\mathcal{D}_F$ est l'idéal de $\mathcal{O}_F$ engendré par $P'_\pi(\pi)$.

b) Montrer que $v_p(\delta_F) \geq f(e-1)$ avec égalité si et seulement si e est premier à p.

2) Soient E une extension finie de $\mathbb{Q}$ et d_E le discriminant de E. On suppose que

$$\mathbb{Q}_p \otimes_{\mathbb{Q}} E \ = \ L_1 \times L_2 \times \dots L_g$$

où $L_1, L_2, \dots, L_g$ sont des extensions finies de $\mathbb{Q}_p$. Pour $i = 1, 2, \dots, g$, on note e_i l'indice de ramification de l'extension $L_i/\mathbb{Q}_p$ et f_i son degré résiduel.

a) Montrer que $v_p(d_E) \geq \Sigma_{i=1}^{g} f_i(e_i - 1)$.

b) A quelle condition a-t'on l'égalité ?

Exercice C

Soit $P = X^5 - 5X + 5 \in \mathbb{Q}[X]$.

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

Dans la suite on note E le corps $\mathbb{Q}[X]/(P)$ et λ l'image de X dans E.

2) Montrer que

$$\mathbb{R} \otimes_{\mathbb{Q}} E \ \simeq \ \mathbb{R} \times \mathbb{C} \times \mathbb{C}\,.$$

3) Calculer le discriminant du polynôme P.

4 .a) Montrer que $E/\mathbb{Q}$ est non ramifiée en dehors de 3, 5 et 41.

b) Si p est un nombre premier différent de 3, 5 ou 41, l'anneau $\mathbb{Z}[\lambda]$ est il p-clos ?

5 .a) Montrer que $v_{41}(d_E) = 1$.

b) En déduire que $\mathbb{Z}[\lambda]$ est 41-clos et qu'il existe un et un seul idéal maximal $\mathfrak{p}$ de $\mathcal{O}_E$ au-dessus de 41 qui est ramifié dans l'extension $E/\mathbb{Q}$.

c) Calculer l'indice de ramification et le degré résiduel de $\mathfrak{p}/(41)$.

6 .a) Combien y-a-t'il d'idéaux maximaux de $\mathcal{O}_E$ au-dessus de 5 ?

b) Calculer $v_5(d_E)$.

c) L'anneau $\mathbb{Z}[\lambda]$ est-il 5-clos ?

7 .a) Montrer qu'il existe deux éléments distincts μ_1, μ_2 dans $\mathbb{Z}_3$ tels que $P(3\mu_1 - 1) = P(3\mu_2 - 1) = 0$.

b) Montrer que

$$\mathbb{Q}_3 \otimes_{\mathbb{Q}} E \ \simeq \ \mathbb{Q}_3 \times \mathbb{Q}_3 \times L_3$$

où L_3 est une extension finie non ramifiée de $\mathbb{Q}_3$.

c) Combien y-a-t'il d'ideaux maximaux de $\mathcal{O}_E$ au-dessus de 3 ? **Indication** *On pourra regarder la décomposition en produit de polynômes irréductibles de l'image de P dans $\mathbb{F}_3[X]$.*

d) Déterminer le degré résiduel et l'indice de ramification de chacun d'eux.

e) L'anneau $\mathbb{Z}[\lambda]$ est il 3-clos ?

8) Calculer d_E.

9) On note M le plus petit sous-corps de $\mathbb{C}$ qui contient toutes les racines du polynôme $X^5 - 5X + 5$.

a) Quels sont les nombres premiers p qui sont ramifiés dans l'extension $M/\mathbb{Q}$?

b) Montrer que M contient le corps $M_0 = \mathbb{Q}(5 \times 41)^{1/2}$, que $\mathcal{O}_{M_0}$ a un et un seul idéal maximal $\mathfrak{p}_0$ au-dessus de 5 et que $\mathfrak{p}_0$ est le seul idéal ramifié dans l'extension M/M_0.

Exercice D

Dans ce problème p est un nombre premier, on choisit une clôture algébrique $\overline{\mathbb{F}_p}$ du corps $\mathbb{F}_p$. Pour tout entier q qui est une puissance de p, on note $\mathbb{F}_q$ l'unique sous-corps de $\overline{\mathbb{F}_p}$ qui a q-éléments. Soit P un polynôme non constant en l'indéterminée T à coefficients dans le corps $\mathbb{F}_p$. On suppose que $(P, P') = 1$ et on note E le quotient de $\mathbb{F}_p[T]$ par l'idéal engendré par P.

1 .a) Montrer qu'il existe un entier $s \geq 1$ et des entiers $r_1 \leq r_2 \ldots \leq r_s$ uniquement déterminés tels que l'anneau E soit isomorphe au produit

$$\mathbb{F}_{p^{r_1}} \times \mathbb{F}_{p^{r_2}} \times \ldots \times \mathbb{F}_{p^{r_s}} \ .$$

b) Exprimer le nombre de facteurs irréductibles de P et le degré d de P en fonction de s et des r_i.

2 .a) Montrer que l'application $\alpha \ : \ E \ \rightarrow \ E$ qui envoie a sur $a^p - a$ est un endomorphisme du $\mathbb{F}_p$-espace vectoriel sous-jacent.

b) Montrer que la dimension du noyau de α est égal au nombre de facteurs irréductibles de P (en particulier, P est irréductible si et seulement si la dimension du noyau de α est égale à 1).